Configuración del servidor Syslog externo en ISE

Contenido

Introducción

Este documento describe cómo configurar el servidor Syslog externo en ISE.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Identity Services Engine (ISE).
- Servidores Syslog

Componentes Utilizados

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

- Identity Services Engine (ISE) versión 3.3.
- Servidor Kiwi Syslog v1.2.1.4

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

Antecedentes

.

Los recopiladores de registros recopilan y almacenan los mensajes de Syslog de ISE. Estos recopiladores de registros se asignan a los nodos de supervisión para que MnT almacene los registros recopilados localmente.

Para recopilar registros externamente, debe configurar servidores syslog externos, que se denominan destinos. Los registros se clasifican en varias categorías predefinidas.

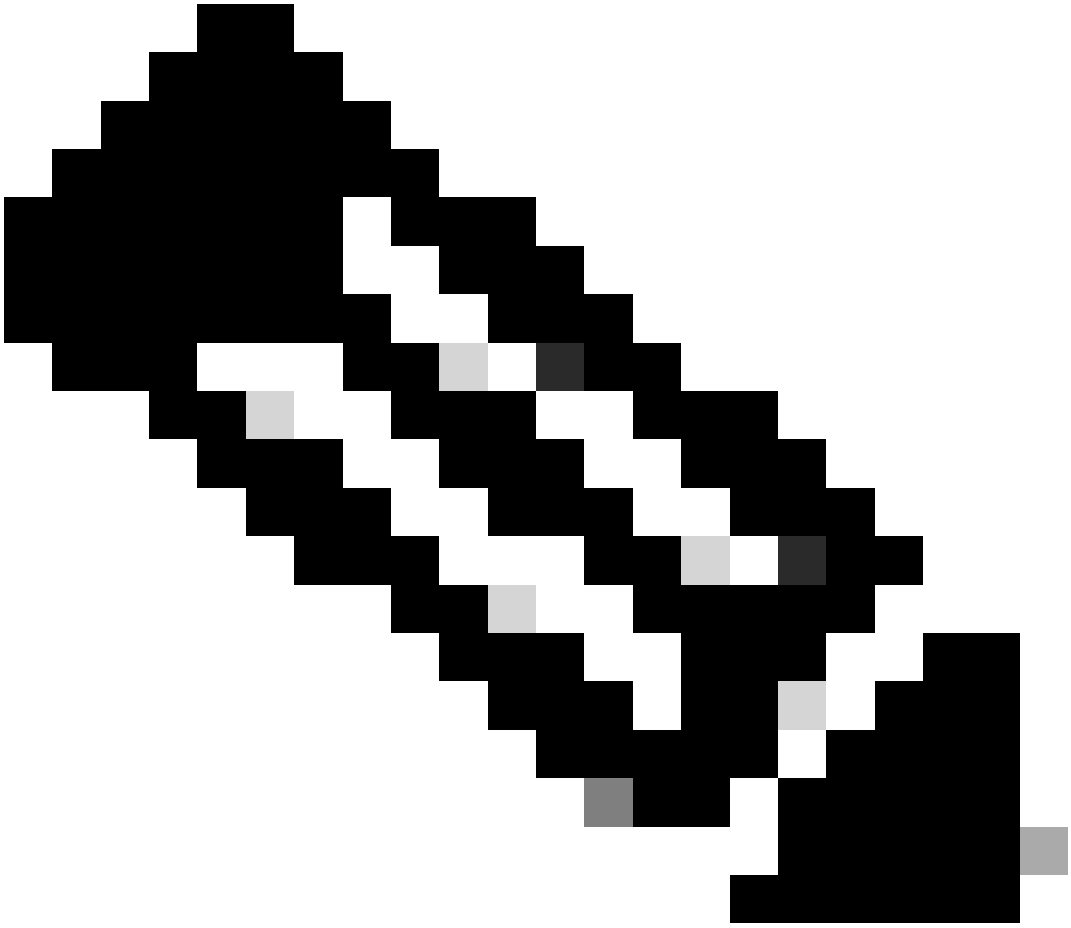
Puede personalizar la salida de registro editando las categorías con respecto a sus destinos, nivel de gravedad, etc.

Configuración

Puede utilizar la interfaz web para crear destinos de servidor syslog remotos a los que se envían mensajes de registro del sistema. Los mensajes de registro se envían a los destinos del servidor syslog remoto de acuerdo con el estándar del protocolo syslog (consulte RFC-3164).

Configuración del destino de registro remoto (UDP Syslog)

En la GUI de Cisco ISE, haga clic en el icono de menú () y seleccione Administración>Sistema>Registro>Destinos de registro remoto > Haga clic en Agregar.



Nota: Este ejemplo de configuración se basa en la captura de pantalla denominada: Configuración del Destino de Registro Remoto.

- Nombre como Remote_Kiwi_Syslog, aquí puede introducir el nombre del servidor de Syslog remoto, que se utiliza con fines descriptivos.
- Target Type as UDP Syslog, en este ejemplo de configuración, UDP Syslog se está utilizando; sin embargo, puede configurar más opciones de la lista desplegable Target Type:

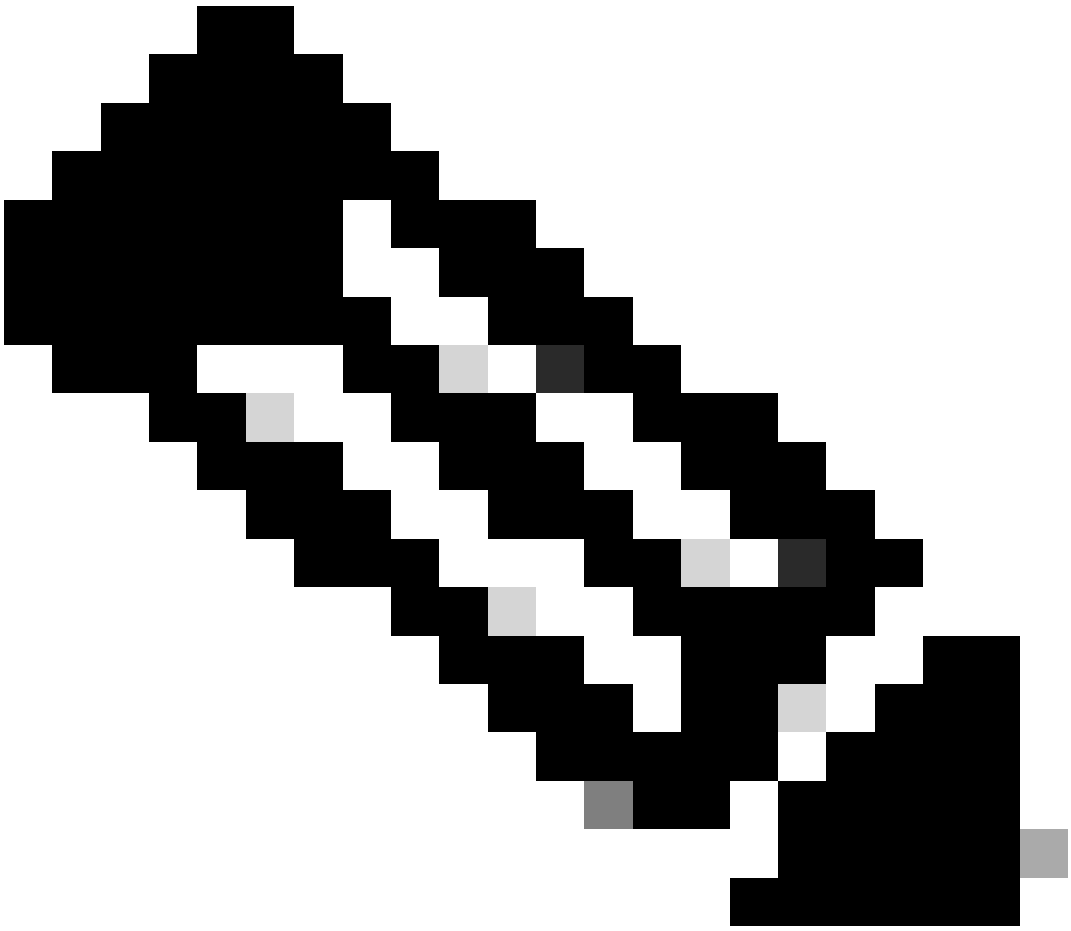
UDP Syslog: Se utiliza para enviar mensajes de syslog a través de UDP, adecuado para un registro ligero y rápido.

TCP Syslog: se utiliza para enviar mensajes de syslog a través de TCP, lo que proporciona fiabilidad con funciones de comprobación de errores y retransmisión.

Syslog seguro: hace referencia a los mensajes de syslog que se envían a través de TCP con cifrado TLS, lo que garantiza la integridad y confidencialidad de los datos.

- Status as Enabled, debe elegirEnabled en la lista desplegable Status (Estado).

- Descripción, si lo desea, puede introducir una breve descripción del nuevo destino.
- Host/Dirección IP, donde debe introducir la dirección IP o el nombre de host del servidor de destino que almacena los registros.Cisco ISE admite los formatos IPv4 e IPv6 para el registro.



Nota: Es esencial mencionar que si va a configurar un servidor syslog con FQDN, debe configurar el almacenamiento en caché de DNS para evitar el impacto en el rendimiento. Sin almacenamiento en caché de DNS, ISE consulta al servidor DNS cada vez que debe enviarse un paquete syslog al destino de registro remoto configurado con FQDN. Esto tiene un gran impacto en el rendimiento de ISE.

Utilice service cache enableel comando en todas las PSN de la implementación para superar esto:

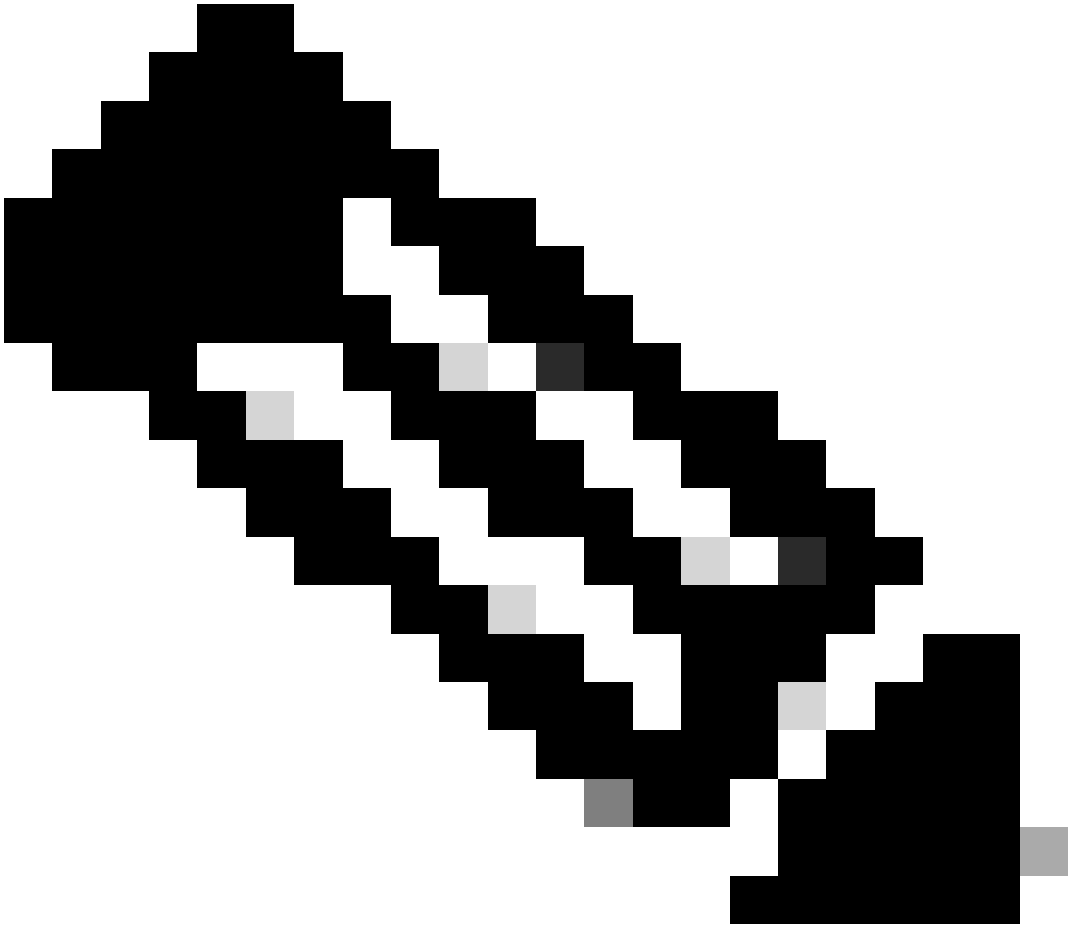
Ejemplo:

```
ise/admin(config)# service cache enable hosts ttl 180
```

- **Puerto** como **514**, en este ejemplo de configuración, el servidor Syslog Kiwi escucha en el puerto **514** que es el puerto predeterminado para los mensajes syslog UDP. Sin embargo, los usuarios pueden cambiar este número de puerto a cualquier valor entre 1 y 65535.Asegúrese de que ningún firewall está bloqueando el puerto deseado.

- **Facility Code** como **LOCAL6**, puede elegir el código de recurso de syslog que se debe utilizar para el registro, en la lista desplegable. Las opciones válidas son de Local0 a Local7.

- **Longitud máxima** como **1024**, aquí puede ingresar la longitud máxima de los mensajes de destino del registro remoto. La longitud máxima está establecida en **1024** de forma predeterminada en la versión 3.3 de ISE, los valores van de 200 a 1024 bytes.



Nota: Para evitar el envío de mensajes truncados al destino de registro remoto, puede modificar la Longitud máxima como 8192.

- **Incluir alarmas para este destino,** para que sea sencillo, en este ejemplo de configuración, **Incluir alarmas para este destino no está marcado; sin embargo,** cuando marca esta casilla de verificación, los mensajes de alarma también se envían al servidor remoto.

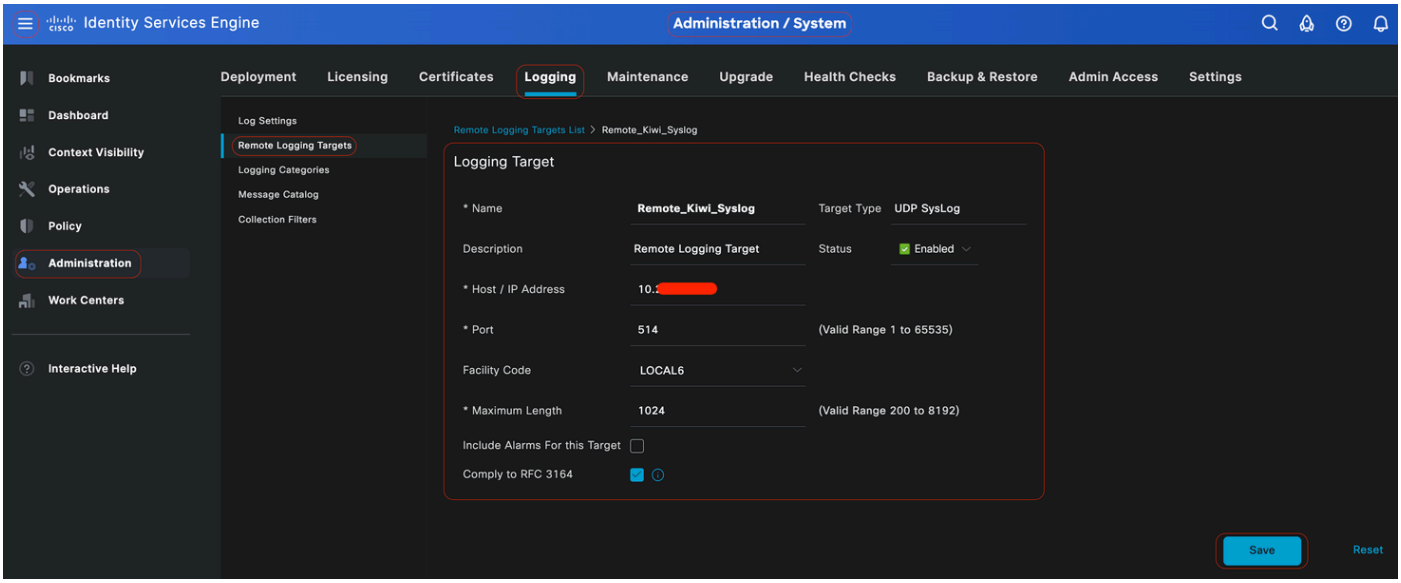
- **La opción Cumplir con RFC 3164** está marcada, cuando se marca esta casilla de verificación, los delimitadores (, ; { } \ \) de los mensajes de syslog enviados a los servidores remotos no escapan aunque se utilice una barra diagonal inversa (\).

-

Una vez finalizada la configuración, haga clic en **Save**.

-

Una vez guardado, el sistema mostrará esta advertencia: **Ha elegido crear una conexión no segura (TCP/UDP) con el servidor. ¿Está seguro de que desea continuar?**, haga clic en **Sí**.



Configuración del destino remoto

Configuración del Destino Remoto en Categorías de Registro

Cisco ISE envía eventos auditables al destino de syslog. Una vez configurado el destino de registro remoto, deberá asignar el **destino de registro remoto** a las categorías deseadas para reenviar los eventos auditables.

Los destinos de registro se pueden asignar a cada una de estas categorías de registro. Los registros de eventos de estas categorías de registro se generan sólo a partir de nodos PSN y se pueden configurar para enviar los registros relevantes al servidor Syslog remoto, en función de los servicios que estén habilitados en esos nodos:

- **Auditoría AAA**
- **Diagnóstico de AAA**
- **Contabilidad**
- **MDM externa**
- **ID pasiva**
- **Auditoría de aprovisionamiento de clientes y estado**
- **Diagnósticos de aprovisionamiento de clientes y estado**
- **Profiler**

Los registros de eventos de estas categorías de registro se generan a partir de todos los nodos de la implementación y se pueden configurar para enviar los registros relevantes al servidor Syslog remoto:

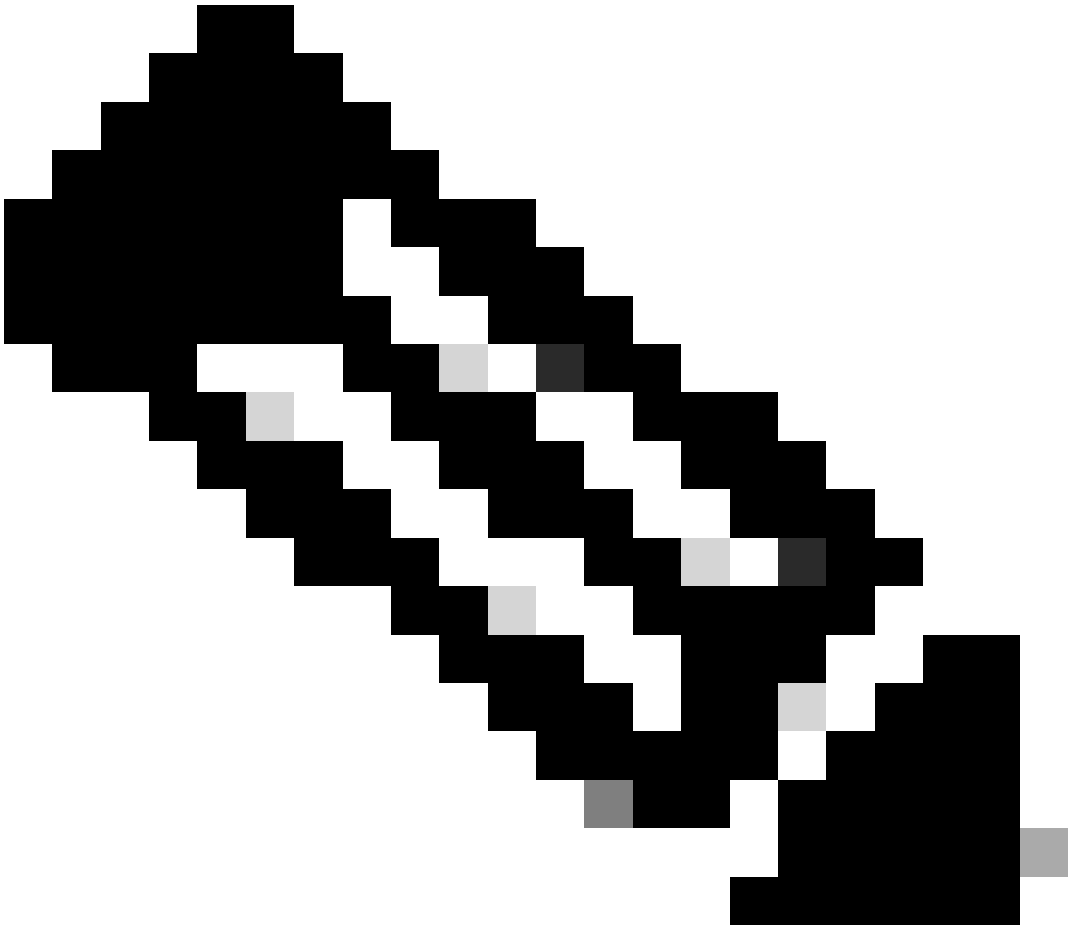
- **Auditoría administrativa y operativa**
-

Diagnóstico del sistema

•

Estadísticas del sistema

En este ejemplo de configuración, va a configurar el destino remoto en cuatro categorías de registro, estas 3 para enviar registros de tráfico de autenticación: **Autenticaciones pasadas**, **Intentos fallidos** y **Contabilización de radio** y esta categoría para el tráfico de registro del administrador de ISE:



Nota: **Este ejemplo de configuración se basa en la captura de pantalla denominada: Configuración del Destino de Registro Remoto**

En la GUI de Cisco ISE, haga clic en el icono de menú () y seleccione **Administration>System>Logging>Logging Categories**, y haga clic en **la categoría requerida** (**Autenticaciones pasadas, Intentos fallidos y Contabilización RADIUS).**

Paso 1-Nivel de gravedad del registro: Un mensaje de evento se asocia a un nivel de gravedad, que permite a un administrador filtrar los mensajes y asignarle prioridad. Seleccione el nivel de gravedad del registro según sea necesario. Para algunas categorías de registro, este valor se establece de forma predeterminada y no se puede editar. Para algunas categorías de registro, puede elegir uno de estos niveles de gravedad en una lista desplegable:

- **MORTAL**: Nivel de emergencia. Este nivel significa que no puede utilizar Cisco ISE y que debe tomar inmediatamente las medidas necesarias.
- **ERROR**: este nivel indica una condición de error crítico.
- **ADVERTENCIA**: Este nivel indica una condición normal pero significativa. Este es el nivel predeterminado establecido para muchas categorías de registro.
- **INFO**: Este nivel indica un mensaje informativo.
-

DEBUG: Este nivel indica un mensaje de error de diagnóstico.

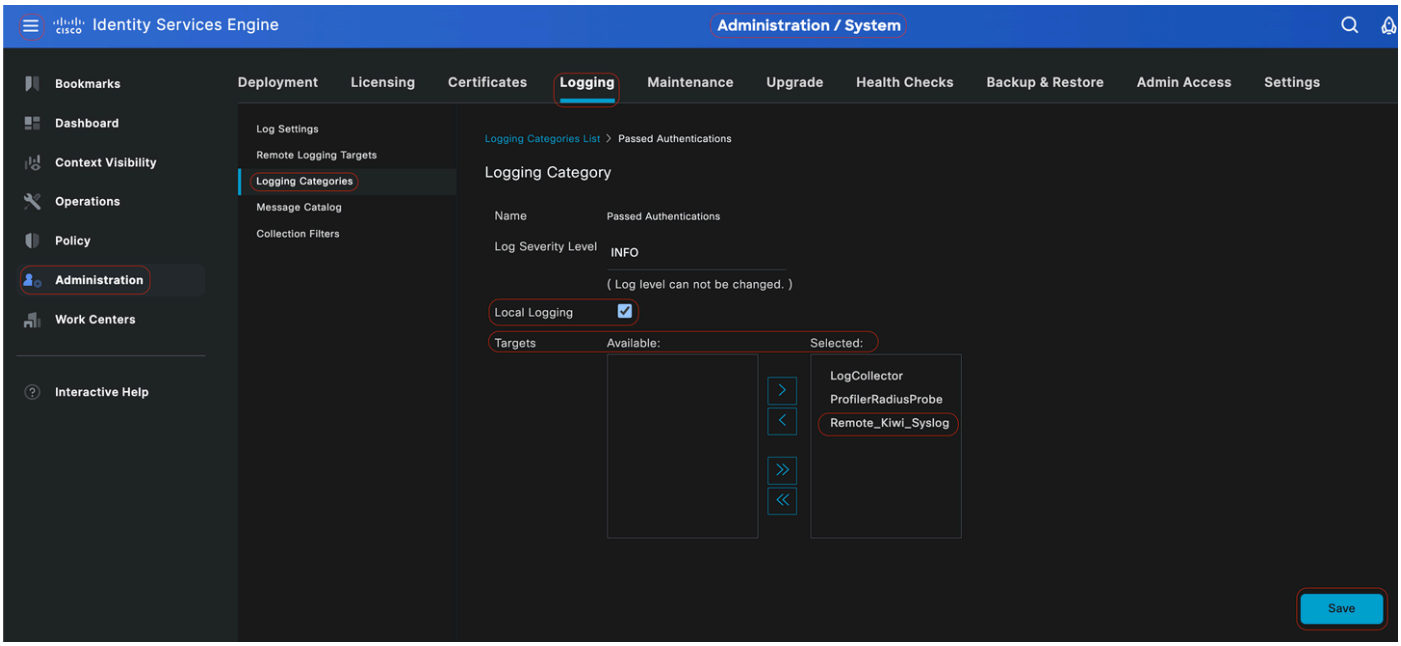
Paso 2: **Registro Local: Esta casilla de verificación habilita la generación de registro local.** Esto significa que los registros generados por los PSN también se guardan en el PSN específico que genera el registro. Se recomienda mantener la configuración predeterminada

Paso 3: Destinos: Esta área permite elegir los destinos de una categoría de registro mediante la transferencia de los destinos entre las áreasDisponible y Seleccionadasmediante los iconos de flecha hacia la izquierda y hacia la derecha.

El área Disponible contiene los destinos de registro existentes, tanto locales (predefinidos) como externos (definidos por el usuario).

El área Seleccionado, que inicialmente está vacía, muestra los destinos que se han seleccionado para la categoría.

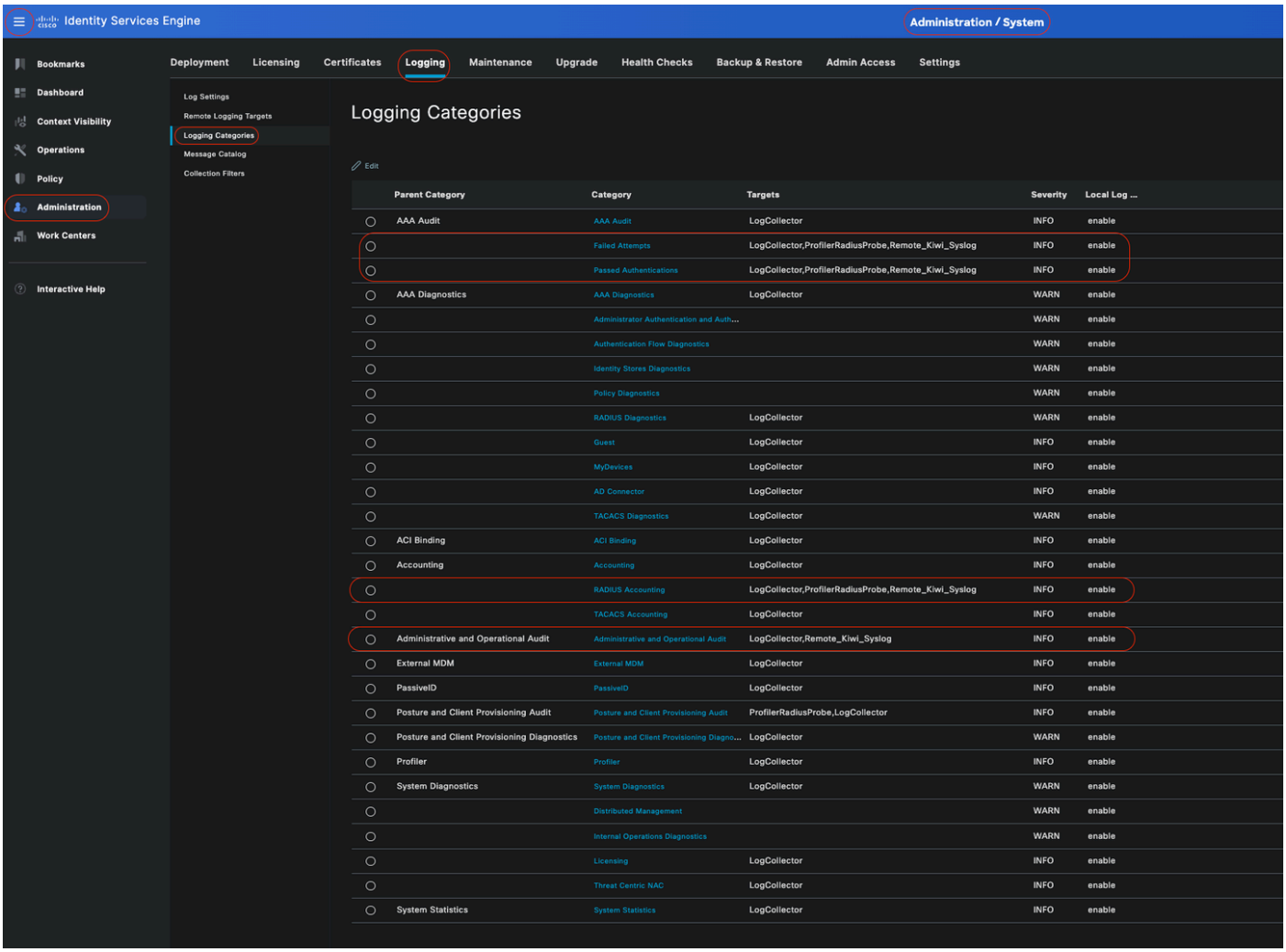
Paso 4- Repita del paso 1 al paso 3 para agregar el destino remoto en las categorías **Intentos fallidos y Contabilización de radio**.



Asignación de destinos remotos a las categorías deseadas

Paso 5- Compruebe que el destino remoto se encuentra en las categorías requeridas.Debe poder ver el destino remoto que acaba de agregar.

En esta captura de pantalla, puede ver el destino remoto **Remote_Kiwi_Syslog** asignado a las categorías requeridas.



Verificación de categorías

Descripción de categorías

Se genera un mensaje cuando se produce un evento. Existen diferentes tipos de mensajes de eventos generados a partir de varios recursos, como el núcleo, el correo, el nivel de usuario, etc.

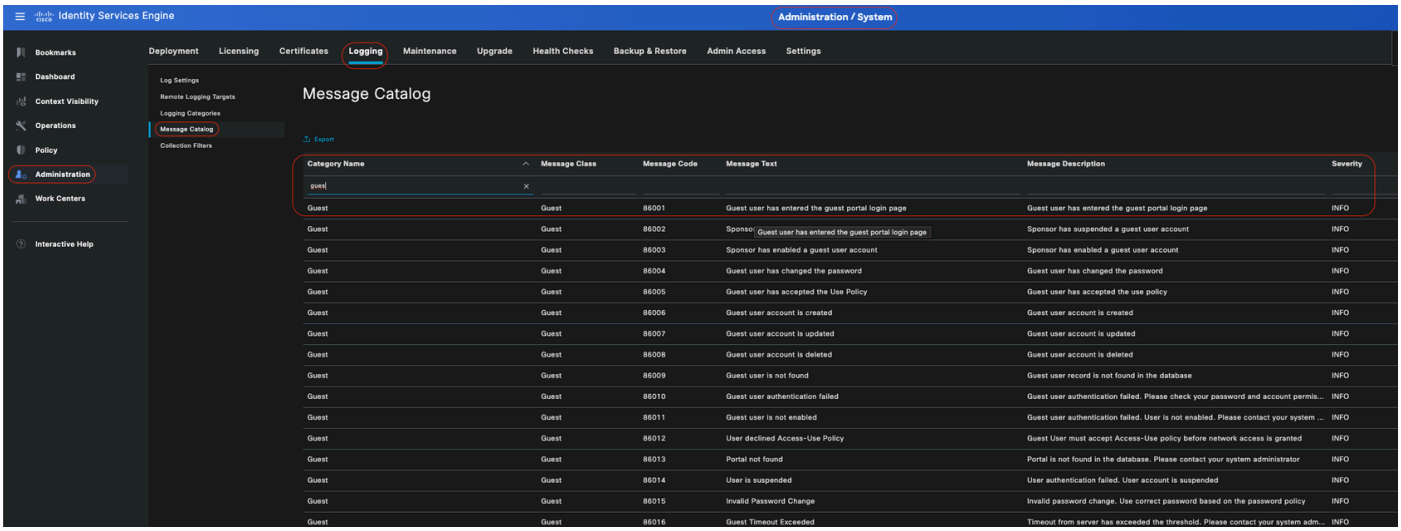
Estos errores se categorizan dentro del Catálogo de mensajes y estos eventos también se organizan jerárquicamente en categorías.

Estas categorías tienen categorías principales que contienen una o algunas categorías.

Categoría principal	Categoría
Auditoría AAA	Auditoría AAA Intentos fallidos Autenticación superada
Diagnóstico de AAA	Diagnóstico de AAA Autenticación y autorización del administrador

	Diagnóstico de flujo de autenticación Diagnóstico del almacén de identidades Diagnóstico de políticas Diagnóstico de Radius Guest
Contabilidad	Contabilidad Contabilización RADIUS
Auditoría administrativa y operativa	Auditoría administrativa y operativa
Auditoría de aprovisionamiento de clientes y estado	Auditoría de aprovisionamiento de clientes y estado
Diagnósticos de aprovisionamiento de clientes y estado	Diagnósticos de aprovisionamiento de clientes y estado
Profiler	Profiler
Diagnóstico del sistema	Diagnóstico del sistema Administración distribuida Diagnóstico de operaciones internas
Estadísticas del sistema	Estadísticas del sistema

En esta captura de pantalla puede ver que **Guest** es una clase de mensaje y está categorizada como **Guest Category**. Esta categoría de invitado tiene una categoría principal denominada **Diagnósticos AAA**.



Catálogo de mensajes

Verificación y resolución de problemas

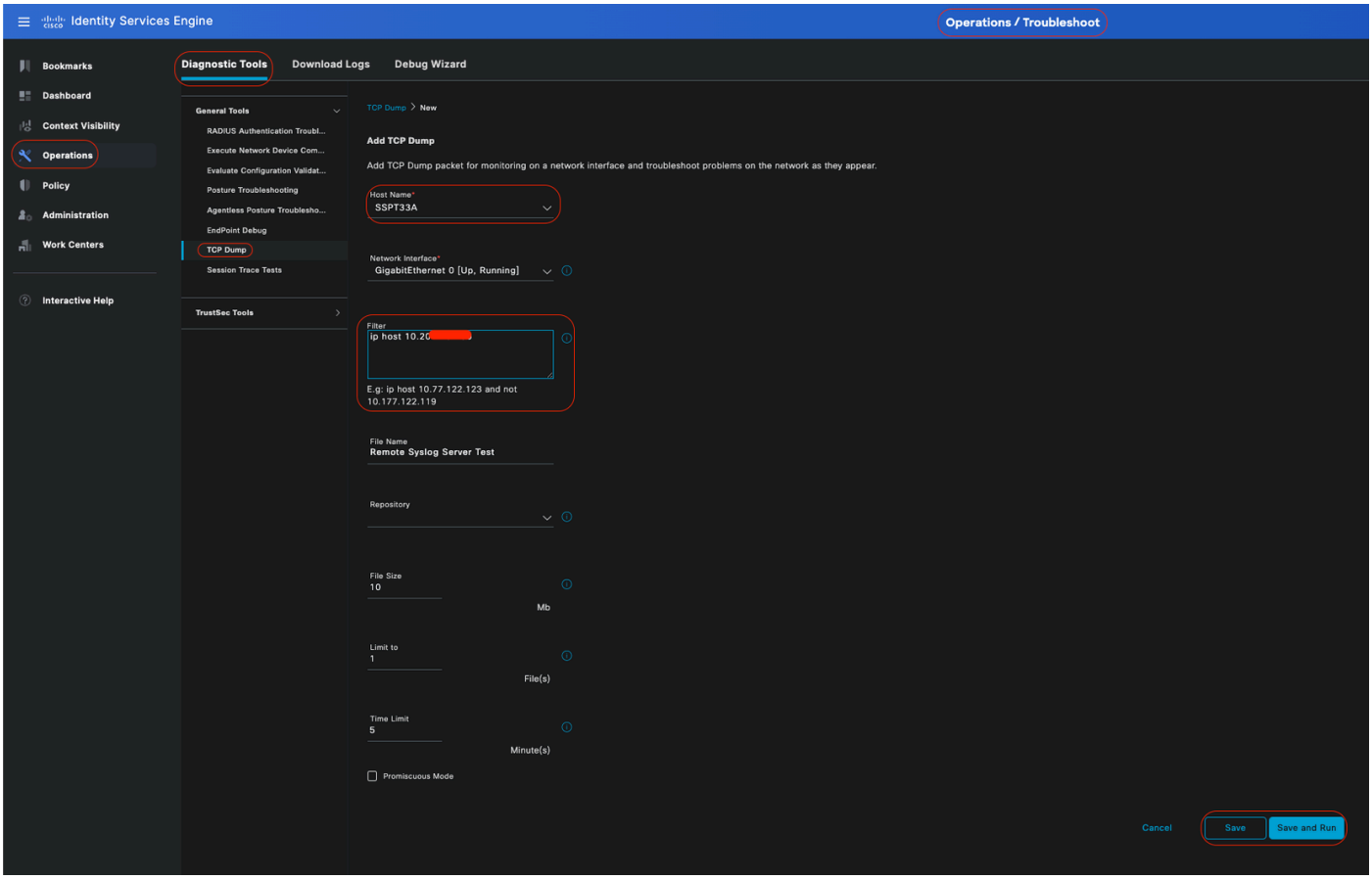
Realizar un volcado TCP contra el destino de registro remoto es el paso más rápido de solución de problemas y verificación para confirmar si se están enviando o no eventos de registro.

La captura se debe realizar desde el PSN que autentica al usuario porque PSN va a generar mensajes de registro y estos mensajes se van a enviar al destino remoto

En la GUI de Cisco ISE, haga clic en el icono Menú ( ) y seleccione **Operaciones**> **Solucionar problemas**>**Volcado TCP**> Haga clic en **Agregar**.

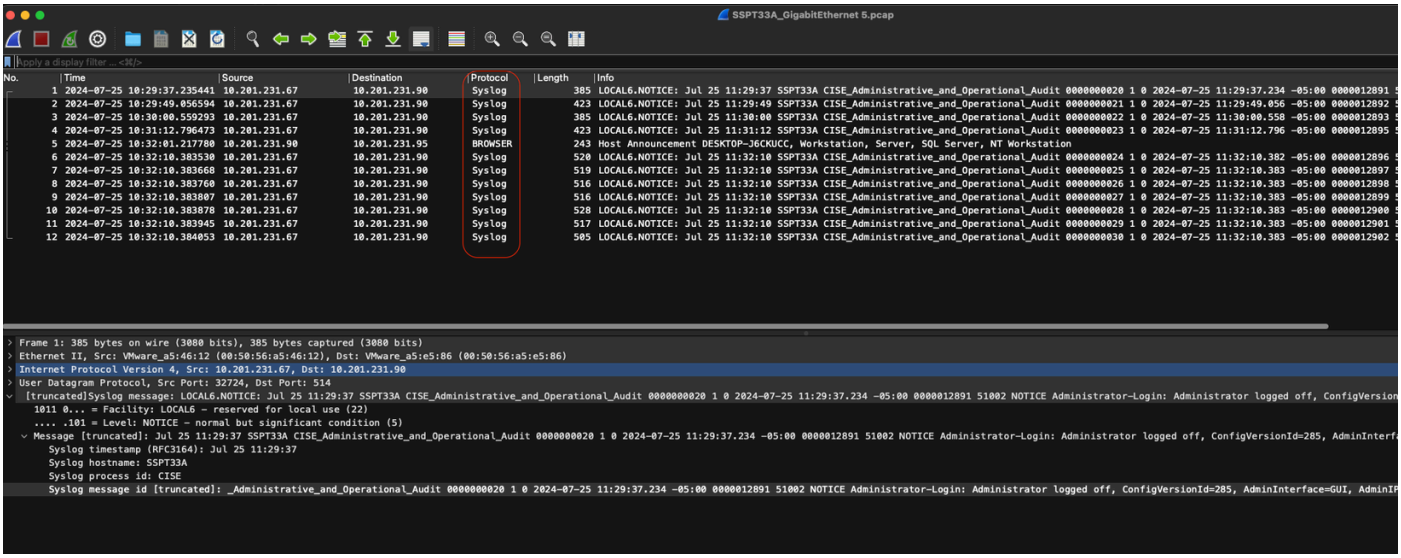
- Debe filtrar el tráfico, agregar el campo de filtro de host IP <remote_target_IP_address>.

- Debe tomar la captura de las autenticaciones de gestión de PSN.



Volcado de TCP

En esta captura de pantalla, puede ver cómo ISE envía mensajes de Syslog para el tráfico de registro del administrador de ISE.



Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).