Configurar Servidor syslog externo no ISE

Contents

Introdução

Este documento descreve como configurar o Servidor syslog externo no ISE.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Identity Services Engine (ISE).
- Servidores Syslog

Componentes Utilizados

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

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

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 a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

.

As mensagens de syslog do ISE são coletadas e armazenadas pelos coletores de log. Esses coletores de logs são atribuídos aos nós de monitoramento para que o MnT armazene os logs coletados localmente.

Para coletar logs externamente, você configura servidores syslog externos, que são chamados de destinos. Os registros são classificados em várias categorias predefinidas.

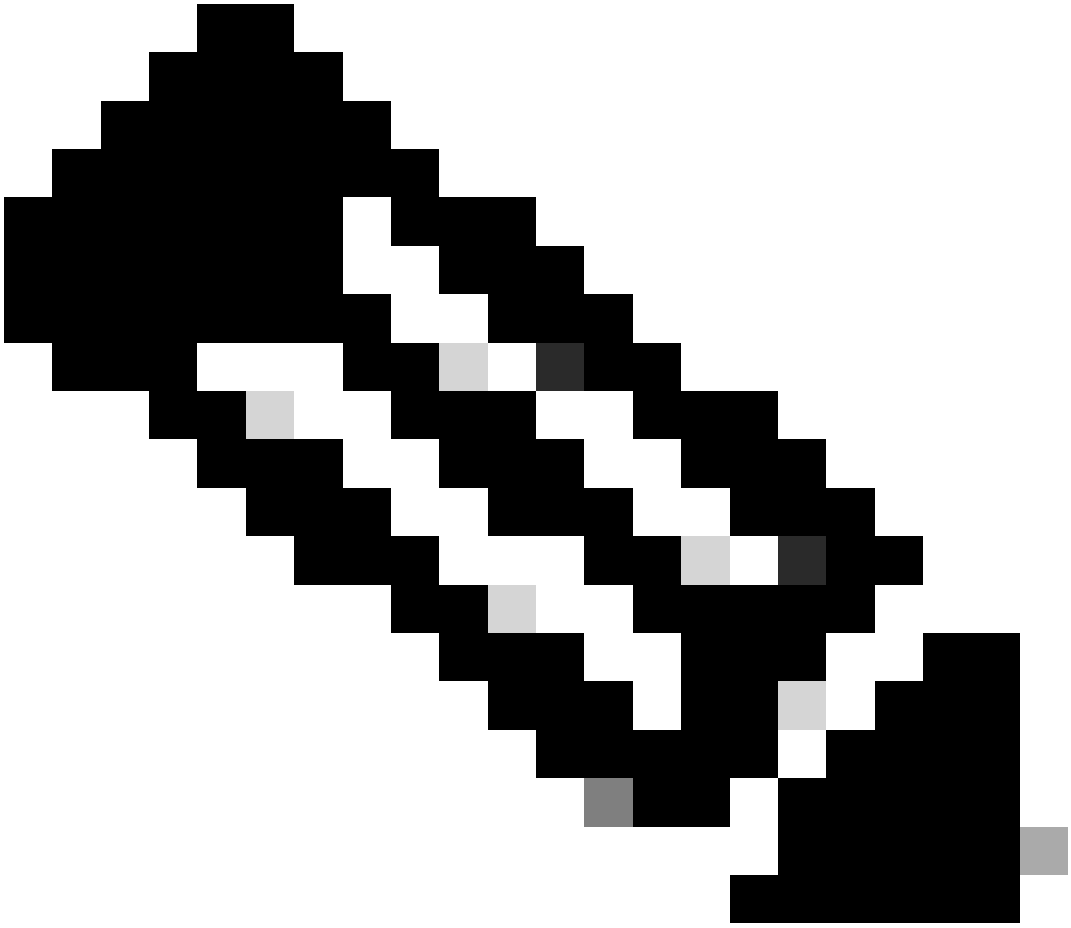
Você pode personalizar a saída do registro editando as categorias com relação aos seus destinos, nível de gravidade e assim por diante.

Configuração

Você pode usar a interface da Web do para criar destinos remotos do Servidor syslog para os quais as mensagens de log do sistema são enviadas. As mensagens de log são enviadas aos destinos do servidor syslog remoto de acordo com o padrão do protocolo syslog (consulte RFC-3164).

Configurando o destino de registro remoto (UDP Syslog)

Na GUI do Cisco ISE, clique no ícone Menuicon ( ) e selecioneAdministração>Sistema>Registro>Destinos de registro remoto > Clique em Adicionar.



Observação: este exemplo de configuração é baseado na captura de tela chamada: Configurando o destino de registro remoto.

- Name as Remote_Kiwi_Syslog, aqui você pode digitar o nome do servidor Syslog Remoto, que é usado para fins descritivos.
- Target Type as UDP Syslog, neste exemplo de configuração, o UDP Syslog está sendo usado; no entanto, você pode configurar mais opções na lista suspensa Target Type:

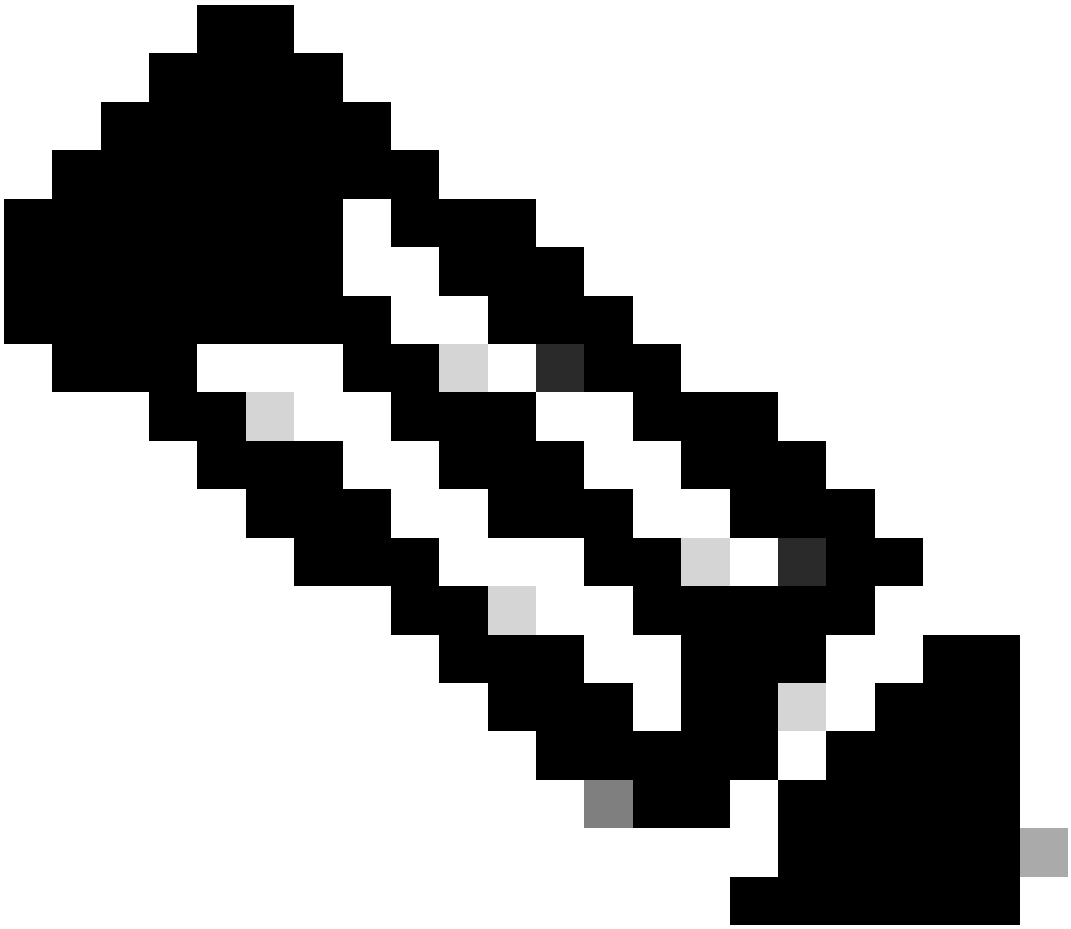
UDP Syslog: usado para enviar mensagens de syslog por UDP, adequado para registro leve e rápido.

Syslog TCP: usado para enviar mensagens de syslog sobre TCP, que fornece confiabilidade com verificação de erros e recursos de retransmissão.

Syslog seguro: refere-se a mensagens de syslog enviadas por TCP com criptografia TLS, garantindo a integridade e a confidencialidade dos dados.

- Status como Enabled, você deve escolherEnabledna lista suspensa Status.

- Descrição, como opção, você pode informar uma breve descrição do novo alvo.
- Host/endereço IP, aqui você digita o endereço IP ou o nome de host do servidor de destino que armazena os logs. O Cisco ISE suporta os formatos IPv4 e IPv6 para registro.



Observação: é essencial mencionar que, se você for configurar um Servidor syslog com FQDN, deverá configurar o cache DNS para evitar impacto no desempenho. Sem o cache DNS, o ISE consulta o servidor DNS cada vez que um pacote de syslog precisa ser enviado ao destino de registro remoto configurado com o FQDN. Isso tem um impacto sério no desempenho do ISE.

Use service cache enableo comando em todas as PSNs da implantação para superar isso:

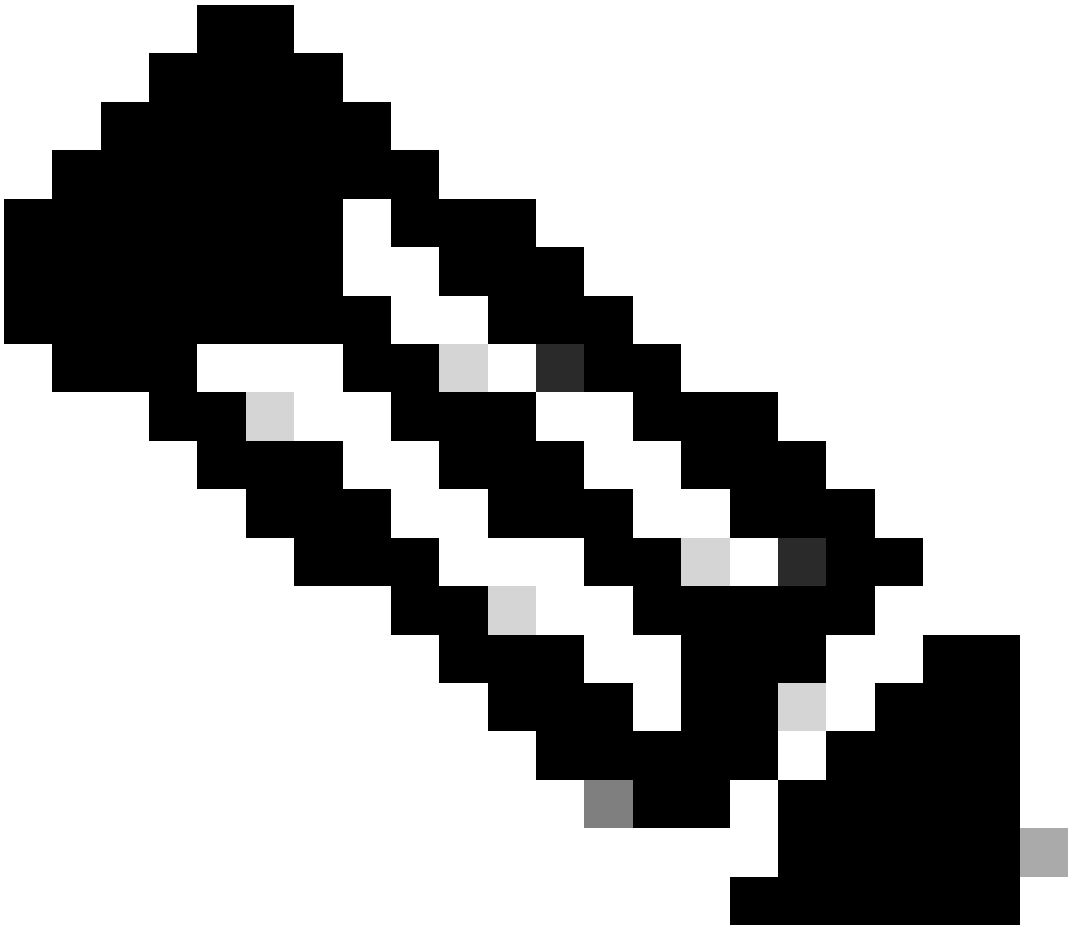
Exemplo

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

• **Porta** como **514**, neste exemplo de configuração, o Servidor Syslog Kiwi está escutando na porta **514**, que é a **porta padrão para mensagens syslog UDP.** No entanto, os usuários podem alterar esse número de porta para qualquer valor entre 1 e 65535.Verifique se a porta desejada não está sendo bloqueada por nenhum Firewall.

• **Código do recurso** como **LOCAL6**, você pode escolher o código do recurso syslog que deve ser usado para o registro, na lista suspensa. As opções válidas são Local0 a Local7.

• **Comprimento máximo** como **1024**, aqui você pode digitar o comprimento máximo das mensagens de destino de log remoto. O comprimento máximo é definido como **1024** por padrão na versão 3.3 do ISE, os valores são de 200 a 1024 bytes.



Observação: para evitar o envio de mensagens truncadas ao seu destino de registro remoto, você pode modificar o Comprimento

máximo como 8192.

- **Incluir alarmes para este alvo**, para mantê- lo simples, neste exemplo de configuração, a opção **Incluir alarmes para este alvo não está assinalada; contudo, quando assinalar esta opção, as mensagens de alarme também serão enviadas para o servidor remoto.**

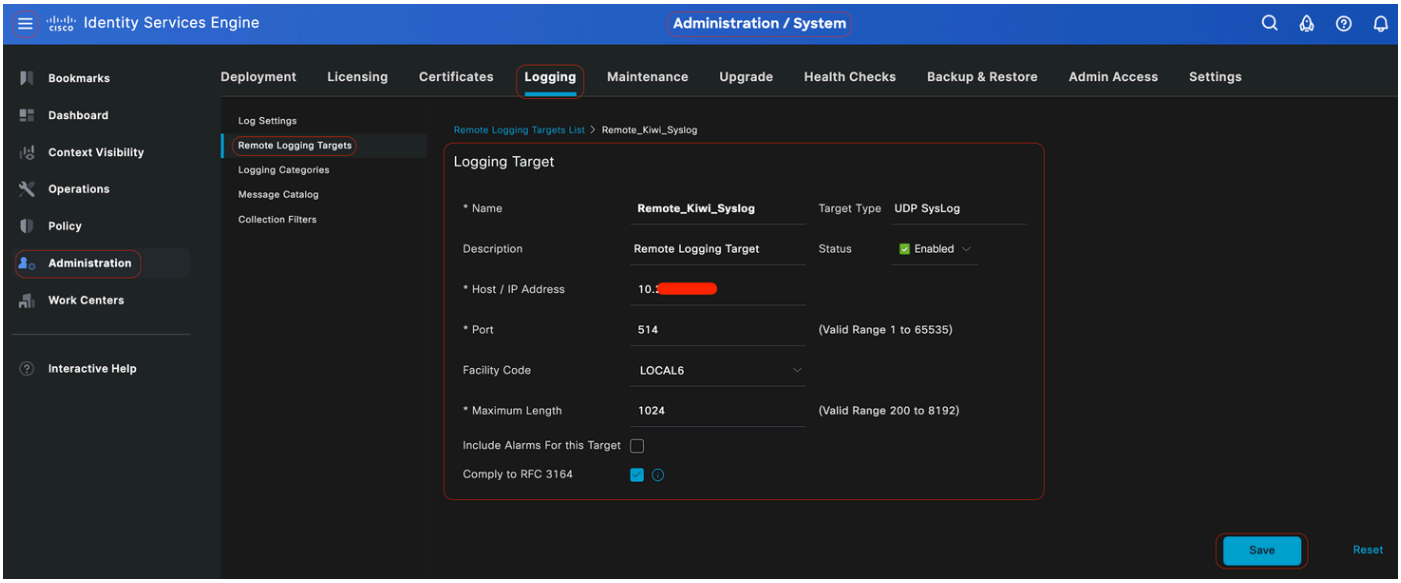
- **A conformidade com RFC 3164** está marcada, quando você marca esta caixa de seleção, os delimitadores (, ; { } \ \) nas mensagens de syslog enviadas aos servidores remotos não são escapados, mesmo se uma barra invertida (\) é usada.

-

Quando a configuração estiver concluída, clique em **Save**.

-

Após salvar, o sistema exibirá este aviso: **Você optou por criar uma conexão não segura (TCP/UDP) com o servidor. Tem certeza de que deseja continuar?**, clique em **Sim**.



Configurando o destino remoto

Configurando Destino Remoto em Registrando Categorias

O Cisco ISE envia eventos auditáveis para o destino do syslog. Depois de ter configurado o Destino de registro remoto, você precisará mapear o **Destino de registro remoto** para as categorias desejadas para encaminhar os eventos auditáveis.

Os destinos de log podem ser mapeados para cada uma dessas categorias de log. Os logs de eventos dessas categorias de log são gerados somente a partir de nós PSN e podem ser configurados para enviar os logs relevantes ao servidor Syslog Remoto, dependendo dos serviços habilitados nesses nós:

- **Auditoria AAA**
- **Diagnóstico AAA**
- **Relatório**
- **MDM externo**
- **ID Passivo**
- **Auditoria de provisionamento de clientes e postura**
- **Diagnóstico de provisionamento de clientes e postura**
- **Profiler**

Os logs de eventos dessas categorias de log são gerados de todos os nós na implantação e podem ser configurados para enviar os logs relevantes ao servidor Syslog Remoto:

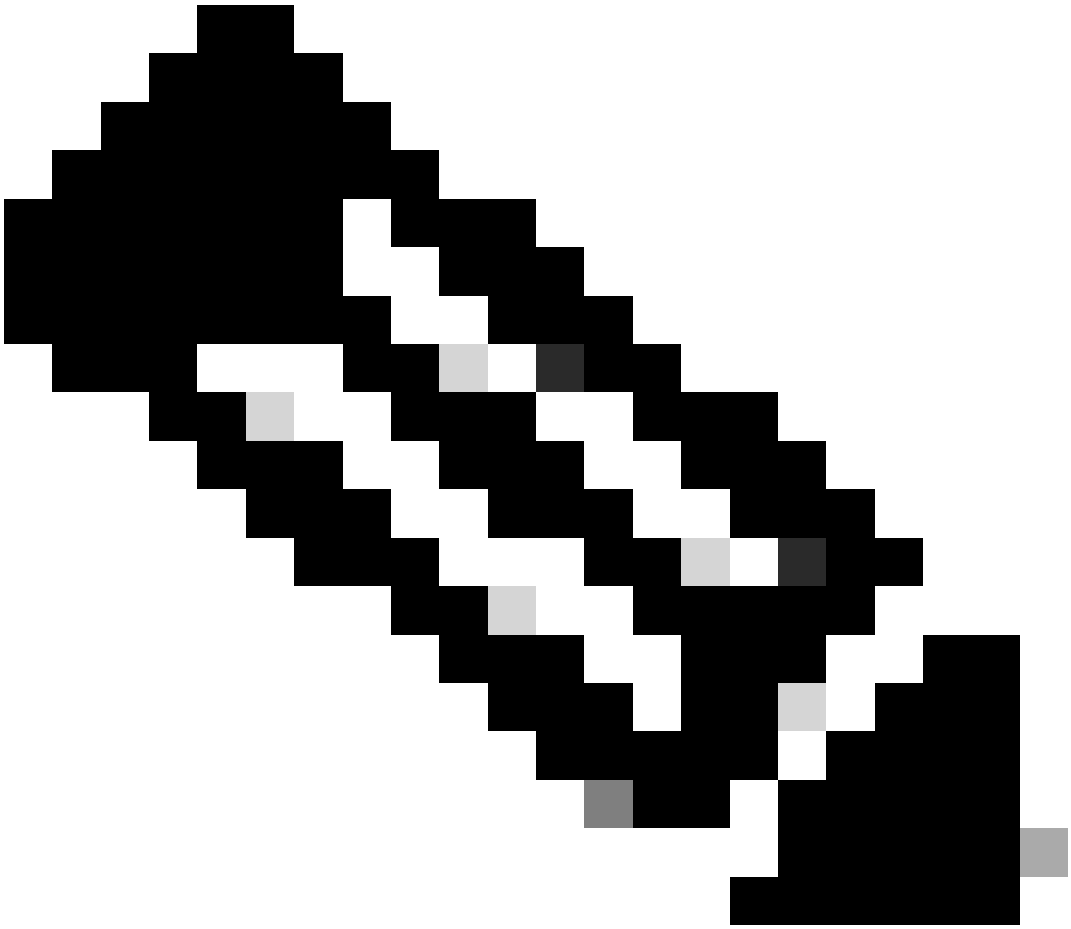
- **Auditoria administrativa e operacional**
-

Diagnóstico do sistema

•

Estatísticas do sistema

Neste exemplo de configuração, você configurará o Destino remoto em quatro Categorias de log, essas 3 para enviar logs de tráfego de autenticação: **Autenticações aprovadas**, **Tentativas com falha** e **Contabilidade Radius** e esta categoria para o tráfego de log do Administrador do ISE:



Observação: **Este exemplo de configuração é baseado na captura de tela: Configurando o destino de registro remoto**

Na GUI do Cisco ISE, clique no ícone do menu () e selecione **Administração>Sistema>**Registro>**Categorias de registro** e clique na **categoria necessária** (**Autenticações aprovadas, Tentativas com falha e Contabilidade de raio).**

Etapa 1-Nível de gravidade do log: Uma mensagem de evento é associada a um nível de gravidade, que permite que um administrador filtre as mensagens e as priorize. Selecione o nível de gravidade do log conforme necessário. Para algumas categorias de log, esse valor é definido por padrão e você não pode editá-lo. Para algumas categorias de log, você pode escolher um destes níveis de gravidade em uma lista suspensa:

- **FATAL**: Nível de emergência. Esse nível significa que você não pode usar o Cisco ISE e deve tomar imediatamente as medidas necessárias.
- **ERRO**: este nível indica uma condição de erro crítica.
- **AVISO**: este nível indica uma condição normal, mas significativa. Esse é o nível padrão definido para muitas categorias de log.
- **INFO**: este nível indica uma mensagem informativa.
- **DEBUG**: Este nível indica uma mensagem de bug de diagnóstico.

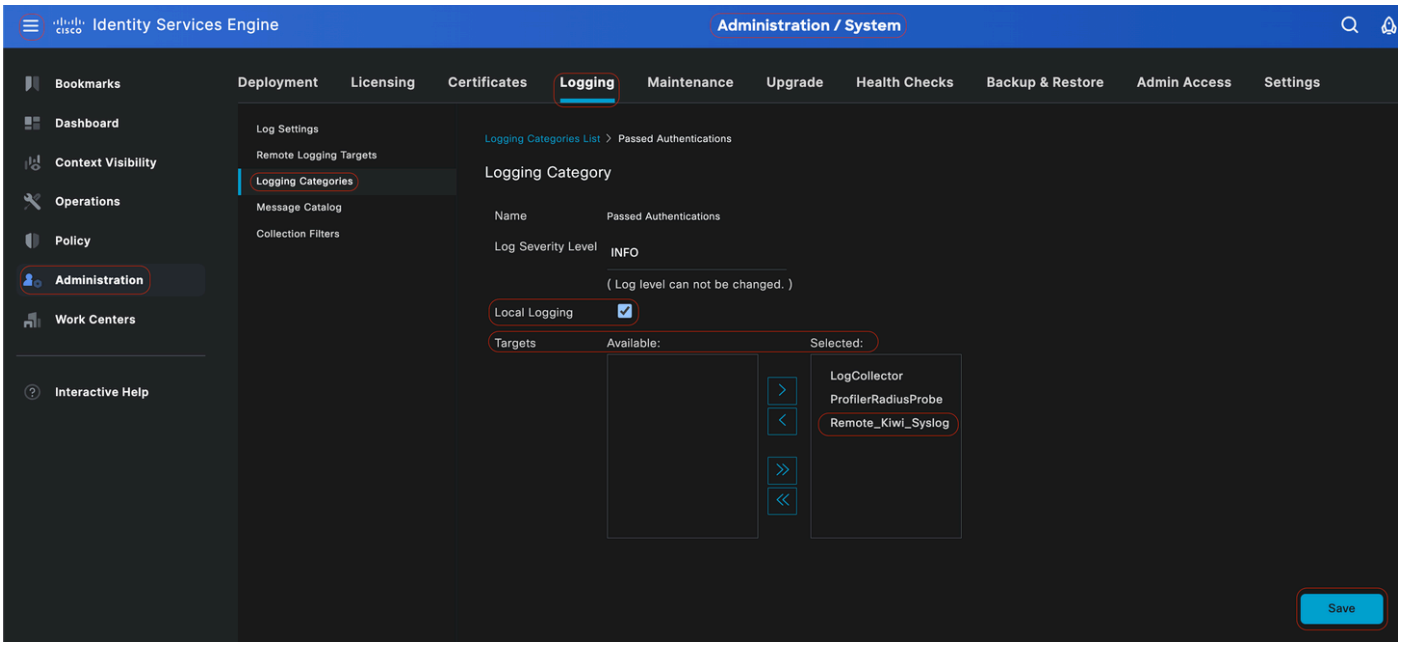
Etapa 2 - **Registro local: Esta caixa de seleção ativa a geração de registro local.** Isso significa que os logs gerados pelas PSNs também são salvos na PSN específica que gera o log. Recomendamos manter a configuração padrão

Etapa 3- Alvos: Esta área permite que você escolha os alvos para uma categoria de log transferindo os alvos entre as áreas Disponível e Selecionado usando os ícones de seta para a esquerda e direita.

A área Disponível contém os destinos de log existentes, local (predefinido) e externo (definido pelo usuário).

A área Selecionado, que está inicialmente vazia, exibe os destinos que foram escolhidos para a categoria.

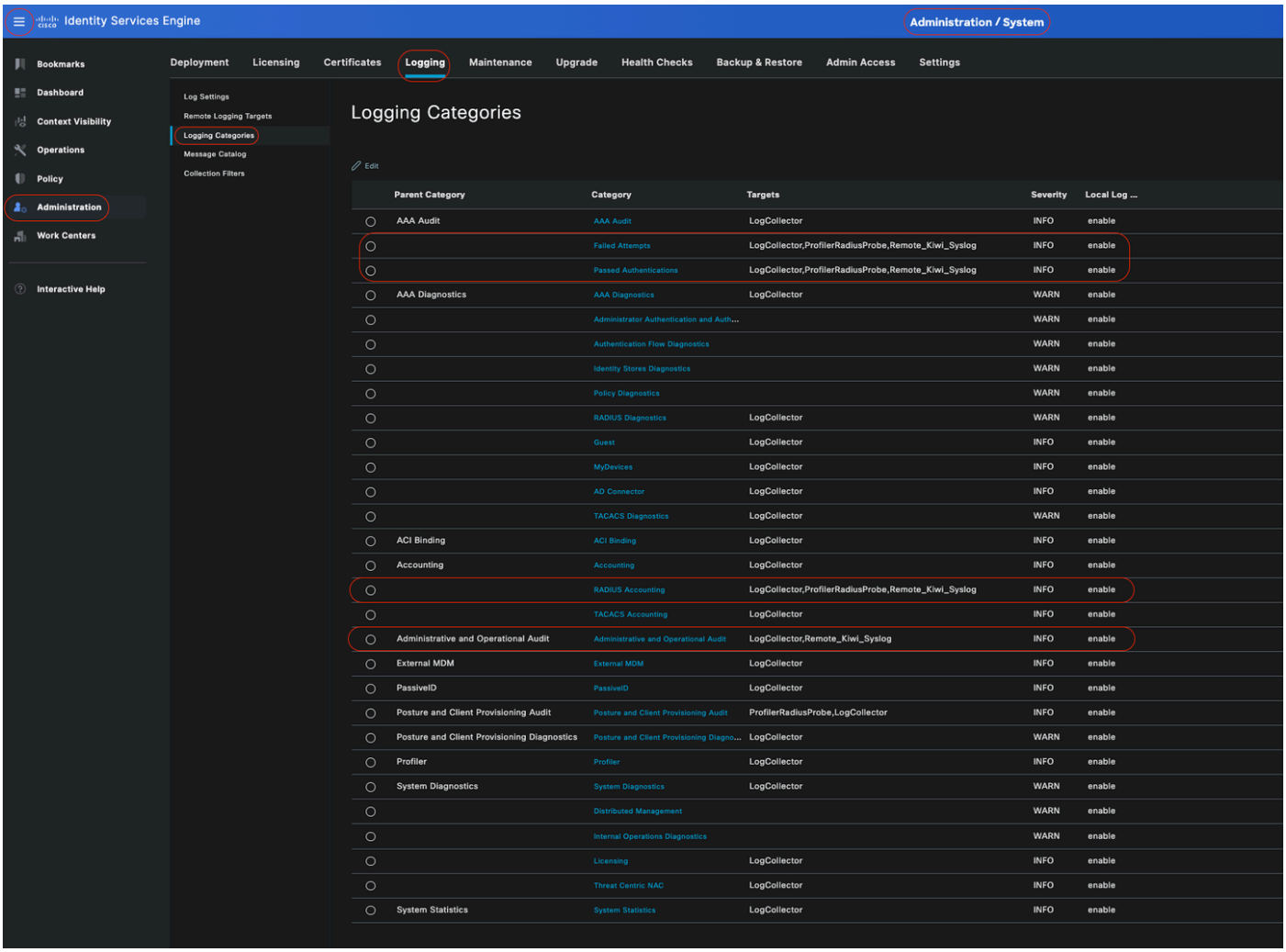
Etapa 4- Repita da etapa 1 à etapa 3 para adicionar o destino remoto em **Tentativas com falha e** categorias de relatório Radius.



Mapeando Alvos Remotos para Categorias pretendidas

Etapa 5- Verifique se o Destino remoto está sob as categorias necessárias.Você deve ser capaz de ver o destino remoto que acabou de adicionar.

Nesta captura de tela, você pode ver o destino remoto **Remote_Kiwi_Syslog** mapeado para as categorias necessárias.



Verificando categorias

Noções básicas sobre categorias

Uma mensagem é gerada quando ocorre um evento. Há diferentes tipos de mensagens de evento geradas de vários recursos, como kernel, e-mail, nível de usuário e assim por diante.

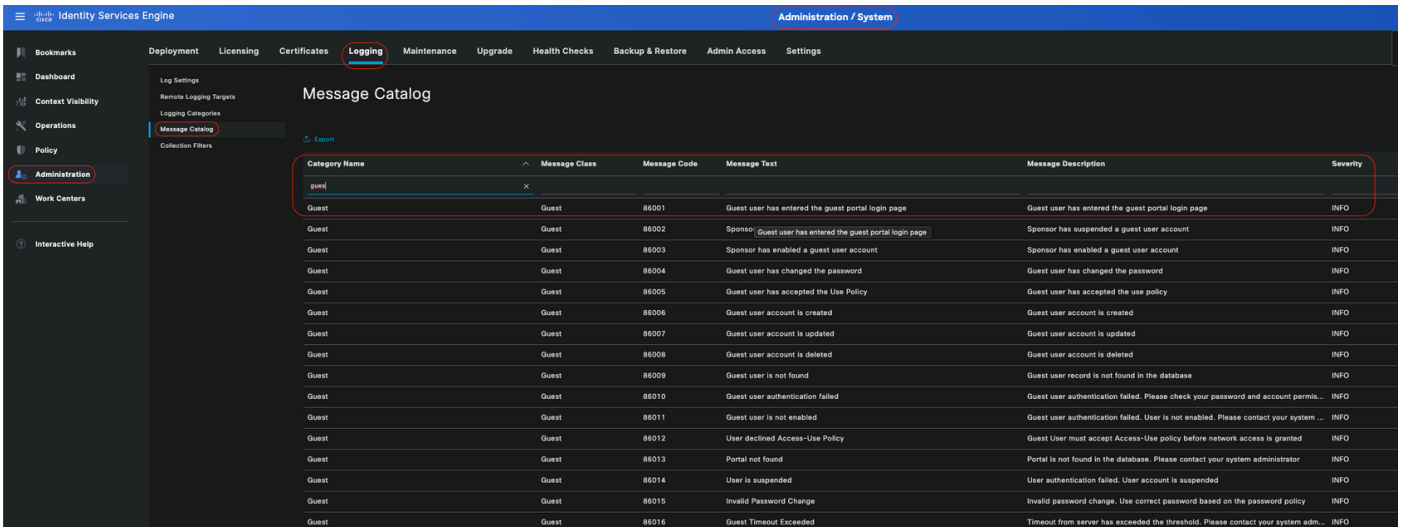
Esses erros são categorizados no Catálogo de mensagens e esses eventos também são organizados hierarquicamente em categorias.

Essas categorias têm categorias pai que contêm uma ou algumas categorias.

Categoria pai	Categoria
Auditoria AAA	Auditoria AAA Tentativas com Falha Autenticação Aprovada
Diagnóstico AAA	Diagnóstico AAA Autenticação e autorização do administrador

	Diagnóstico de fluxo de autenticação Diagnóstico do Repositório de Identidades Diagnóstico de política Diagnósticos Radius Convidado
Relatório	Relatório Contabilidade RADIUS
Auditoria administrativa e operacional	Auditoria administrativa e operacional
Auditoria de provisionamento de clientes e postura	Auditoria de provisionamento de clientes e postura
Diagnóstico de provisionamento de clientes e postura	Diagnóstico de provisionamento de clientes e postura
Profiler	Profiler
Diagnóstico do sistema	Diagnóstico do sistema Gerenciamento distribuído Diagnóstico de Operações Internas
Estatísticas do sistema	Estatísticas do sistema

Nesta captura de tela, você pode ver que **Guest** é uma classe de mensagem e categorizada como uma **categoria de convidado**. Esta categoria de convidado tem uma categoria pai chamada **Diagnóstico AAA**.



Catálogo de mensagens

Verificação e solução de problemas

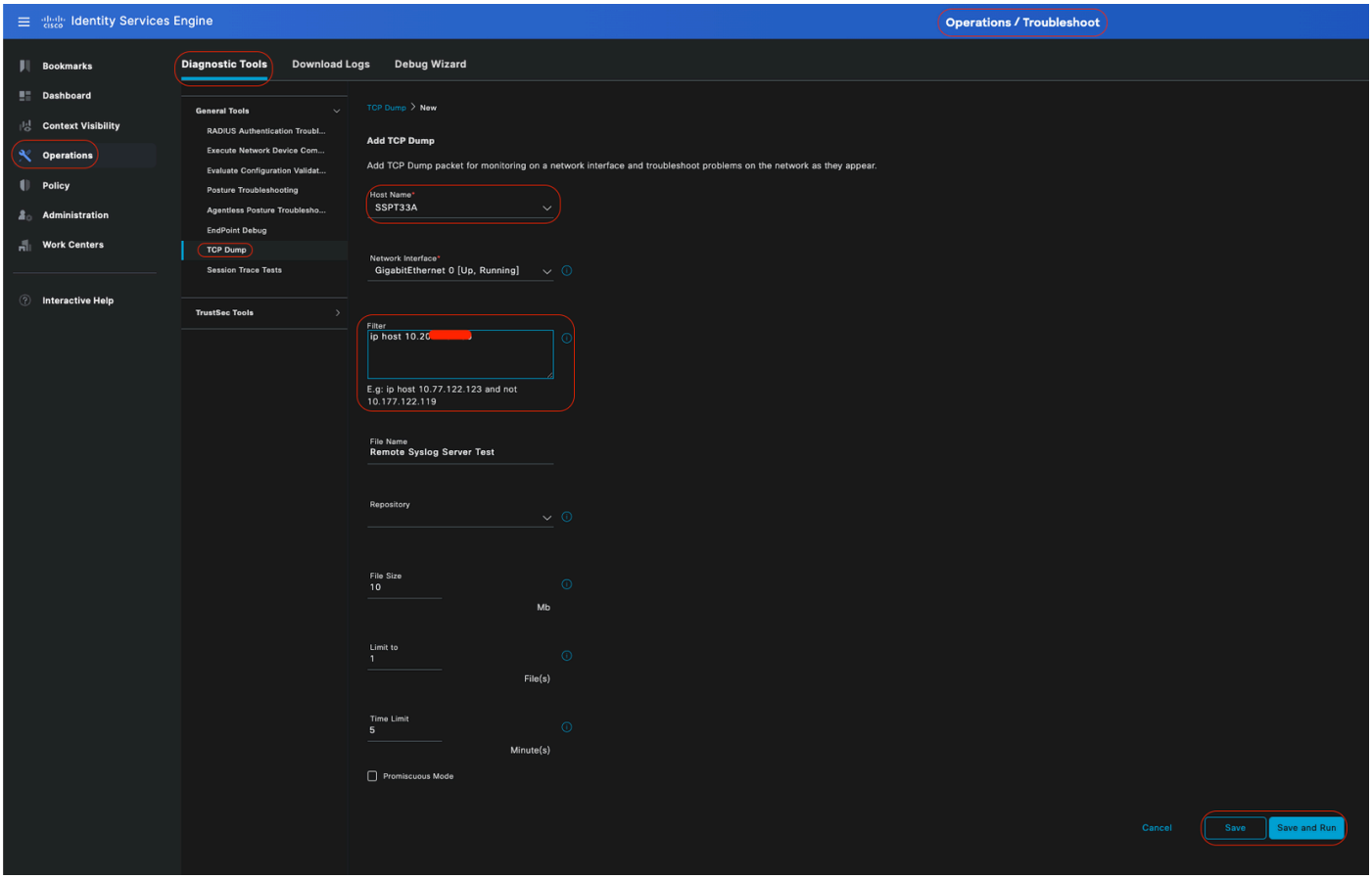
Fazer um despejo TCP em relação ao destino de registro remoto é a etapa mais rápida de solução de problemas e verificação para confirmar se os eventos de registro estão ou não sendo enviados.

A captura deve ser obtida da PSN que autentica o usuário, pois a PSN gerará mensagens de log e essas mensagens serão enviadas ao Destino Remoto

Na GUI do Cisco ISE, clique no ícone do menu ( ) e escolha **Operations**> Troubleshoot>TCP Dump> Clique em Adicionar.

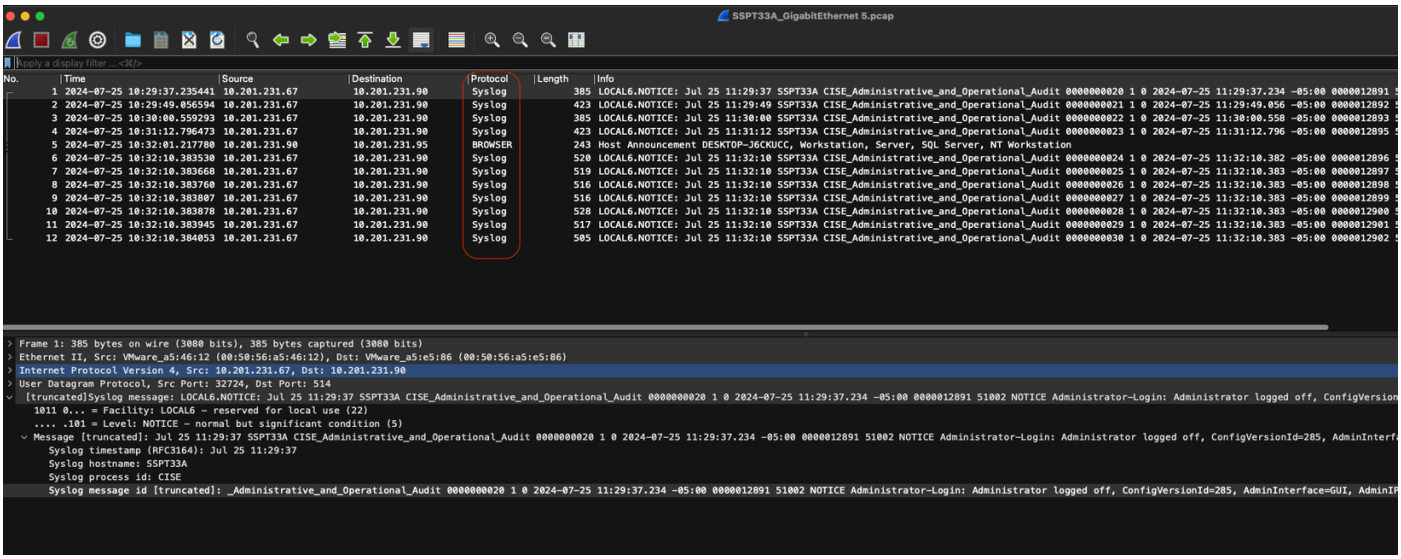
- Você deve filtrar o tráfego, adicionar o campo de filtro ip host <remote_target_IP_address>.

- Você deve capturar as autenticações de tratamento de PSN.



Despejo TCP

Nesta captura de tela, você pode ver como o ISE está enviando mensagens de Syslog para o administrador do ISE que registra o tráfego.



Tráfego de Syslog

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.