在ISE上配置外部系统日志服务器

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 配置远程日志记录目标（UDP系统日志）
- 示例
- 在Logging Categories下配置远程目标

了解类别

检验和故障排除

简介

本文档介绍如何在ISE上配置外部系统日志服务器。

先决条件

要求

Cisco 建议您了解以下主题：

- 身份服务引擎(ISE)。
- 系统日志服务器

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 身份服务引擎(ISE)3.3版本。
- Kiwi系统日志服务器v1.2.1.4

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

.

来自ISE的系统日志消息由日志收集器收集和存储。这些日志收集器分配给监控节点，因此MnT在

本地存储收集的日志。

要从外部收集日志，您需要配置外部系统日志服务器，这些服务器称为目标。日志分为各种预定义类别。

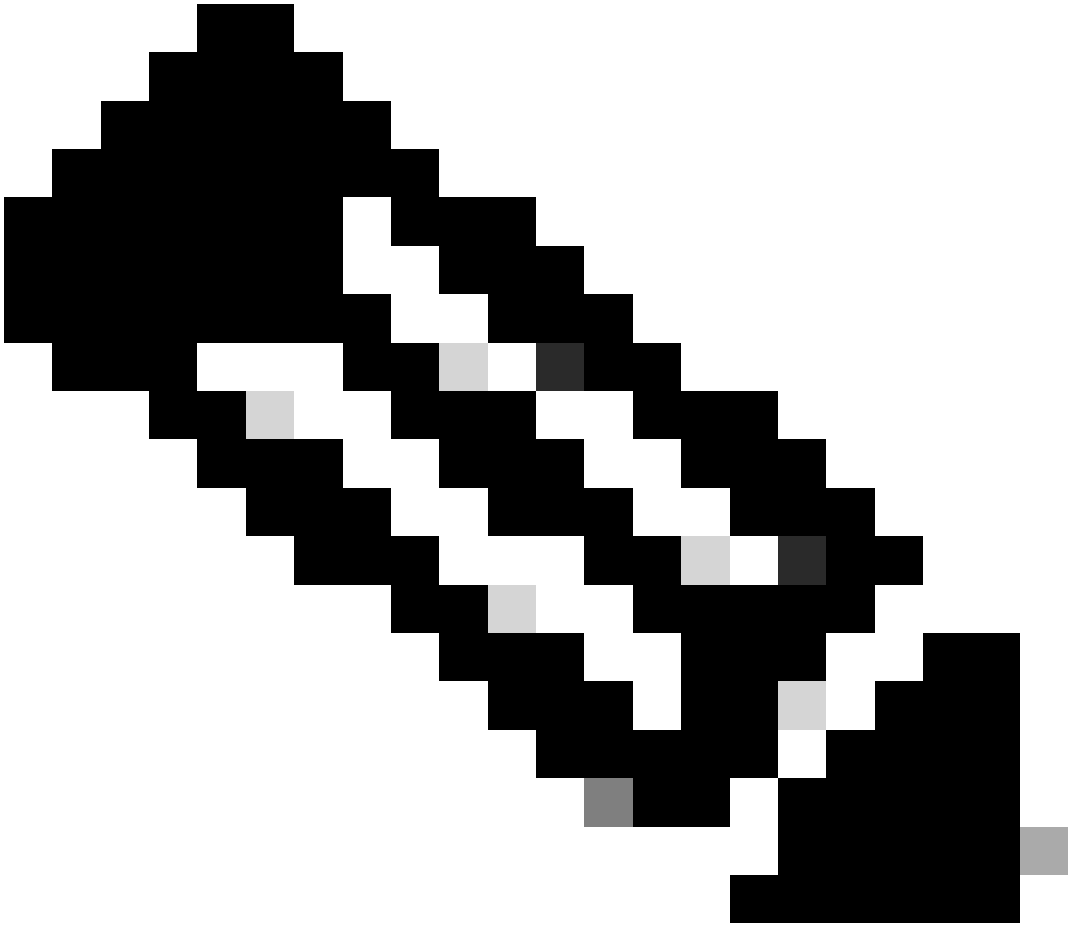
您可以通过编辑与其目标、严重性级别等相关的类别来自定义日志记录输出。

配置

您可以使用Web界面创建远程系统日志服务器目标，系统日志消息将发送到这些目标。根据系统日志协议标准将日志消息发送到远程系统日志服务器目标（请参阅RFC-3164）。

配置远程日志记录目标（UDP系统日志）

在Cisco ISE GUI中，点击菜单图标( )并选择Administration>System>Logging>Remote Logging Targets >Click Add。



注意：此配置示例基于以下屏幕截图：配置远程日志记录目标。

- 名称为Remote_Kiwi_Syslog，您可以在此处输入远程系统日志服务器的名称，此名称用于描述性目的。
- 目标类型为UDP Syslog，在此配置示例中，使用的是UDP Syslog;但是，您可以从目标类型下拉列表配置更多选项：

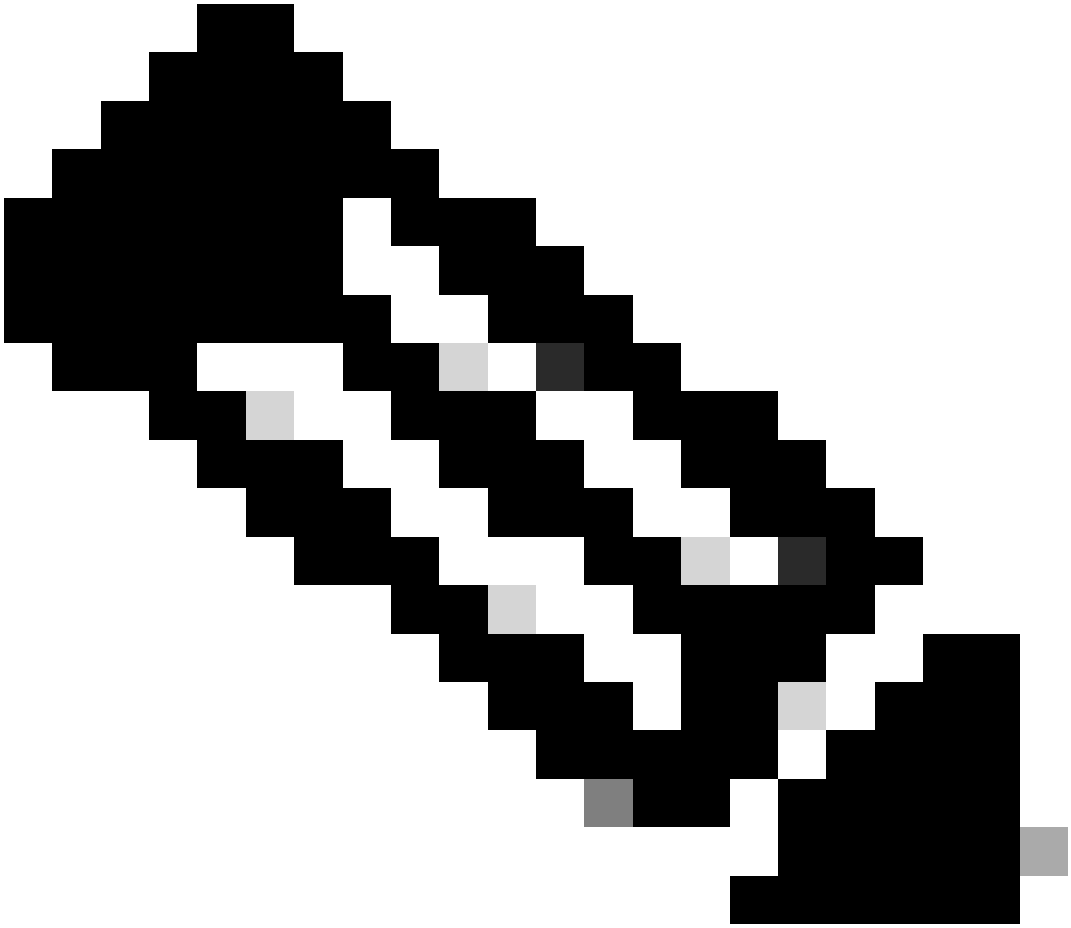
UDP系统日志：用于通过UDP发送系统日志消息，适用于轻量级和快速日志记录。

TCP系统日志：用于通过TCP发送系统日志消息，通过错误检查和重新传输功能提供可靠性。

安全系统日志：是指通过TCP使用TLS加密发送的系统日志消息，确保数据完整性和机密性。

- 状态为Enabled，您必须从Statuss下拉列表中选择Enabled。
- 说明（可选）您可以输入新目标的简要说明。
- Host / IP Address，此处输入存储日志的目标服务器的IP地址或主机名。Cisco ISE支持

IPv4和IPv6格式的日志记录。



注意：必须指出的是，如果要使用FQDN配置系统日志服务器，必须设置DNS缓存以避免对性能产生影响。如果没有DNS缓存，ISE会在每次必须将系统日志数据包发送到配置了FQDN的远程日志记录目标时查询DNS服务器。这会对ISE性能产生严重影响。

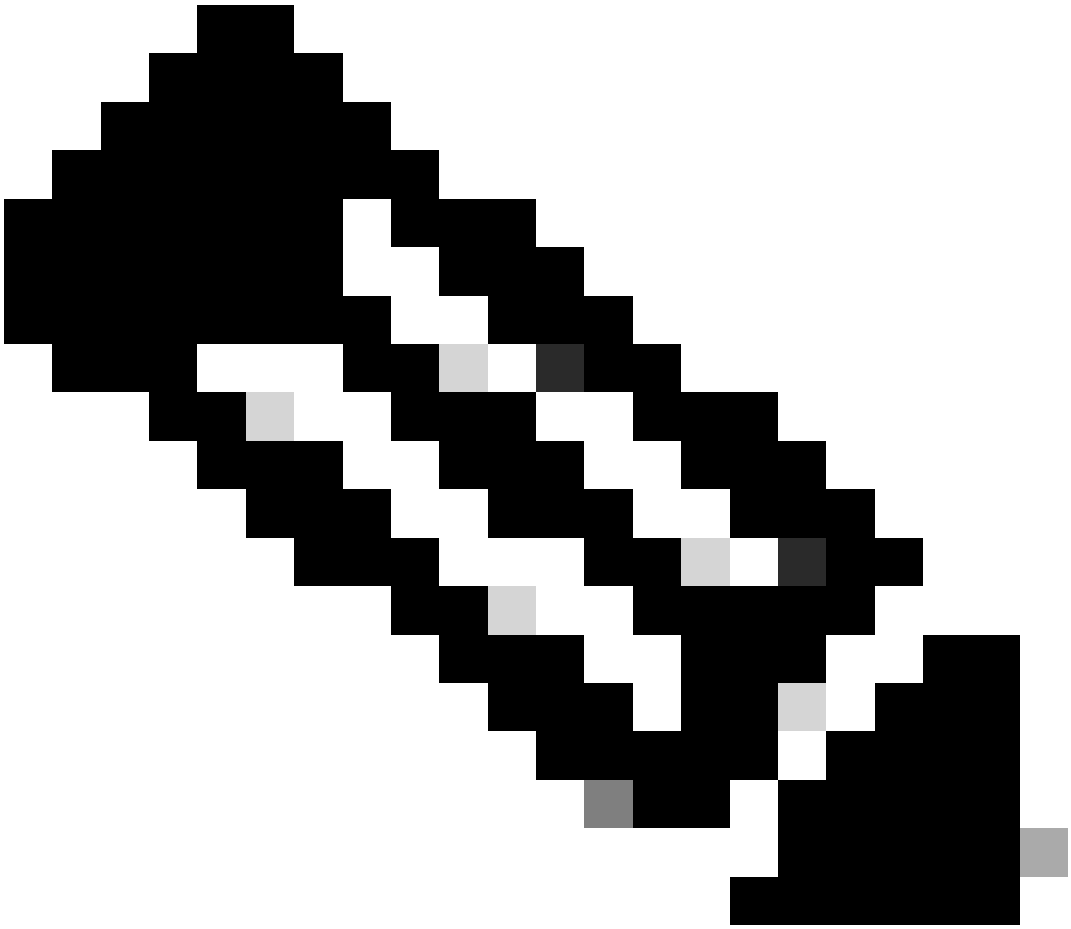
在部service cache enable署的所有PSN中使用命令可以克服以下问题：

示例

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

- 端口为514，在此配置示例中，Kiwi Syslog服务器正在侦听端口514，该端口是UDP系统日志消息的默认端口。但是，用户可以将此端口号更改为1到65535之间的任意值。请确保您的所需端口未被任何防火墙阻止。

- Facility Code as LOCAL6，您可以从下拉列表中选择必须用于日志记录的系统日志设备代码。有效选项为Local0到Local7。
- 最大长度为1024，您可以在此处输入远程日志目标消息的最大长度。默认情况下，ISE 3.3版本将最大长度设置为1024，值介于200到8192字节之间。

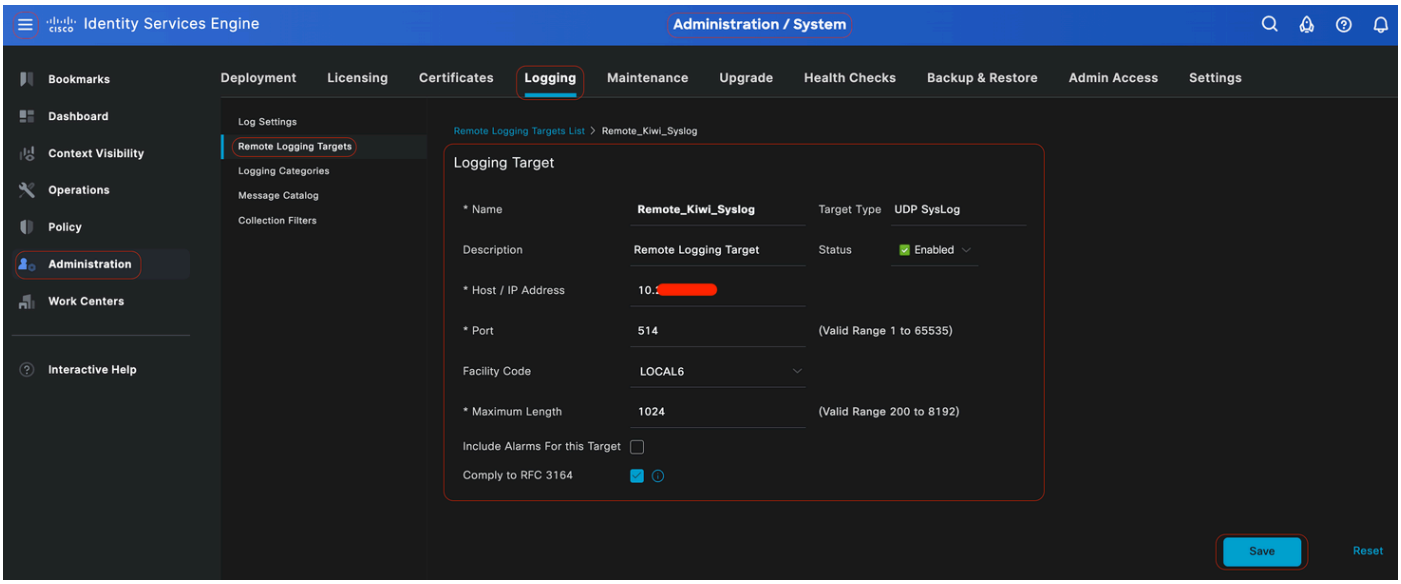


注意：为避免将截断的消息发送到远程目标，您可以将Maximum Length修改为8192。

- 包括此目标的警报，为使其简单，在此配置示例中，包括此目标的警报未选中；但是,选中此复选框时，警报消息也会发送到远程服务器。
- Compliance to RFC 3164已选中，当您选中此复选框时，分隔符(,;{ } \ \)在发送到远程服务器的系统日志消息中，即使使用反斜线(\)也不会转义。

- 配置完成后，单击Save。

- 保存后，系统将显示以下警告：您已选择创建与服务器的不安全(TCP/UDP)连接。是否确定要继续？请点击是。



配置远程目标

在Logging Categories下配置远程目标

思科ISE将可审核事件发送到系统日志目标。配置远程日志记录目标后，您需要将远程日志记录目标映射到预期类别以转发可审计事件。

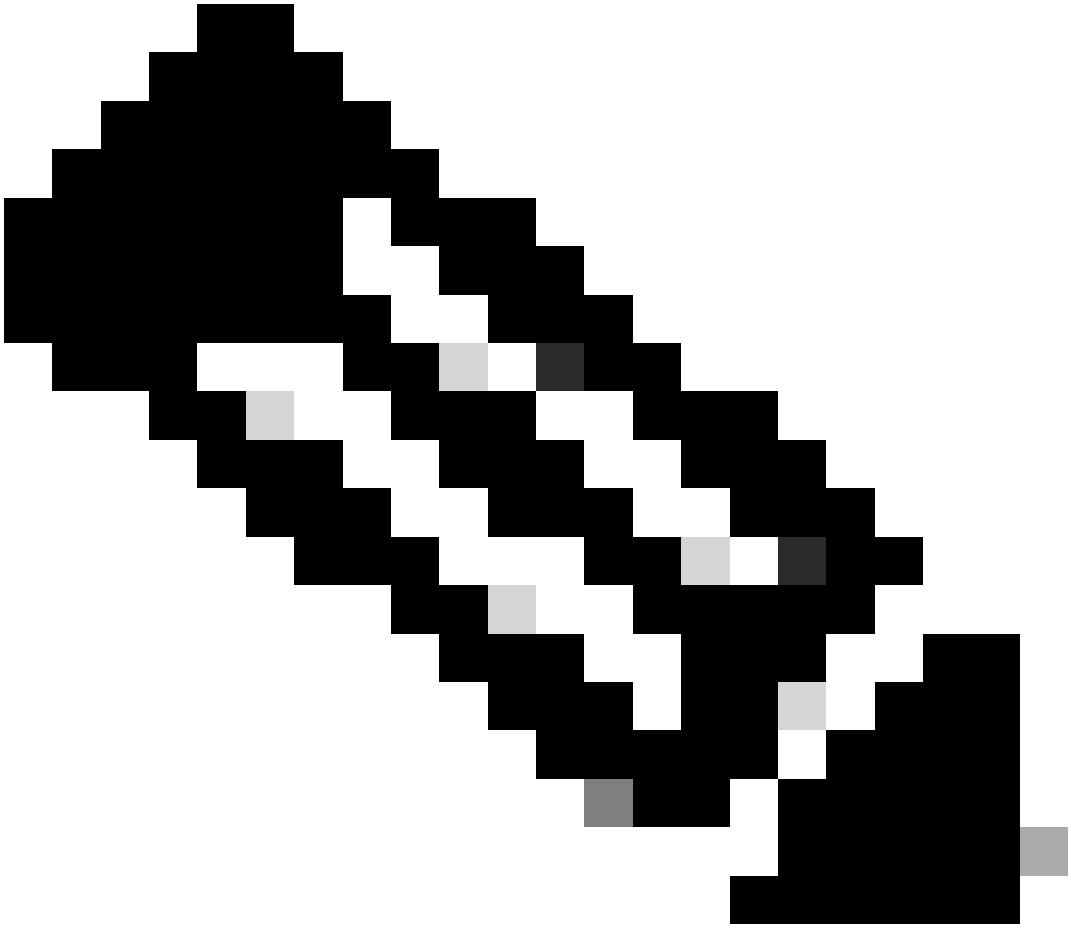
然后，可以将日志记录目标映射到这些日志记录类别中的每一个。这些日志类别中的事件日志仅从PSN节点生成，并且可以配置为根据在这些节点上启用的服务将相关日志发送到远程系统日志服务器：

- AAA审计
- AAA诊断
- 记账
- 外部MDM
- 被动Id
- 状态和客户端调配审核
- 状态和客户端调配诊断
- 分析器

这些日志类别中的事件日志是从部署中的所有节点生成的，可以配置为将相关日志发送到远程系统日志服务器：

- 行政和业务审计
- 系统诊断
- 系统统计信息

在此配置示例中，您将在四个日志记录类别下配置远程目标，这3个类别用于发送身份验证流量日志：通过ISE管理员日志记录流量的身份验证、失败尝试和Radius记帐，以及此类别：



注意：此配置示例基于以下屏幕截图：配置远程日志记录目标

在Cisco ISE GUI中，点击菜单图标(

)并选择Administration>System>Logging>Logging Categories，然后单击所需的类别(Passed Authentications、Failed Attempts和Radius Accounting)。

第1步 — 日志严重性级别：事件消息与严重性级别相关联，该严重性级别允许管理员过滤消息并对其进行优先排序。根据需要选择日志严重性级别。对于某些日志记录类别，此值是默认设置的，您无法对其进行编辑。对于某些日志记录类别，您可以从下拉列表中选择以下严重性级别之一：

- 致命:紧急级别。此级别表示您不能使用思科ISE，您必须立即采取必要操作。
- 错误：此级别表示出现严重错误情况。
- 警告:此级别表示正常但重要的情况。这是为许多日志记录类别设置的默认级别。
- 信息:此级别表示信息性消息。
- 调试:此级别表示诊断错误消息。

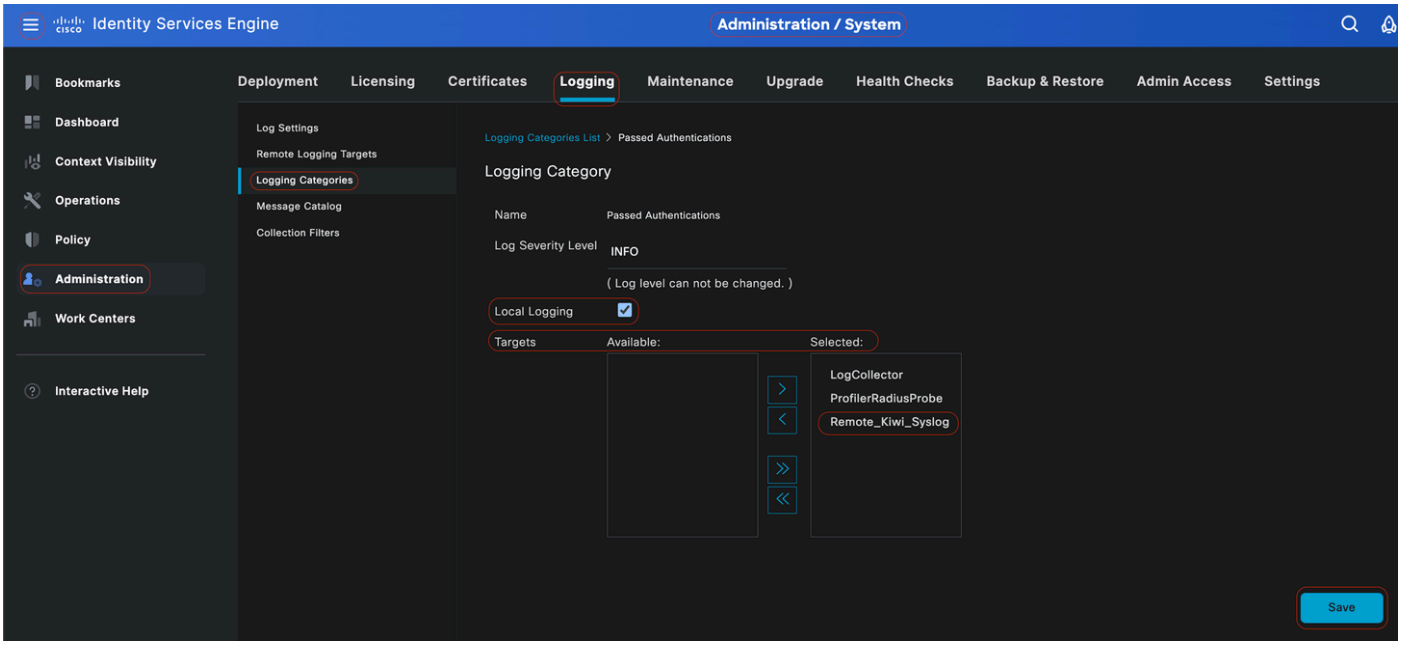
第2步 — 本地日志记录：此复选框启用本地日志生成。这意味着PSN生成的日志也保存在生成日志的特定PSN上。我们建议保留默认配置

第3步 — 目标：此区域允许您选择日志记录类别的目标，方法是使用左箭头和右箭头图标在Availableand和Selectedareas之间传输目标。

Availablearea包含现有的日志记录目标，包括本地（预定义）和外部（用户定义）。

Selectedarea（最初为空）随后显示为该类别选择的目标。

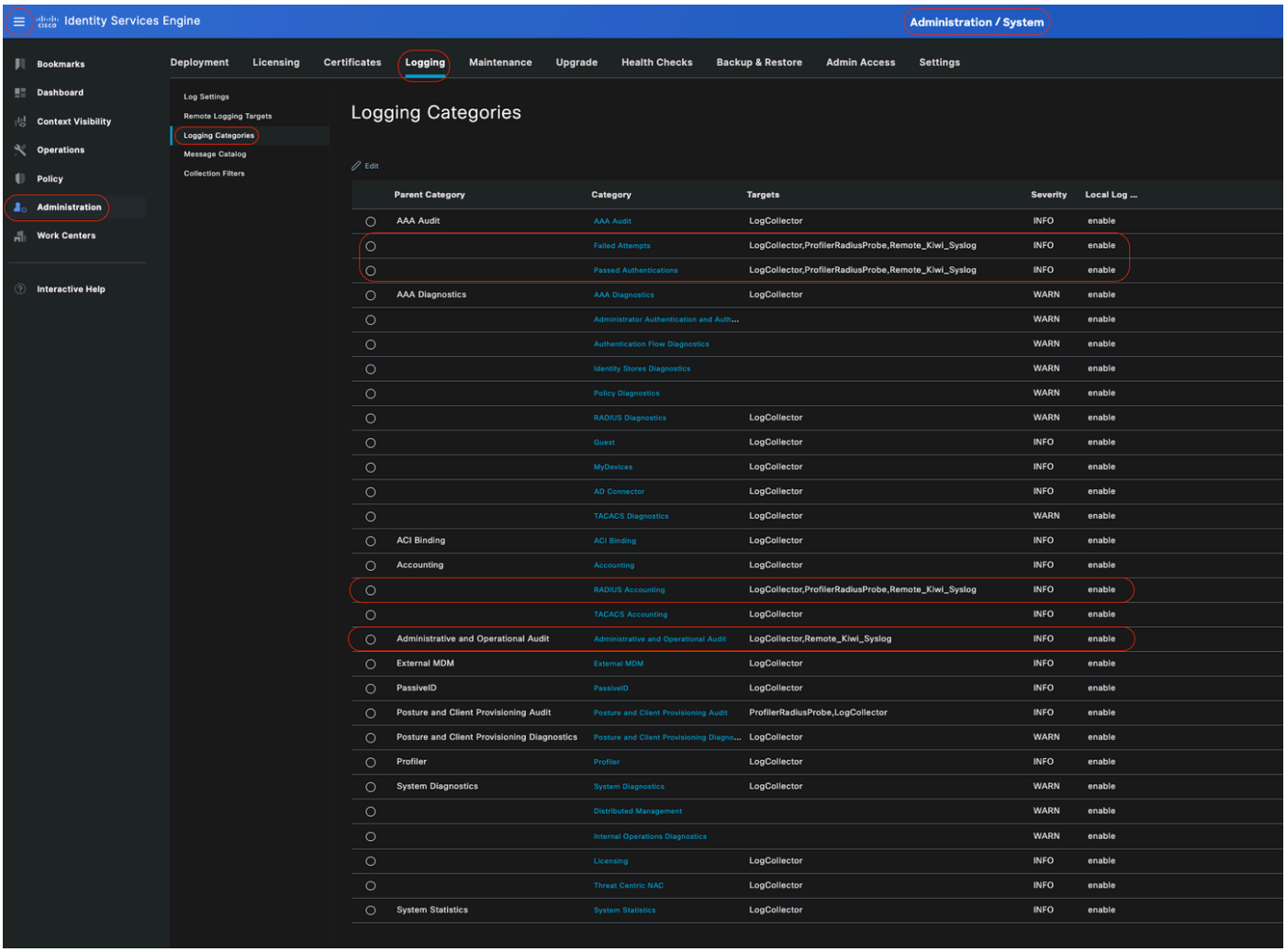
第4步 — 从第1步重复到第3步，在Failed Attempts和Radius Accounting类别下添加远程目标。



将远程目标映射到目标类别

第5步 — 验证远程目标是否位于所需的类别下。您必须能够看到刚刚添加的远程目标。

在此屏幕截图中，您可以看到映射至所需类别的远程目标Remote_Kiwi_Syslog。



检验类别

了解类别

事件发生时生成消息。从多个工具（例如内核、邮件、用户级别等）生成的事件消息类型多种多样。

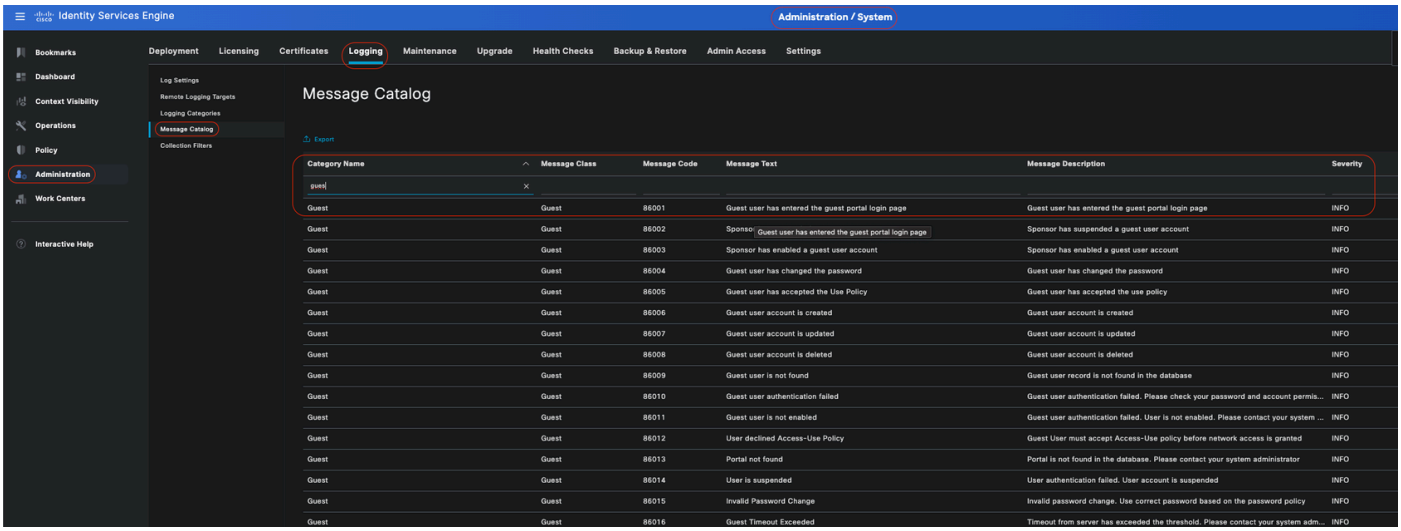
这些错误在邮件目录中进行了分类，这些事件也按照层次结构进行了分类。

这些类别的父类别包含一个或多个类别。

父类别	分类
AAA审计	AAA审计 失败的尝试 通过身份验证
AAA诊断	AAA诊断 管理员身份验证和授权

	身份验证流诊断 身份库诊断 策略诊断 Radius诊断 访客
记账	记账 RADIUS 记帐
行政和业务审计	行政和业务审计
状态和客户端调配审核	状态和客户端调配审核
状态和客户端调配诊断	状态和客户端调配诊断
分析器	分析器
系统诊断	系统诊断 分布式管理 内部运行诊断
系统统计信息	系统统计信息

在此屏幕截图中，您可以看到Guest是消息类并分类为Guest Category。此Guest Category具有名为AAA Diagnostics的父类别。



邮件目录

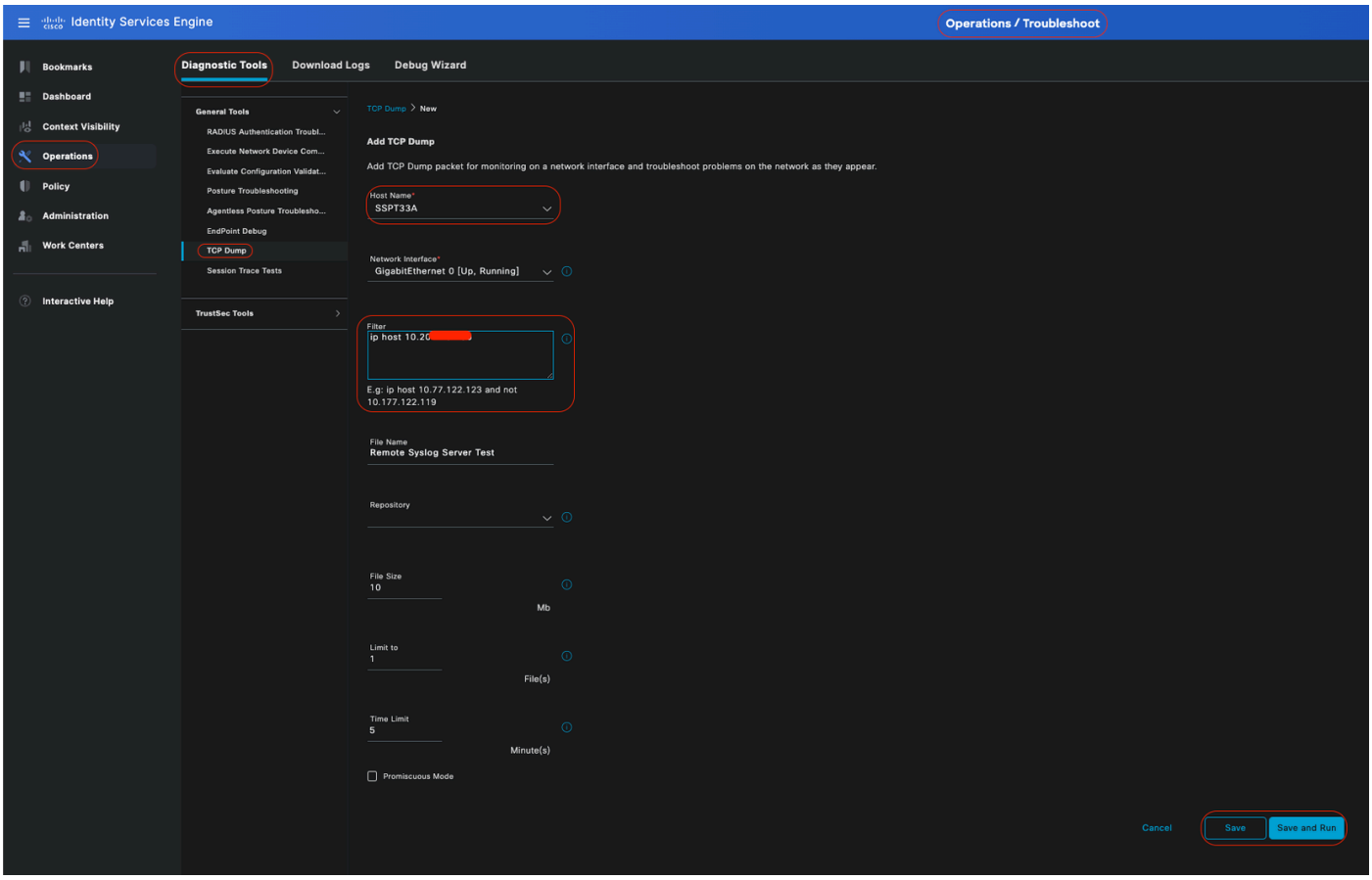
检验和故障排除

对远程日志记录目标执行TCP转储是确认是否发送日志事件的最快故障排除和验证步骤。

捕获必须来自对用户进行身份验证的PSN，因为PSN将生成日志消息，这些消息将发送到远程目标

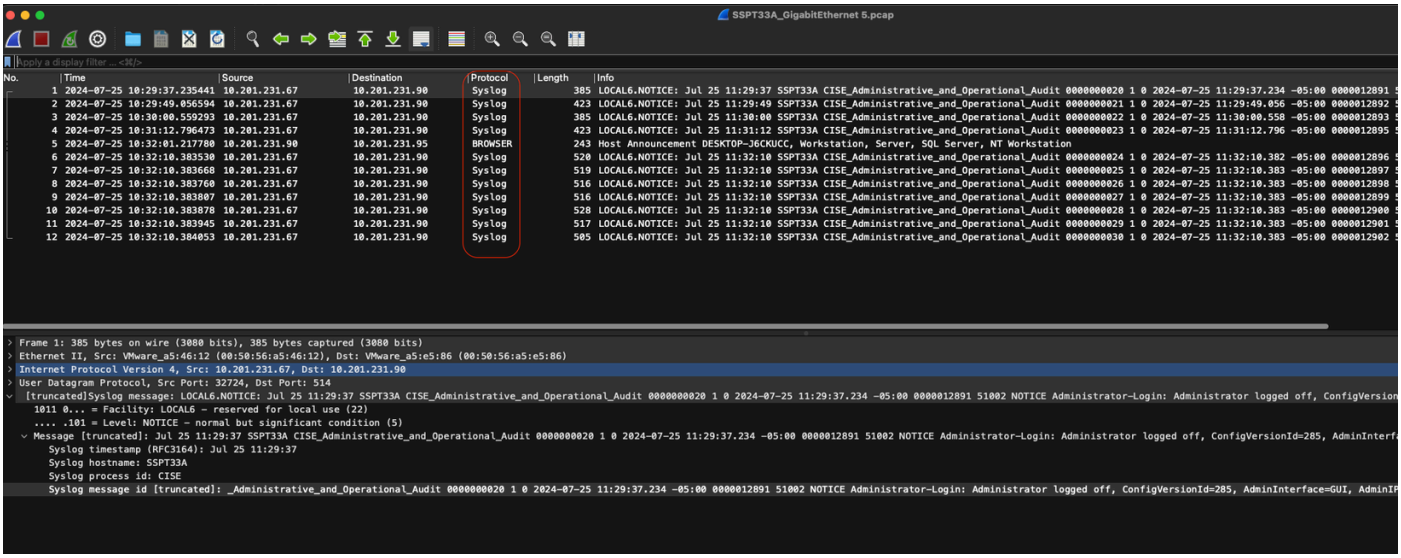
在Cisco ISE GUI中，点击菜单图标( )并选择Operations> Troubleshoot>TCP Dump>单击Add。

- 您必须过滤流量，添加ip host <remote_target_IP_addres> filter字段。
- 您必须从PSN捕获处理身份验证。



TCP转储

在此屏幕截图中，您可以看到ISE如何为ISE管理员日志记录流量发送系统日志消息。



系统日志流量

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。