在ISE上配置外部系统日志服务器

目录

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 Syslog Server 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

.

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

本地存储收集的日志。

要收集外部日志，您需要配置外部系统日志服务器，这些服务器称为目标。日志可分为各种预定义类别。

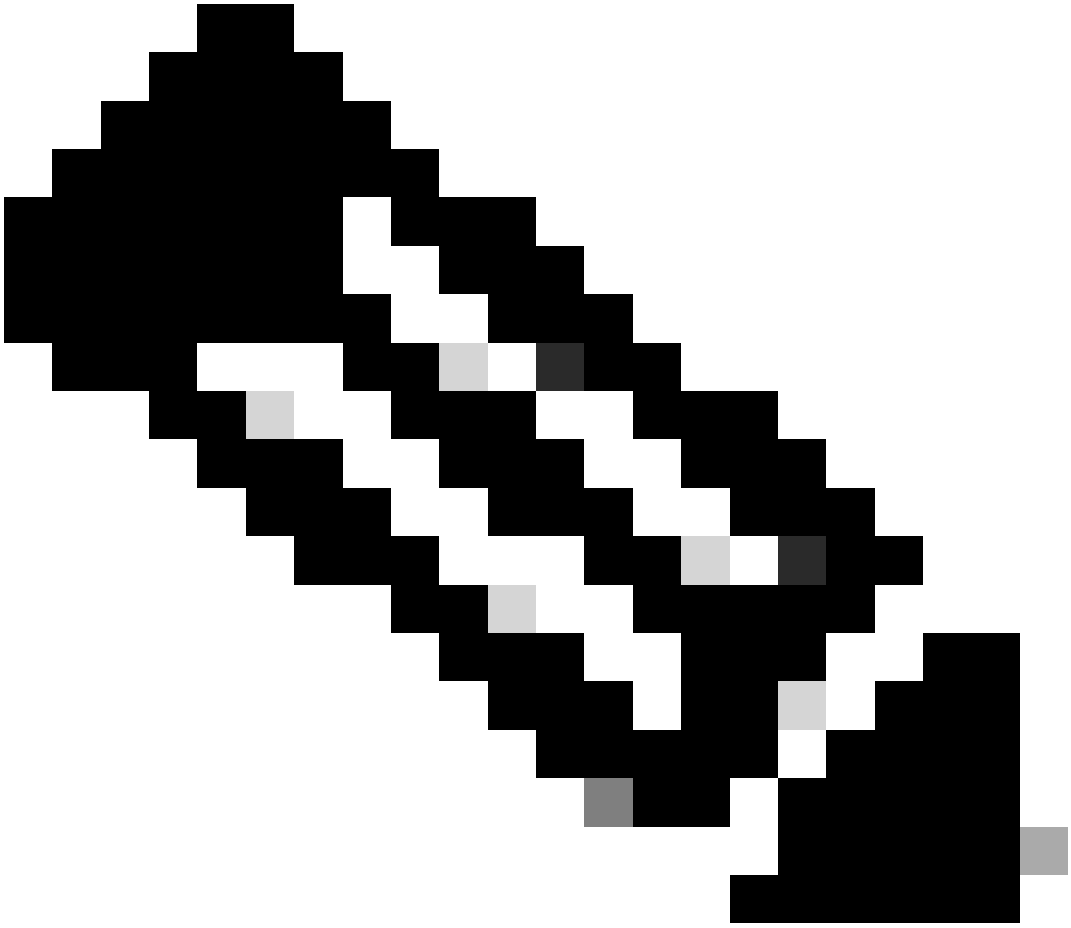
您可以通过编辑与其目标、严重性级别等相关的类别来自定义日志记录输出。

配置

可以使用Web界面创建系统日志消息发送到的远程系统日志服务器目标。日志消息根据系统日志协议标准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 Syslog)

在思科ISE GUI中，点击Menuicon ( )并选择Administration>System>Logging>Remote Logging Targets >点击Add。



注意：此配置示例基于名为“配置远程日志记录目标”的屏幕快照。

- 名称为Remote_Kiwi_Syslog，您可以在此处输入远程Syslog服务器的名称，此名称用于说明目的。
- 目标类型为UDP Syslog，在此配置示例中，使用了UDP Syslog；但是，您可以从Target Type下拉列表配置更多选项：

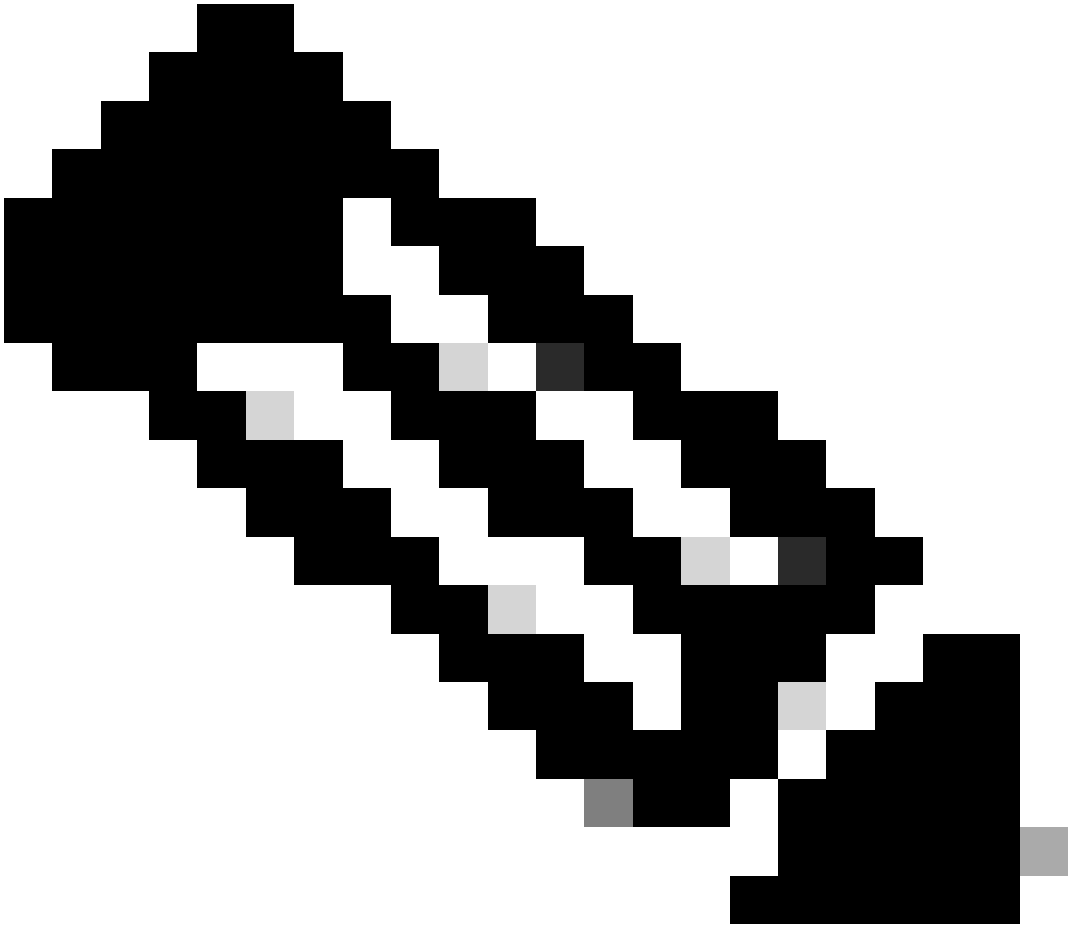
UDP系统日志：用于通过UDP发送系统日志消息，适用于轻量级和快速日志记录。

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

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

- 状态为已启用，必须从状态下拉列表中选择已启用。
- 说明，（可选）您可以输入新目标的简要说明。
- Host / IP Address，在这里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，则必须设置DNS缓存以避免对性能产生影响。如果没有DNS缓存，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，ISE都会查询DNS服务器。这会对ISE性能产生严重影响。

在部署的所有PSN中使用service cache enable命令可克服此问题：

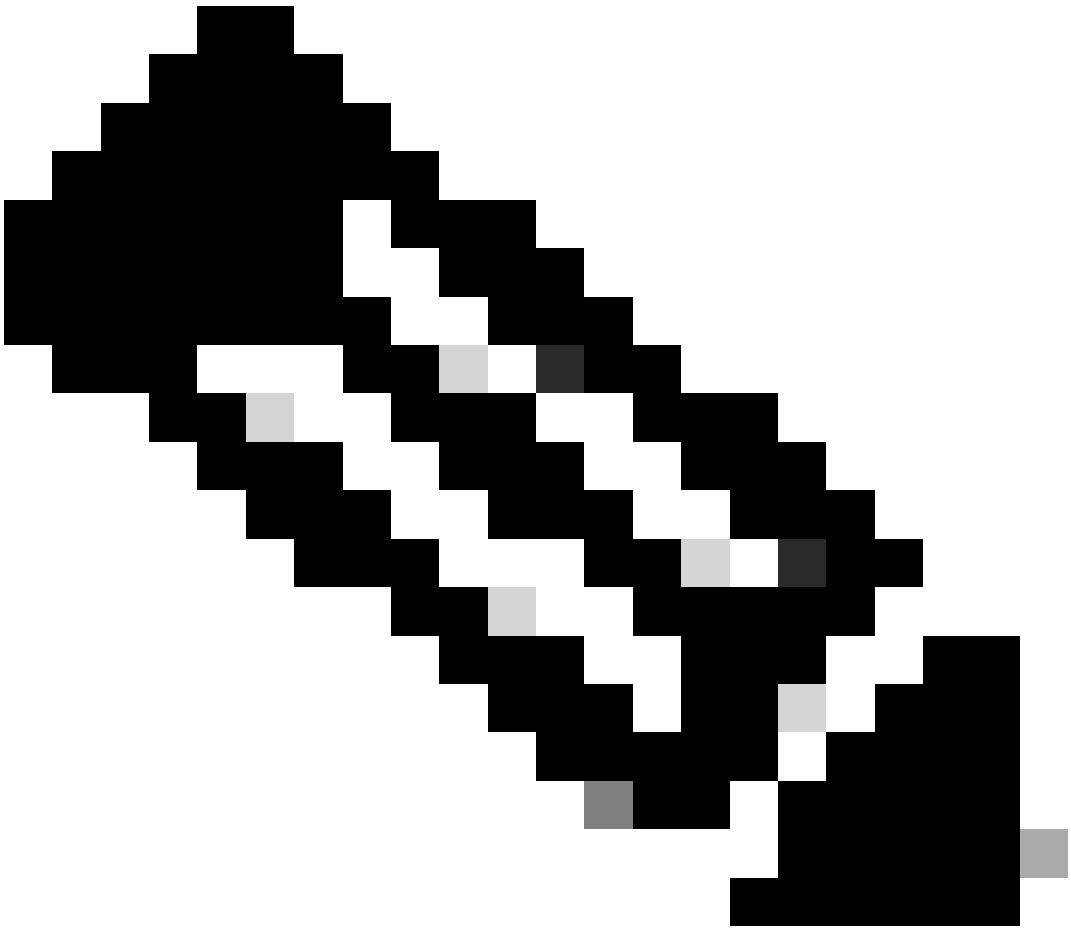
示例

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

- 端口作为**514**，在此配置示例中，Kiwi Syslog服务器在侦听端口**514**，该端口是UDP syslog消息的默认端口。 但是，用户可以将此端口号更改为1到65535之间的任何值。请确保所需的端口未被任何防火墙阻止。

- **Facility Code** 作为**LOCAL6**，您可以从下拉列表中选择必须用于日志记录的Syslog设备代码。有效选项为Local0到Local7。

- **Maximum Length**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，最大长度设置为**1024** ISE 3.3版本，值介于200到1024字节之间。



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

- **Include Alarms For This Target**（为了使其简单），在此配置示例中，未选中**Include Alarms For this Target**；但是，选中此复选框时，也会将警报消息发送到远程服务器。

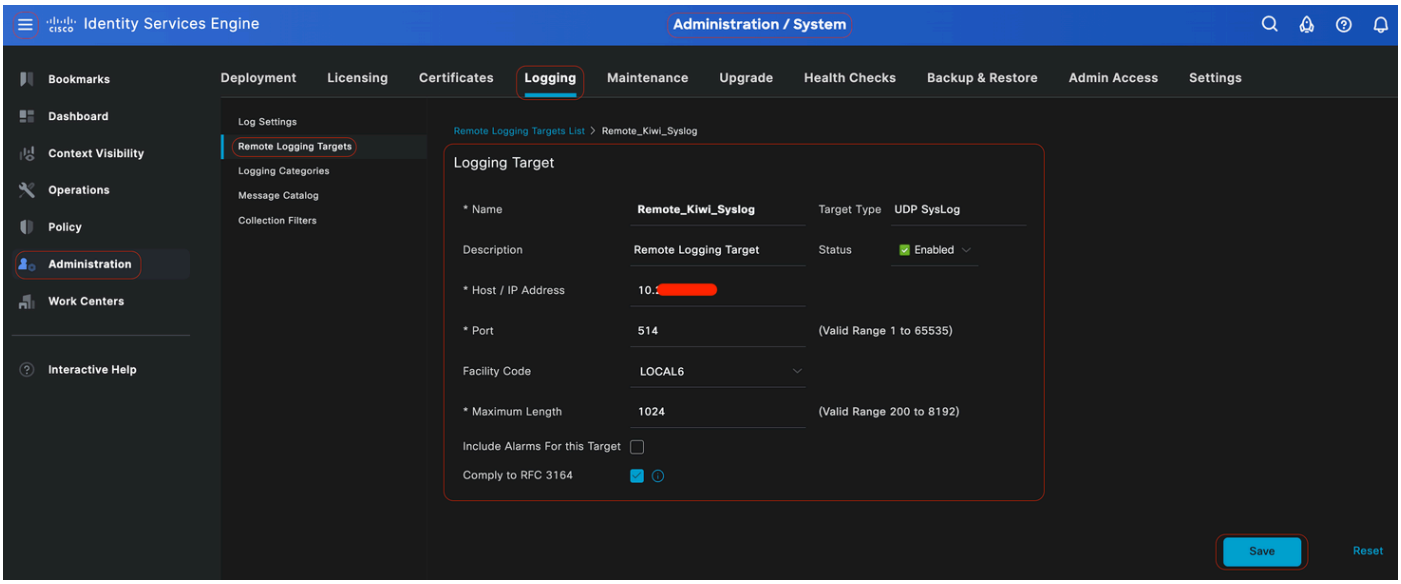
- **Compliance to RFC 3164**已选中，当您选中此复选框时，即使使用反斜线(\)，也不会转义发送到远程服务器的系统日志消息中的定界符(，；{}\\\)。

-

完成配置后，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？，请单击**Yes**。



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所需的类别以转发可审核的事件。

然后，日志记录目标可以映射到这些日志记录类别中的每一项。 这些日志类别中的事件日志只能从PSN节点生成，并且可以根据这些节点上启用的服务，配置为将相关日志发送到远程系统日志服务器：

-

AAA审核

-

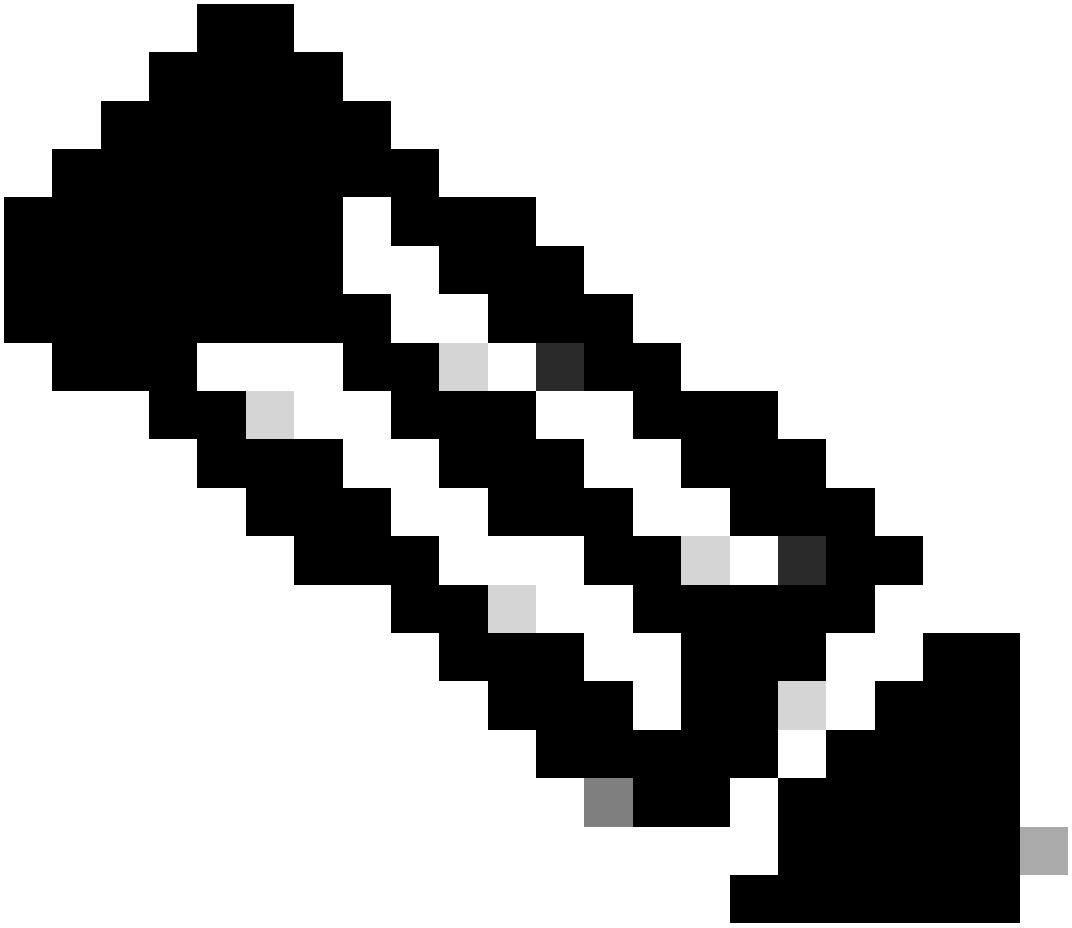
AAA诊断

- 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，这三个类别将发送身份验证流量日志：**Passed Authentications**、**Failed Attempts**和**Radius Accounting**，以及该类别用于ISE管理员日志记录流量：



注意：**此配置示例基于名**为“配置远程日志记录目标”的屏幕快照

在思科ISE GUI中，点击Menuicon (

)并选择**Administration>System>Logging>Logging Categories，**然后点击所需类别**(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，允许管理员过滤消息并设置其优先级。 根据需要选择日志严重性级别。 对于某些日志记录类别，该值默认设置，您无法编辑它。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：

- **FATAL**：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的操作。
- **ERROR**：此级别指示严重错误情况。
- **WARN**：此级别指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。
- **INFO**：此级别表示参考消息。

- **DEBUG**：此级别指示诊断漏洞消息。

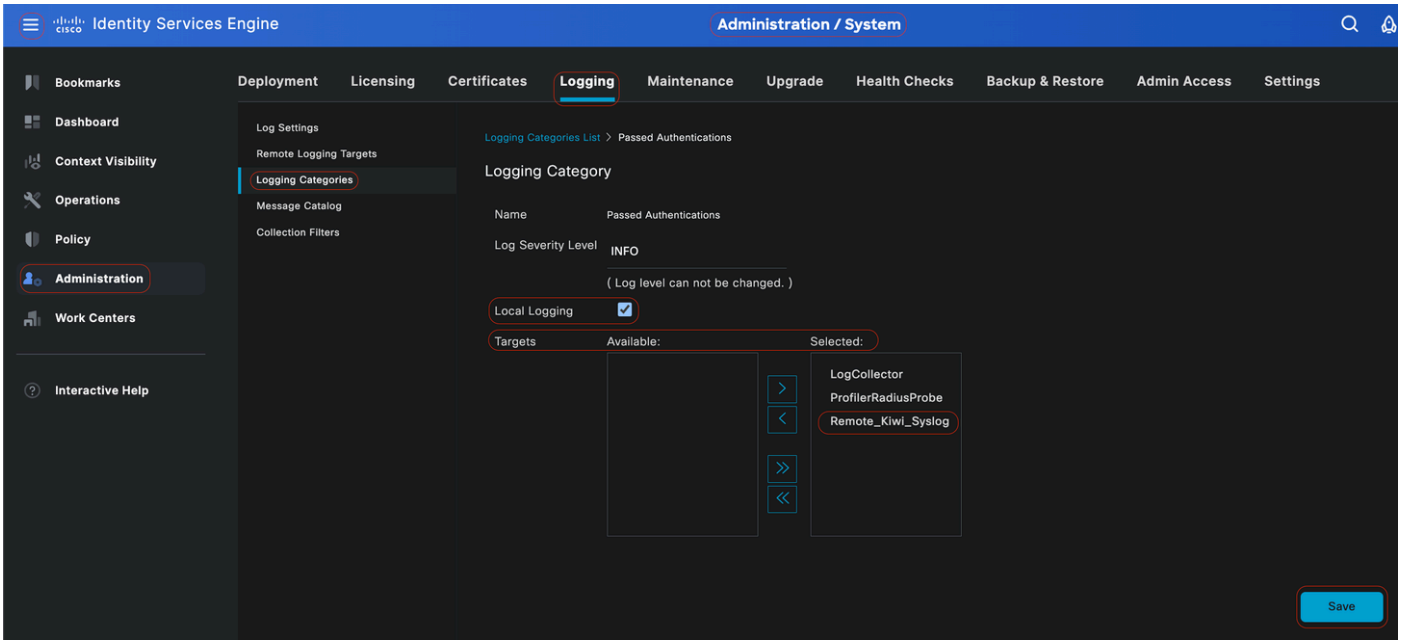
第2步-本地日志记录：此复选框启用本地日志生成。这意味着PSN生成的日志也保存在生成日志的特定PSN上。我们建议保留默认配置

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，本地（预定义）和外部（用户定义）。

Selectedarea最初为空，然后显示为类别选定的目标。

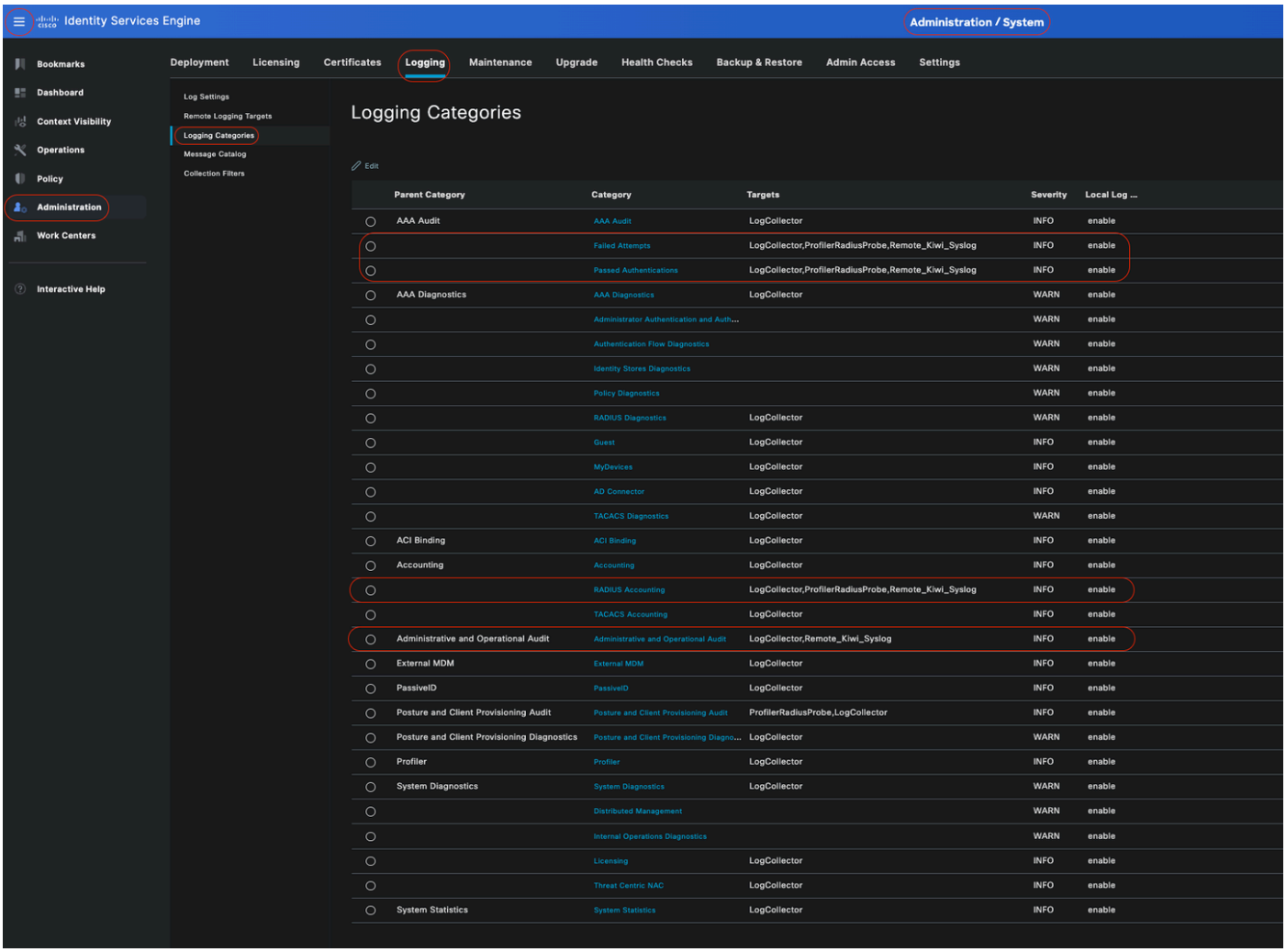
第4步-重复第1步到第3步，在Failed Attempts and Radius Accounting类别下添加远程目标。



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，您可以看到远程目标**Remote_Kiwi_Syslog**映射到所需的类别。



检验类别

了解类别

事件发生时生成消息。从多个工具（如内核、邮件、用户级别等）生成的事件消息有不同类型的生成。

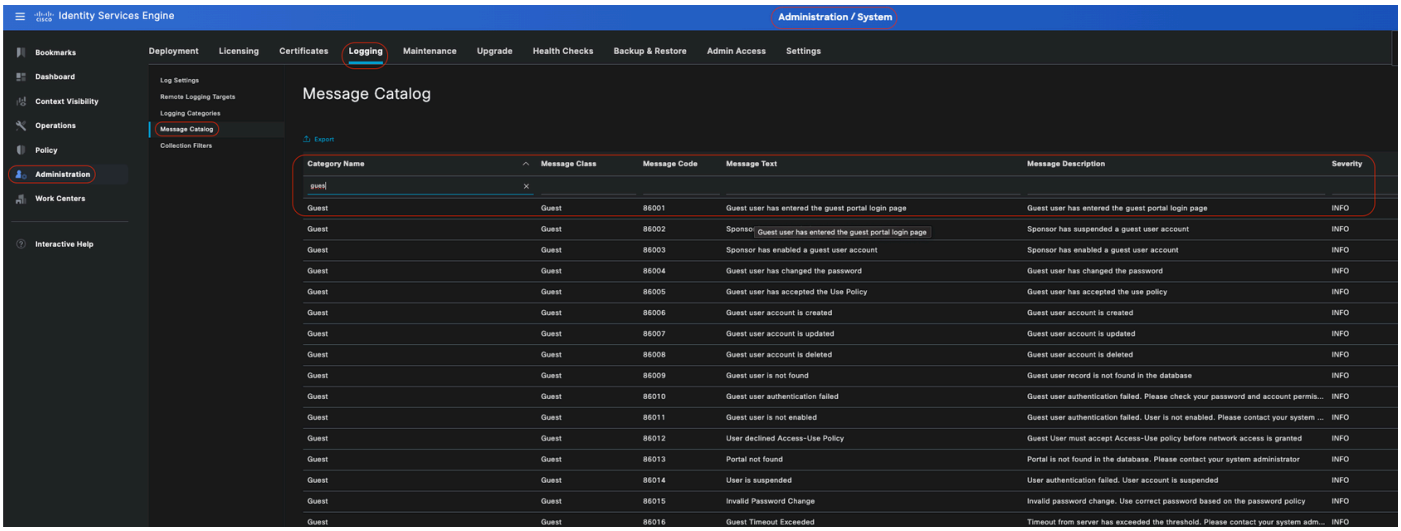
这些错误在消息目录中进行分类，这些事件也按层次进行分类。

这些类别的Parent Categories包含一个或多个类别。

父类别	分类
AAA审核	AAA审核 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，您可以看到访客是消息类并分类为访客类别。 此访客类别有一个称为**AAA**诊断的父类别。



邮件目录

检验和故障排除

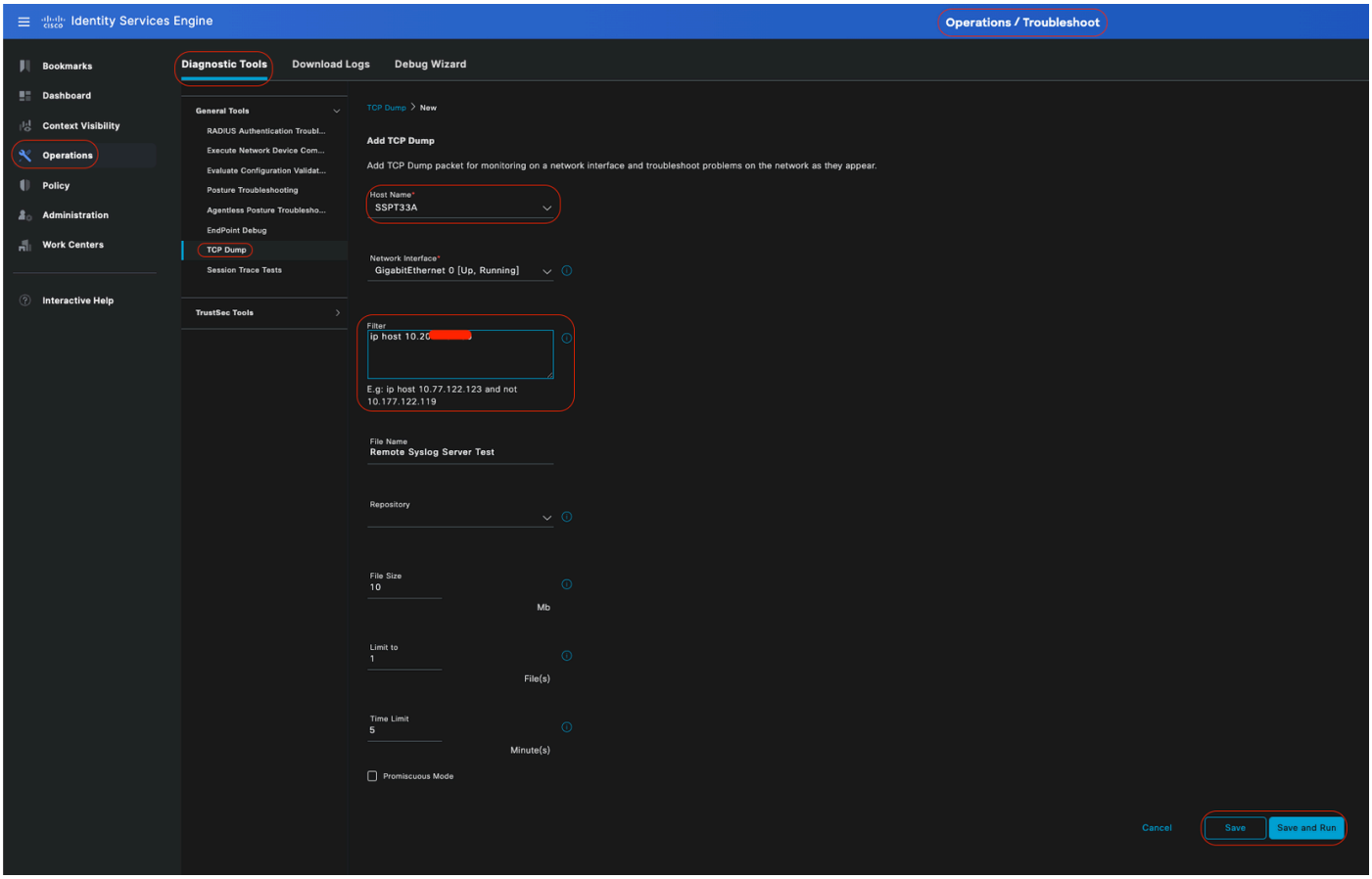
对远程日志记录目标执行TCP转储是确认是否发送日志事件的最快故障排除和验证步骤。

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

在思科ISE GUI中，点击Menuicon ( )并选择**Operations**> **Troubleshoot**> **TCP Dump**>点击**Add**。

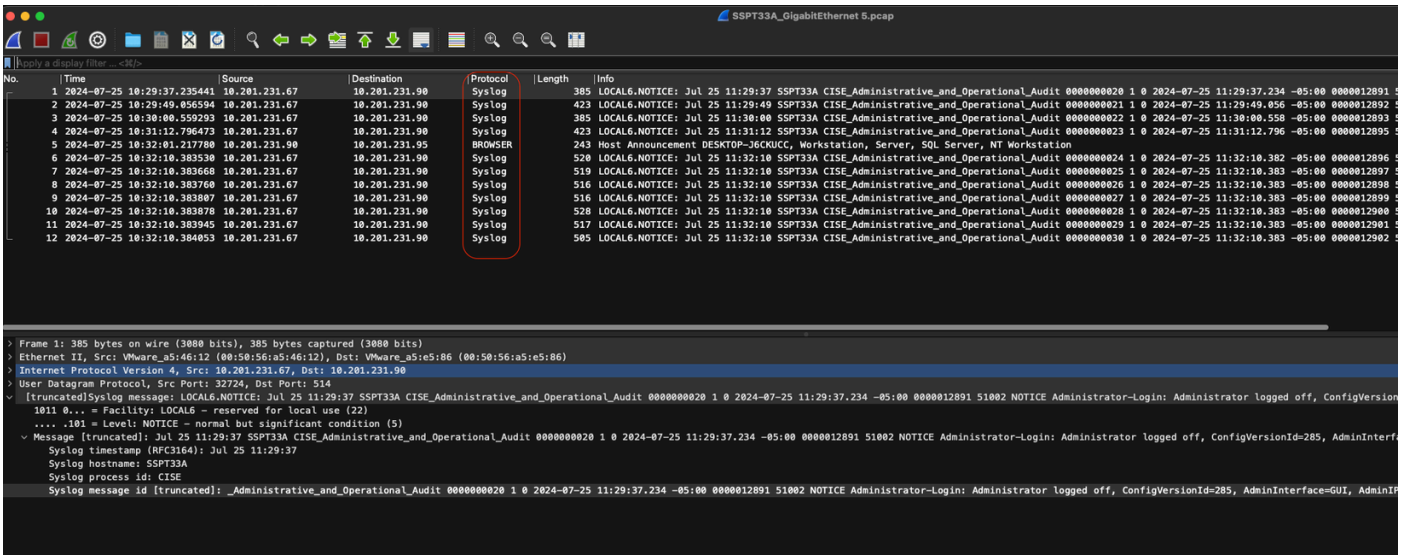
- 您必须过滤流量，添加ip host <remote_target_IP_addres> filter字段。

- 您必须从PSN处理身份验证中获取捕获。



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。


SSPT33A_GigabitEthernet 5.pcap
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
1 2024-07-25 10:29:37.235441 10.201.231.67 10.201.231.90 Syslog 385 LOCAL6.NOTICE: Jul 25 11:29:37 SSPT33A CISE_Administrative_and_Operational_Audit 0000000020 1 0 2024-07-25 11:29:37.234 -05:00 0000012891
2 2024-07-25 10:29:49.056594 10.201.231.67 10.201.231.90 Syslog 423 LOCAL6.NOTICE: Jul 25 11:29:49 SSPT33A CISE_Administrative_and_Operational_Audit 0000000021 1 0 2024-07-25 11:29:49.056 -05:00 0000012892
3 2024-07-25 10:30:00.559293 10.201.231.67 10.201.231.90 Syslog 385 LOCAL6.NOTICE: Jul 25 11:30:00 SSPT33A CISE_Administrative_and_Operational_Audit 0000000022 1 0 2024-07-25 11:30:00.558 -05:00 0000012893
4 2024-07-25 10:31:12.796473 10.201.231.67 10.201.231.90 Syslog 423 LOCAL6.NOTICE: Jul 25 11:31:12 SSPT33A CISE_Administrative_and_Operational_Audit 0000000023 1 0 2024-07-25 11:31:12.796 -05:00 0000012895
5 2024-07-25 10:32:01.217780 10.201.231.90 10.201.231.95 BROWSER 243 Host Announcement DESKTOP-J6CKUCC, Workstation, Server, SQL Server, NT Workstation
6 2024-07-25 10:32:10.383530 10.201.231.67 10.201.231.90 Syslog 520 LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000024 1 0 2024-07-25 11:32:10.382 -05:00 0000012896
7 2024-07-25 10:32:10.383668 10.201.231.67 10.201.231.90 Syslog 519 LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000025 1 0 2024-07-25 11:32:10.383 -05:00 0000012897
8 2024-07-25 10:32:10.383760 10.201.231.67 10.201.231.90 Syslog 516 LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000026 1 0 2024-07-25 11:32:10.383 -05:00 0000012898
9 2024-07-25 10:32:10.383807 10.201.231.67 10.201.231.90 Syslog 516 LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000027 1 0 2024-07-25 11:32:10.383 -05:00 0000012899
10 2024-07-25 10:32:10.383878 10.201.231.67 10.201.231.90 Syslog 528 LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000028 1 0 2024-07-25 11:32:10.383 -05:00 0000012900
11 2024-07-25 10:32:10.383945 10.201.231.67 10.201.231.90 Syslog 517 LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000029 1 0 2024-07-25 11:32:10.383 -05:00 0000012901
12 2024-07-25 10:32:10.384053 10.201.231.67 10.201.231.90 Syslog 505 LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000030 1 0 2024-07-25 11:32:10.383 -05:00 0000012902
Frame 1: 385 bytes on wire (3080 bits), 385 bytes captured (3080 bits)
Ethernet II, Src: VMware_a5:46:12 (00:50:56:a5:46:12), Dst: VMware_a5:e5:86 (00:50:56:a5:e5:86)
Internet Protocol Version 4, Src: 10.201.231.67, Dst: 10.201.231.90
User Datagram Protocol, Src Port: 32724, Dst Port: 514
[truncated]Syslog message: LOCAL6.NOTICE: Jul 25 11:29:37 SSPT33A CISE_Administrative_and_Operational_Audit 0000000020 1 0 2024-07-25 11:29:37.234 -05:00 0000012891 51002 NOTICE Administrator-Login: Administrator logged off, ConfigVersion
1011 0... = Facility: LOCAL6 - reserved for local use (22)
.... .101 = Level: NOTICE - normal but significant condition (5)
Message [truncated]: Jul 25 11:29:37 SSPT33A CISE_Administrative_and_Operational_Audit 0000000020 1 0 2024-07-25 11:29:37.234 -05:00 0000012891 51002 NOTICE Administrator-Login: Administrator logged off, ConfigVersionId=285, AdminInterf
Syslog timestamp (RFC3164): Jul 25 11:29:37
Syslog hostname: SSPT33A
Syslog process id: CISE
Syslog message id [truncated]: _Administrative_and_Operational_Audit 0000000020 1 0 2024-07-25 11:29:37.234 -05:00 0000012891 51002 NOTICE Administrator-Login: Administrator logged off, ConfigVersionId=285, AdminInterface=GUI, AdminIP

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）。