在ISE上配置外部系統日誌伺服器

目錄

簡介

必要條件

- 需求
- 採用元件

背景資訊

組態

- 配置遠端日誌記錄目標（UDP系統日誌）
- 範例
- 在Logging Categories下配置遠端目標

瞭解類別

驗證和故障排除

簡介

本文檔介紹如何在ISE上配置外部系統日誌伺服器。

必要條件

需求

思科建議您瞭解以下主題：

- 身份服務引擎(ISE)。
- 系統日誌伺服器

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 身分識別服務引擎(ISE)3.3版本。
- Kiwi系統日誌伺服器v1.2.1.4

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

.

來自ISE的系統日誌消息由日誌收集器收集和儲存。這些日誌收集器分配給監控節點，因此MnT在

本地儲存所收集的日誌。

要從外部收集日誌，需要配置外部系統日誌伺服器，這些伺服器稱為目標。日誌被劃分為各種預定義類別。

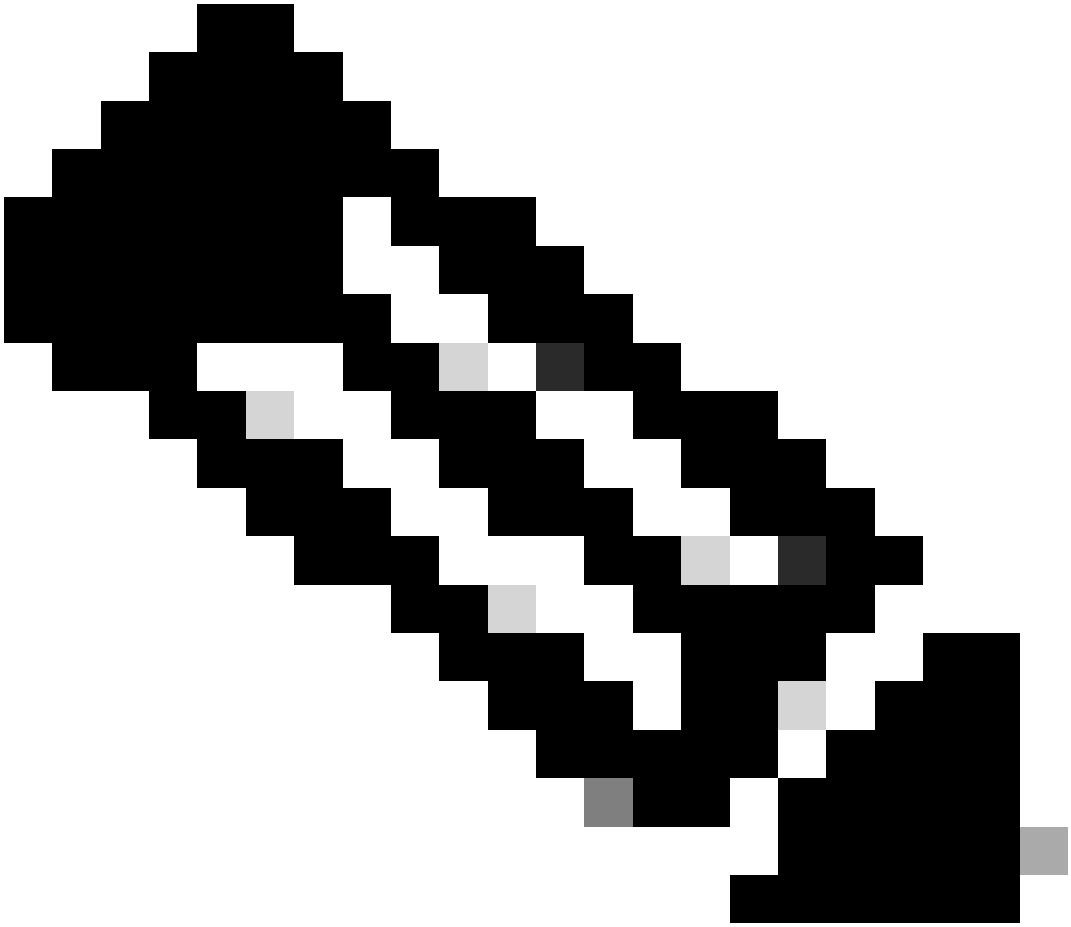
您可以通過編輯與其目標、嚴重性級別等相關的類別來定製日誌記錄輸出。

組態

您可以使用Web介面建立遠端系統日誌伺服器目標，系統日誌消息將傳送到這些目標。日誌消息根據系統日誌協定標準傳送到遠端系統日誌伺服器目標（請參閱RFC-3164）。

配置遠端日誌記錄目標（UDP系統日誌）

在Cisco ISE GUI中，按一下Menuicon( )並選擇Administration>System>Logging>Remote Logging Targets>ClickAdd。



附註：此配置示例基於以下螢幕截圖：正在配置遠端日誌記錄目標。

- 名稱為Remote_Kiwi_Syslog，您可以在此處輸入遠端Syslog伺服器的名稱，此名稱用於說明性目的。
- 目標類型為UDP Syslog，在此配置示例中，使用的是UDP Syslog;但是，您可以從Target Type下拉選單中配置更多選項：

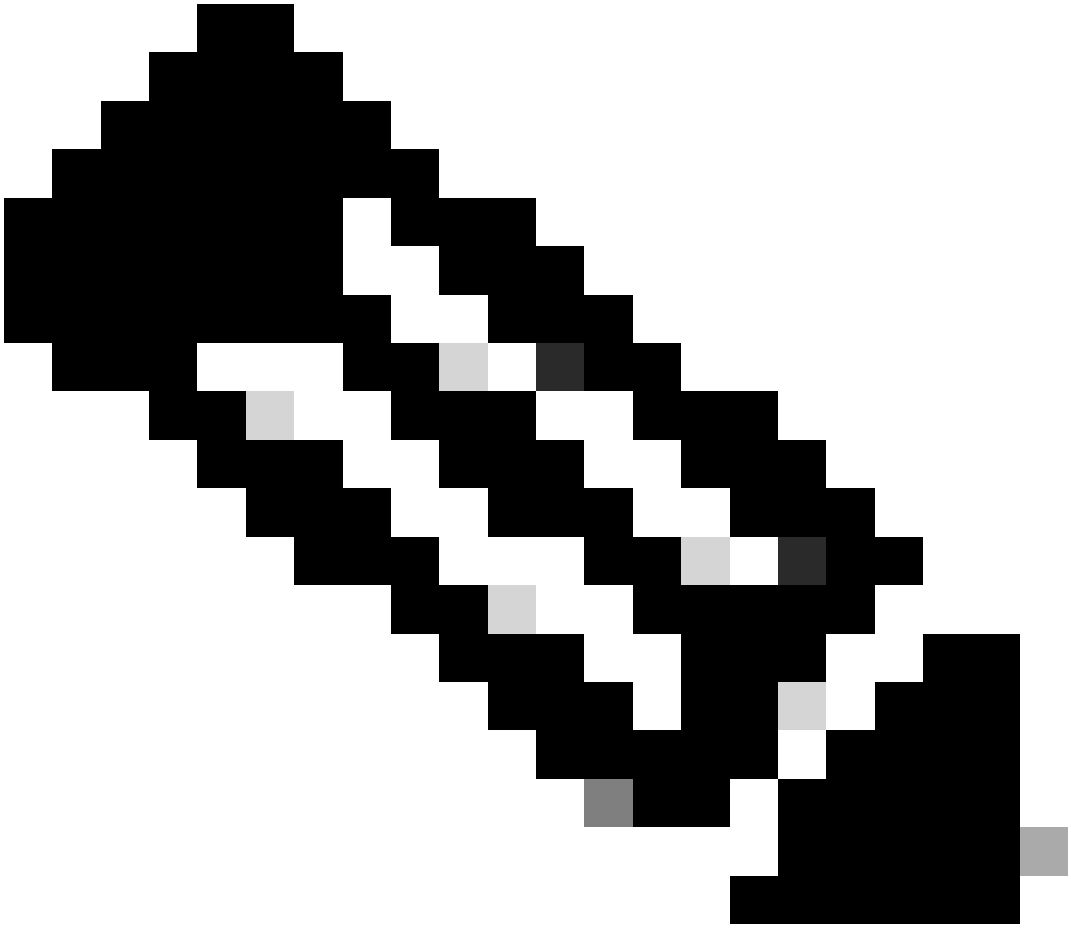
UDP系統日誌：用於通過UDP傳送系統日誌消息，適用於輕量級和快速日誌記錄。

TCP系統日誌：用於通過TCP傳送系統日誌消息，通過錯誤檢查和重新傳輸功能提供可靠性。

安全系統日誌：它是指通過TCP使用TLS加密傳送的系統日誌消息，以確保資料完整性和機密性。

- 狀態為Enabled，您必須從Statuss下拉選單中選擇Enabled。
- 說明（可選）您可以輸入新目標的簡要說明。
- 主機/IP地址，此處輸入儲存日誌的目標伺服器的IP地址或主機名。Cisco ISE支援用於日誌記

錄的IPv4和IPv6格式。



附註：必須指出的是，如果要使用FQDN配置系統日誌伺服器，必須設定DNS快取以避免對效能產生影響。如果沒有DNS快取，每次必須將系統日誌資料包傳送到配置了FQDN的遠端日誌記錄目標時，ISE都會查詢DNS伺服器。這會對ISE效能產生嚴重影響。

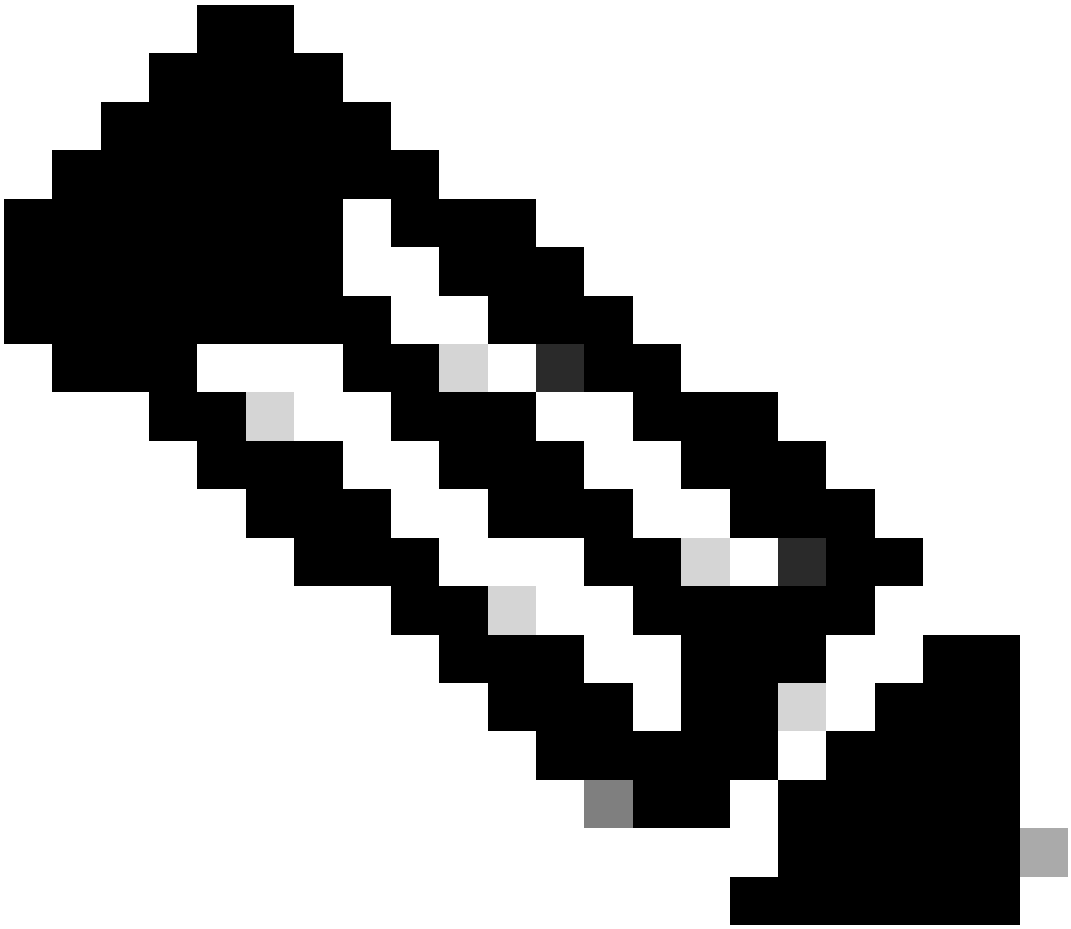
在部service cache enable署的所有PSN中使用命令可以克服以下問題：

範例

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

- 埠為514，在此配置示例中，Kiwi Syslog伺服器正在偵聽埠514，該埠是UDP系統日誌消息的預設埠。但是，使用者可以將此埠號更改為1到65535之間的任意值。請確保您的所需埠未被任何防火牆阻止。

- 設施代碼作為LOCAL6，您可以從下拉選單中選擇必須用於日誌記錄的系統日誌設施代碼。有效選項為Local0到Local7。
- Maximum Length as 1024，您可以在此處輸入遠端日誌目標消息的最大長度。Maximum length預設設定為1024，預設情況下為ISE 3.3版本，值介於200到8192位元組之間。

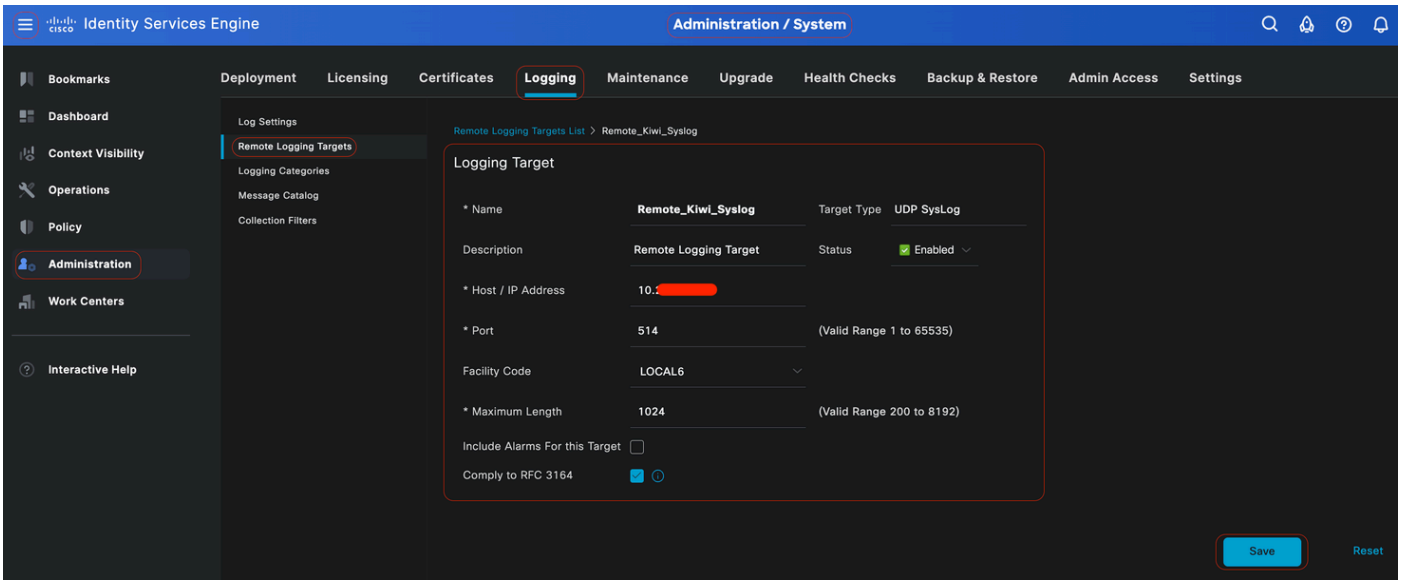


附註：為了避免將截斷的消息傳送到遠端目標，您可以將最大長度修改為8192。

- 包括此目標的警報，為了使其簡單，在此配置示例中，不選中此目標的包括警報；但是,選中此覈取方塊時，也會向遠端伺服器傳送警報消息。
- 已選中「符合RFC 3164」，當您選中此覈取方塊時，分隔符(、;{ } \ \ \)在傳送到遠端伺服器的系統日誌消息中，即使使用反斜線(\)也不會轉義。

- 完成配置後，按一下Save。

- 儲存後，系統將顯示以下警告：您已選擇建立到伺服器的不安全(TCP/UDP)連線。是否確實要繼續？按一下是。



配置遠端目標

在Logging Categories下配置遠端目標

思科ISE將可稽核事件傳送到系統日誌目標。配置遠端日誌記錄目標後，您需要將遠端日誌記錄目標對映到目標類別以轉發可審計的事件。

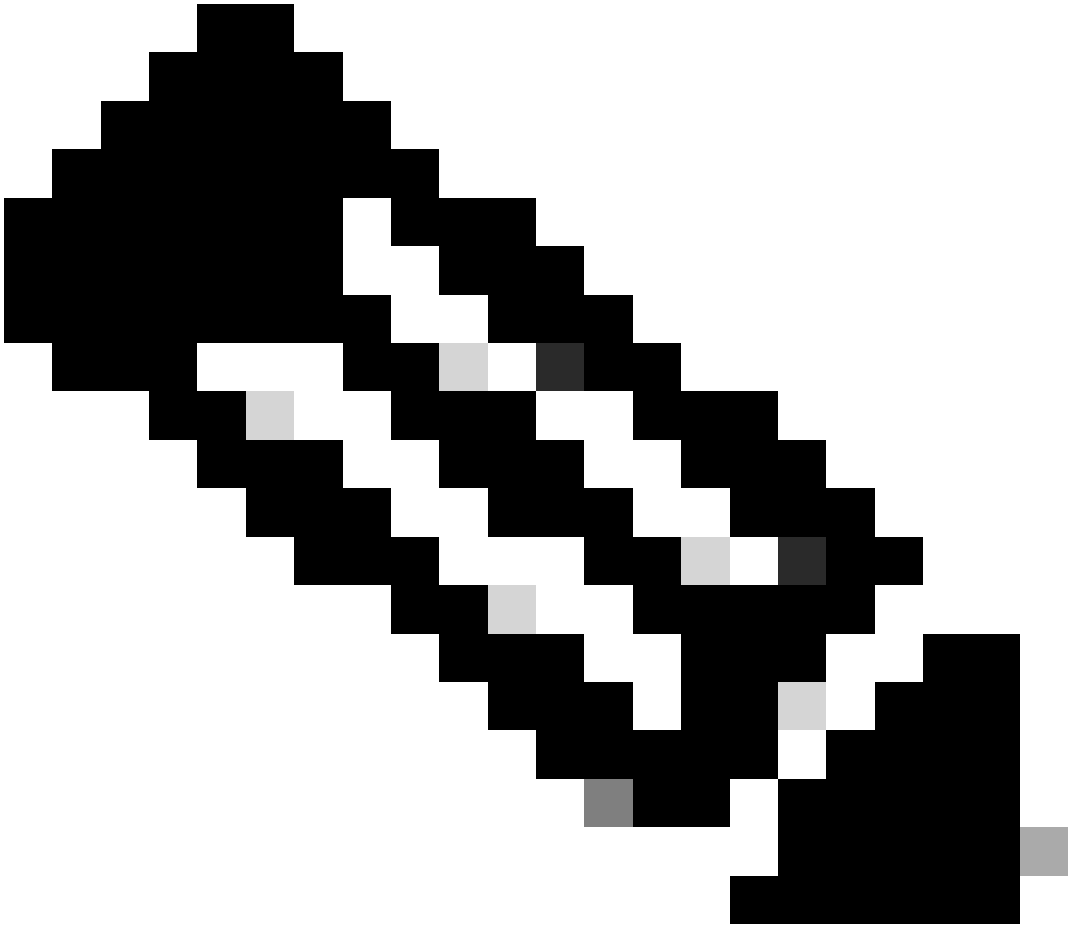
然後，可以將日誌記錄目標對映到這些日誌記錄類別中的每一個。這些日誌類別中的事件日誌僅從PSN節點生成，可以配置為將相關日誌傳送到遠端系統日誌伺服器，具體取決於這些節點上啟用的服務：

- AAA審計
- AAA診斷
- 計量
- 外部MDM
- 被動Id
- 狀態和客戶端調配稽核
- 狀態和客戶端調配診斷
- 探查器

這些日誌類別中的事件日誌是從部署中的所有節點生成的，可以配置為將相關日誌傳送到遠端系統日誌伺服器：

- 行政和業務審計
- 系統診斷
- 系統統計資訊

在此配置示例中，您將在以下四個日誌記錄類別下配置遠端目標，這3個類別用於傳送身份驗證流量日誌：通過ISE管理員日誌記錄流量的身份驗證、失敗嘗試和Radius記帳，以及此類別：



附註：此配置示例基於以下螢幕截圖：配置遠端日誌記錄目標

在Cisco ISE GUI中，按一下Menuicon(

)並選擇Administration>System>Logging>Logging Categories，然後按一下所需的category(Passed Authentications， Failed Attempts and Radius Accounting)。

步驟1 — 日誌嚴重性級別：事件消息與嚴重性級別關聯，管理員可使用此級別篩選消息並設定其優先順序。根據需要選擇日誌嚴重性級別。對於某些日誌記錄類別，此值是預設設定的，您無法對其進行編輯。對於某些日誌記錄類別，您可以從下拉選單中選擇以下嚴重性級別之一：

- 致命:緊急級別。此級別意味著您不能使用思科ISE，您必須立即採取必要的操作。
- 錯誤：此級別表示出現嚴重錯誤情況。
- 警告:此級別表示正常但重要的情況。這是為許多日誌記錄類別設定的預設級別。
- 資訊:此級別表示資訊性消息。
- DEBUG:此級別表示診斷錯誤資訊。

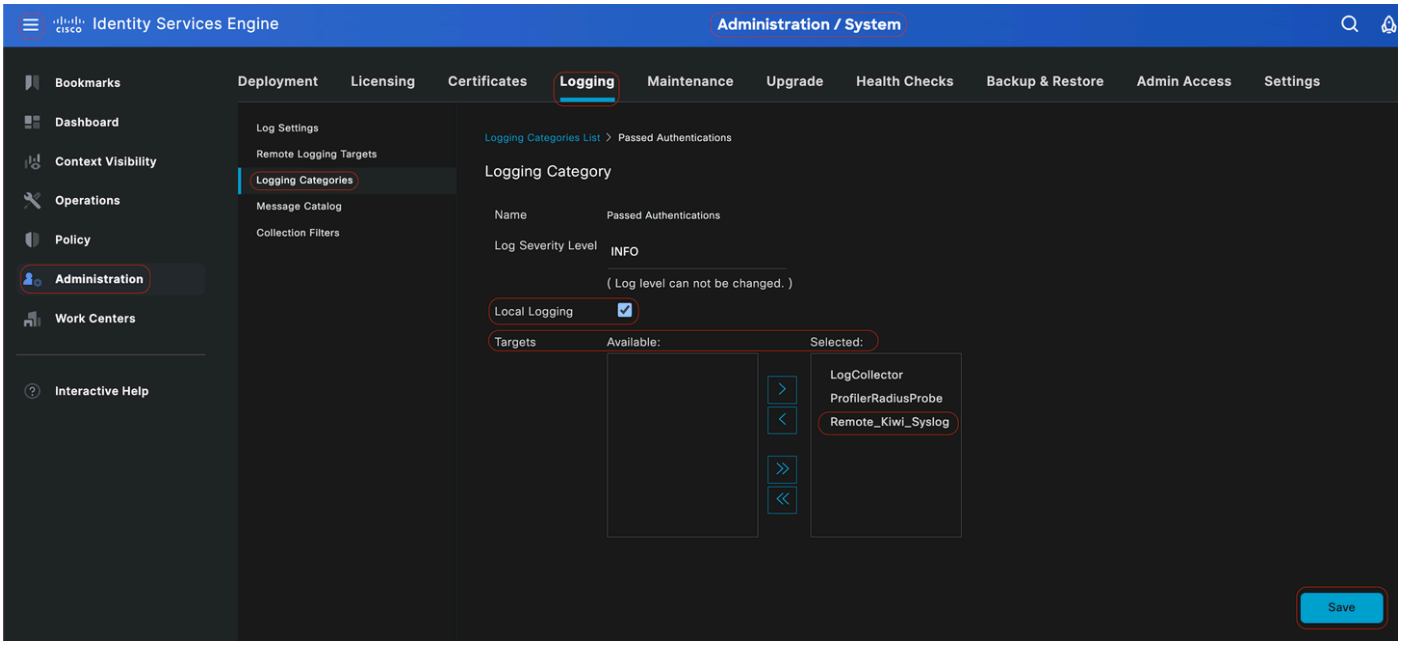
第2步 — Local Logging: 此覈取方塊啟用本地日誌生成。這意味著PSN生成的日誌也儲存在生成日誌的特定PSN上。建議保留預設配置

步驟3 - Targets：此區域允許您通過使用左箭頭和右箭頭圖示在Availableand和Selectedareas之間傳輸目標，從而選擇日誌記錄類別的目標。

Availablearea包含現有的日誌記錄目標，既包括本地（預定義的），也包括外部（使用者定義的）。

Selectedarea（最初為空）隨後顯示為該類別選擇的目標。

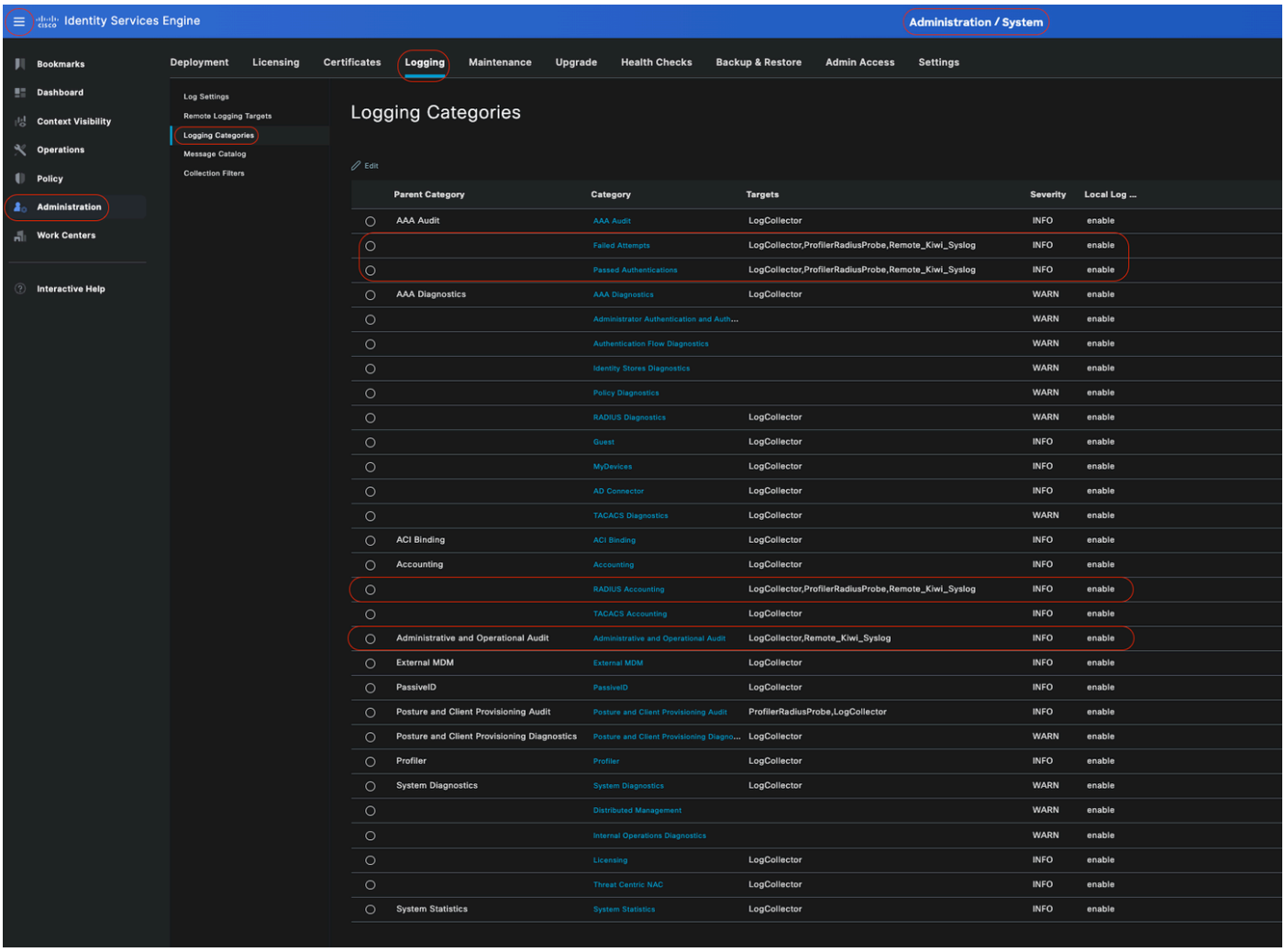
第4步 — 從第1步重複到第3步，將遠端目標新增到Failed Attempts和Radius Accounting類別。



將遠端目標對映到目標類別

步驟5 -驗證您的遠端目標是否在所需類別下。您必須能夠看到您剛剛新增的遠端目標。

在此螢幕截圖中，您可以看到遠端目標Remote_Kiwi_Syslog對映到所需的類別。



驗證類別

瞭解類別

事件發生時生成消息。從多個工具（如核心、郵件、使用者級別等）生成的事件消息型別不同。

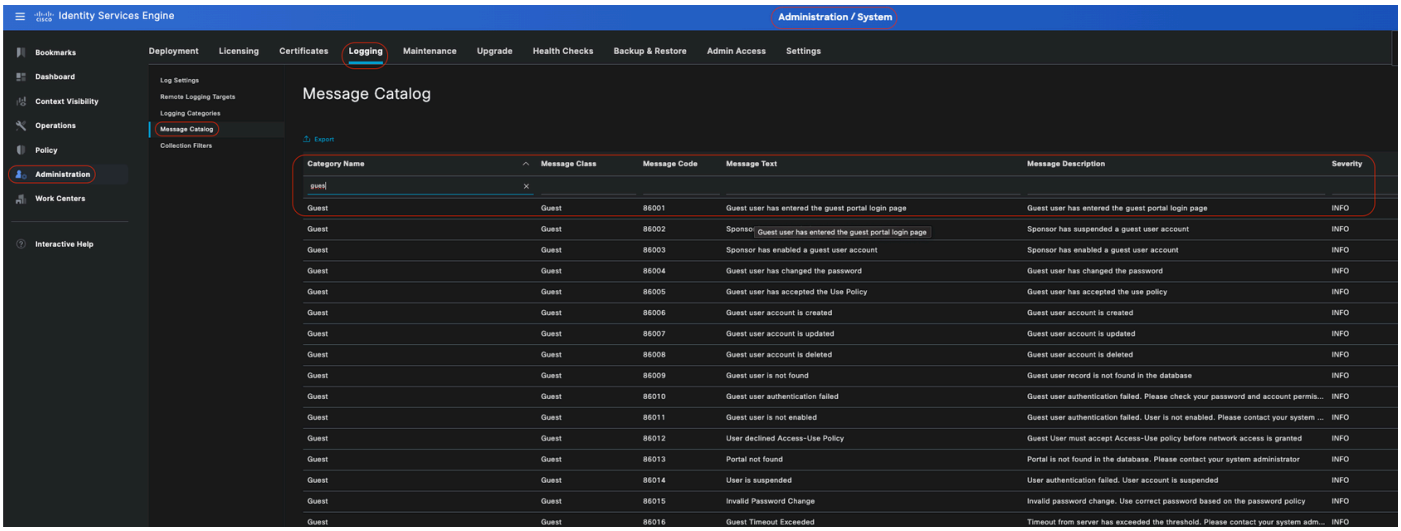
這些錯誤在報文目錄中分類，這些事件還按層次組織成類別。

這些類別具有包含一個或多個類別的父類別。

父類別	類別
AAA審計	AAA審計 失敗的嘗試 通過身份驗證
AAA診斷	AAA診斷 管理員身份驗證和授權

	驗證流程診斷 身份庫診斷 原則診斷 Radius診斷 訪客
計量	計量 RADIUS 計量
行政和業務審計	行政和業務審計
狀態和客戶端調配稽核	狀態和客戶端調配稽核
狀態和客戶端調配診斷	狀態和客戶端調配診斷
探查器	探查器
系統診斷	系統診斷 分散式管理 內部操作診斷
系統統計資訊	系統統計資訊

在此螢幕抓圖中，您可以看到Guest是一個消息類，並被分類為Guest Category。此Guest Category具有一個稱為AAA Diagnostics的父類別。



郵件目錄

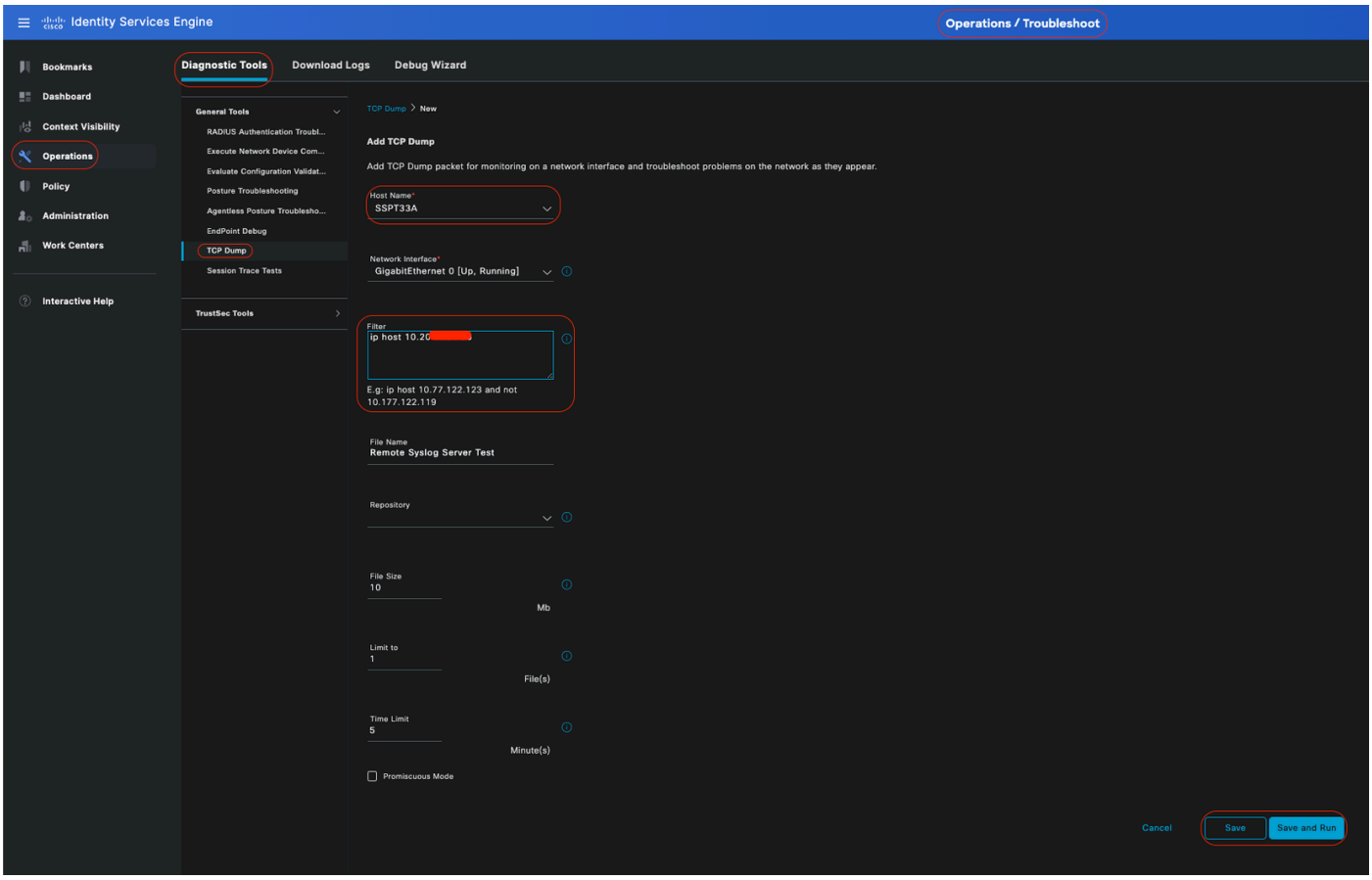
驗證和故障排除

對遠端日誌記錄目標執行TCP轉儲是確認是否傳送日誌事件的最快的故障排除和驗證步驟。

捕獲必須來自對使用者進行身份驗證的PSN，因為PSN將生成日誌消息，這些消息將傳送到遠端目標

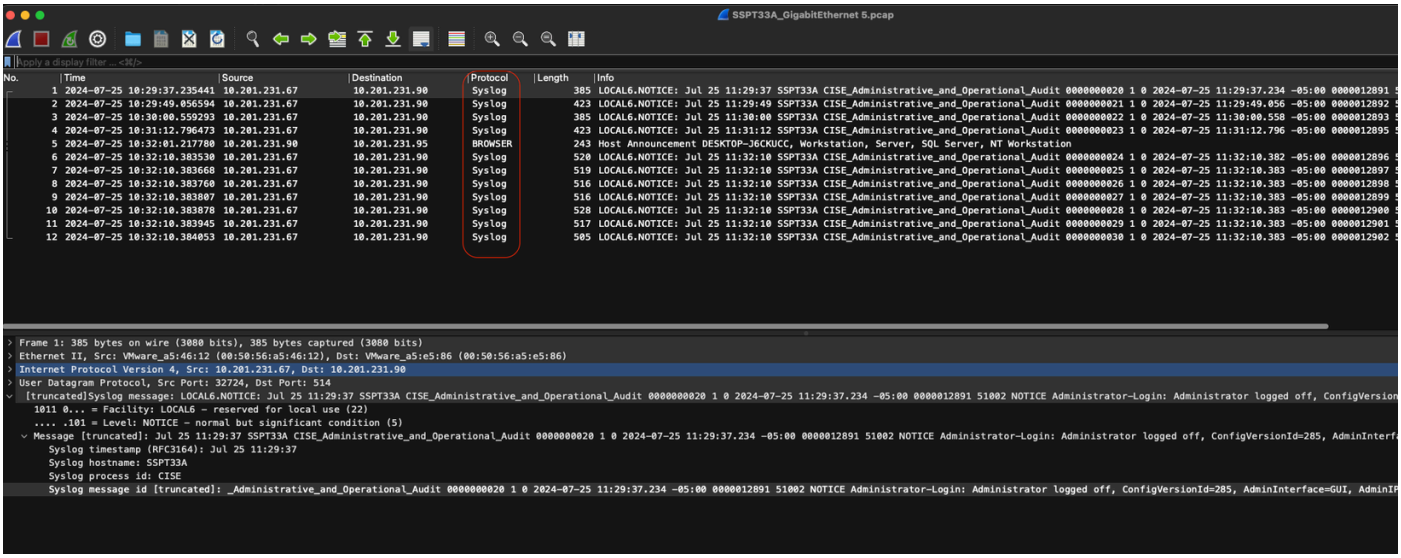
在Cisco ISE GUI中，按一下Menuicon( )並選擇Operations> Troubleshoot>TCP Dump>按一下Add。

- 必須過濾流量，請新增ip host <remote_target_IP_addres>過濾器欄位。
- 您必須從PSN捕獲處理身份驗證。



TCP傾印

在此螢幕截圖中，您可以看到ISE如何為ISE管理員日誌記錄流量傳送系統日誌消息。



系統日誌流量

關於此翻譯
思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。