在ISE上配置外部系統日誌伺服器

目錄

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：

- 身分辨識服務引擎(ISE) 3.3版。
- Kiwi Syslog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。這些日誌收集器被分配給監控節點，以便

MnT在本地儲存所收集的日誌。

要收集外部日誌，需要配置外部系統日誌伺服器，這些伺服器稱為目標。日誌分為各種預定義的類別。

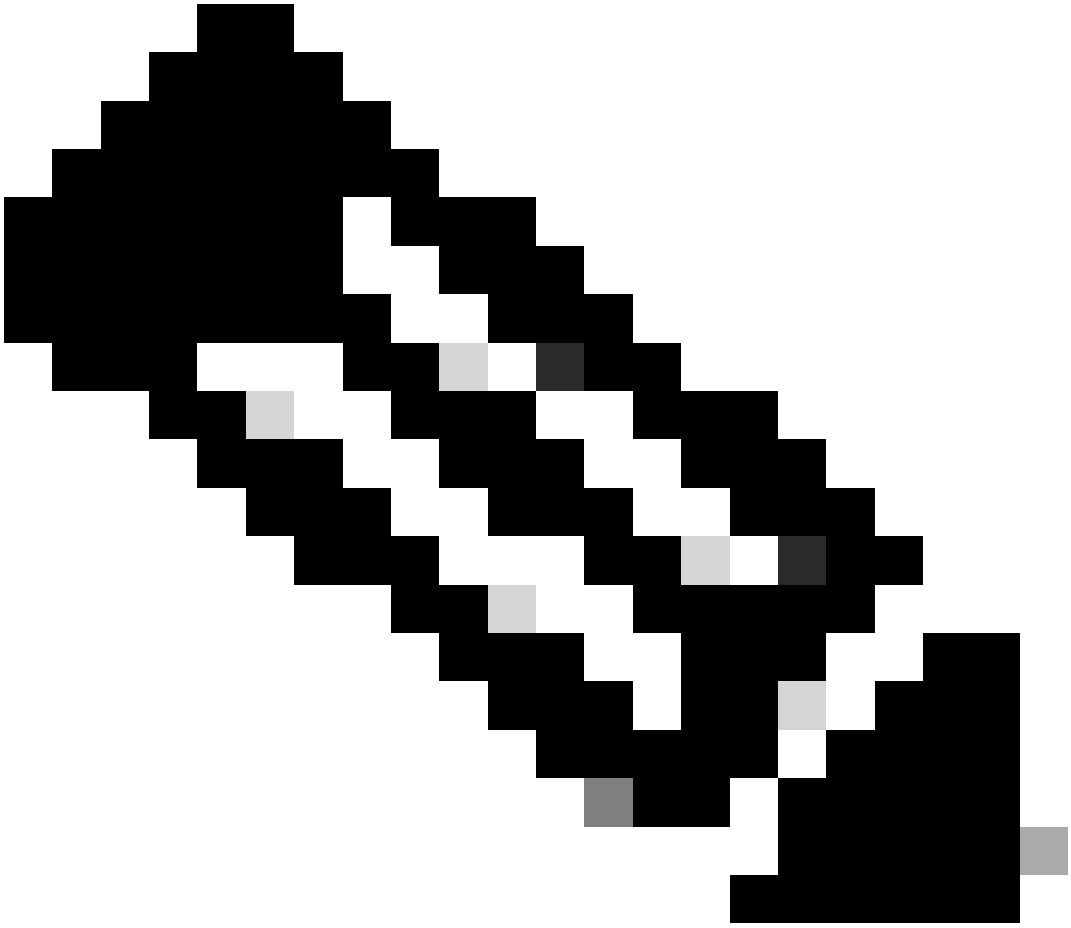
您可以透過編輯與其目標、嚴重性級別相關的類別來自定義日誌記錄輸出。

組態

您可以使用Web介面建立要將系統日誌消息傳送到其中的遠端系統日誌伺服器目標。日誌消息根據syslog協定標準傳送到遠端syslog伺服器目標（請參閱RFC-3164）。

配置遠端日誌記錄目標(UDP Syslog)

在思科ISE GUI中，點選選單圖示(
)並選擇管理>系統>記錄>遠端記錄目標>點選增加。



注意：此配置示例基於名為「配置遠端日誌記錄目標」的螢幕快照。

- 名稱為Remote_Kiwi_Syslog，您可以在此輸入遠端Syslog伺服器的名稱，此名稱用於說明目的。
- 目標型別為UDP Syslog，在此配置示例中，使用的是UDP Syslog；但您可以從目標型別下拉選單配置更多選項：

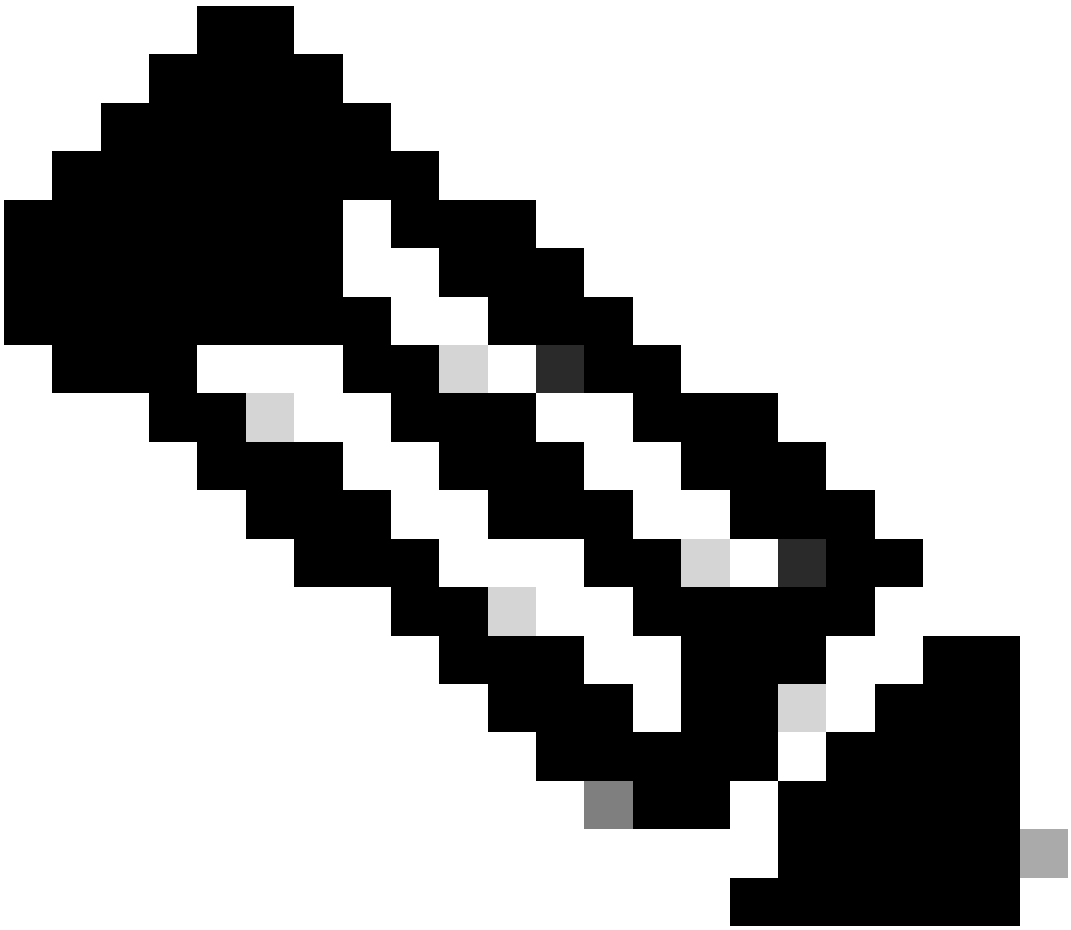
UDP Syslog：用於透過UDP傳送Syslog消息，適用於輕量級和快速日誌記錄。

TCP系統日誌：用於透過TCP傳送系統日誌消息，它透過錯誤檢查和重傳功能提供可靠性。

安全系統日誌：是指使用TLS加密透過TCP傳送的系統日誌消息，確保資料完整性和機密性。

- Status為Enabled，您必須從Statusdrop下拉選單中選擇Enableders。
- 摘要，您可以選擇性地輸入新目標的簡短摘要。
- 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。思科ISE支援IPv4和IPv6格

式的日誌記錄。



注意：必須說明的是，如果要配置帶FQDN的系統日誌伺服器，則必須設定DNS快取以避免對效能產生影響。如果沒有DNS快取，ISE會在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查詢DNS伺服器。這會對ISE效能產生嚴重影響。

在部署的所有PSN中使用service cache enable命令可解決此問題：

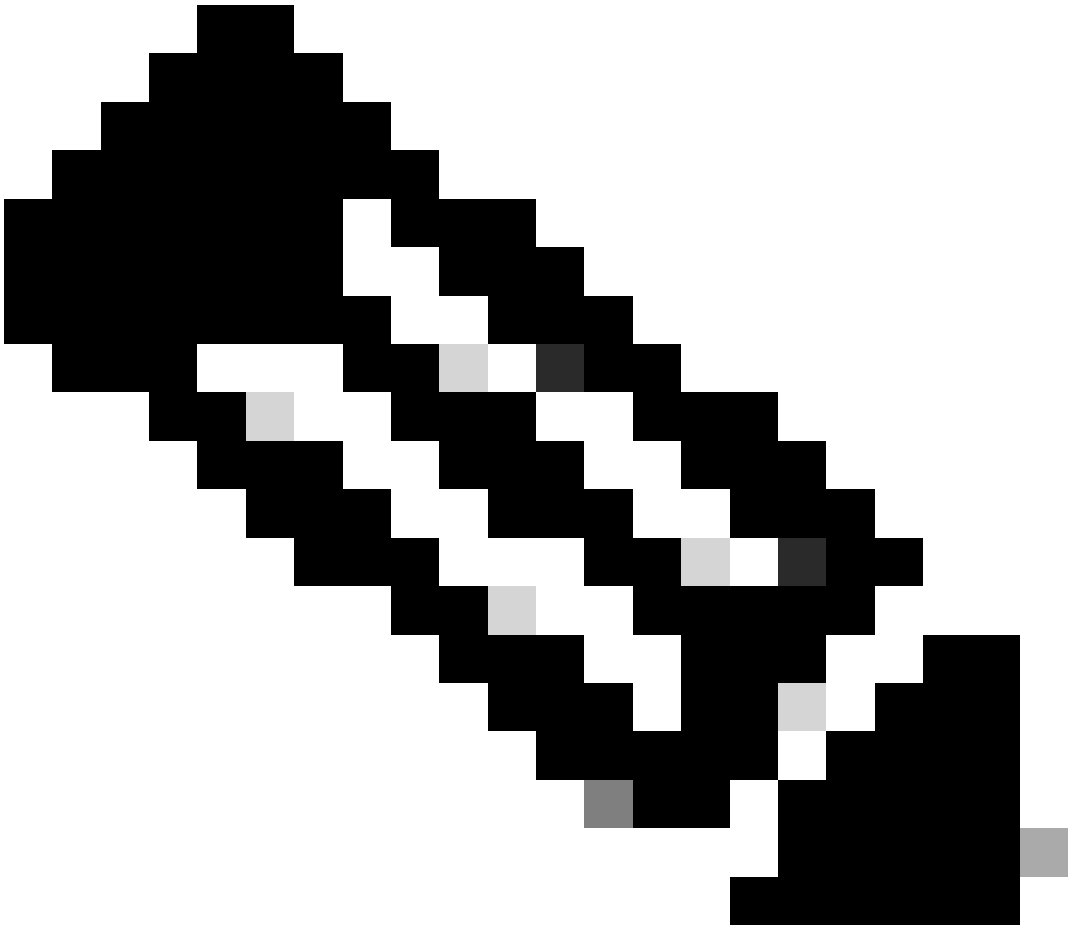
範例

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

- **埠為514**，在此配置示例中，Kiwi Syslog伺服器偵聽埠**514**，這是UDP syslog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。

- **Facility Code** as **LOCAL6**，您可以從下拉選單中選擇必須用於日誌記錄的Syslog裝置代碼。有效選項為Local0到Local7。

- **Maximum Length為1024**，您可以在此處輸入遠端日誌目標消息的最大長度。 最大長度設定為**1024**，預設情況下為ISE 3.3版本，值為200到1024位元組。



注意：為避免將截斷的消息傳送到遠端日誌記錄目標，您可以將「最大長度」修改為「8192」。

- **Include Alarms For this Target**，為了使其簡單，在此配置示例中，未選中**Include Alarms For this Target**；但是，當您選中此覈取方塊時，也會將警報消息傳送到遠端伺服器。

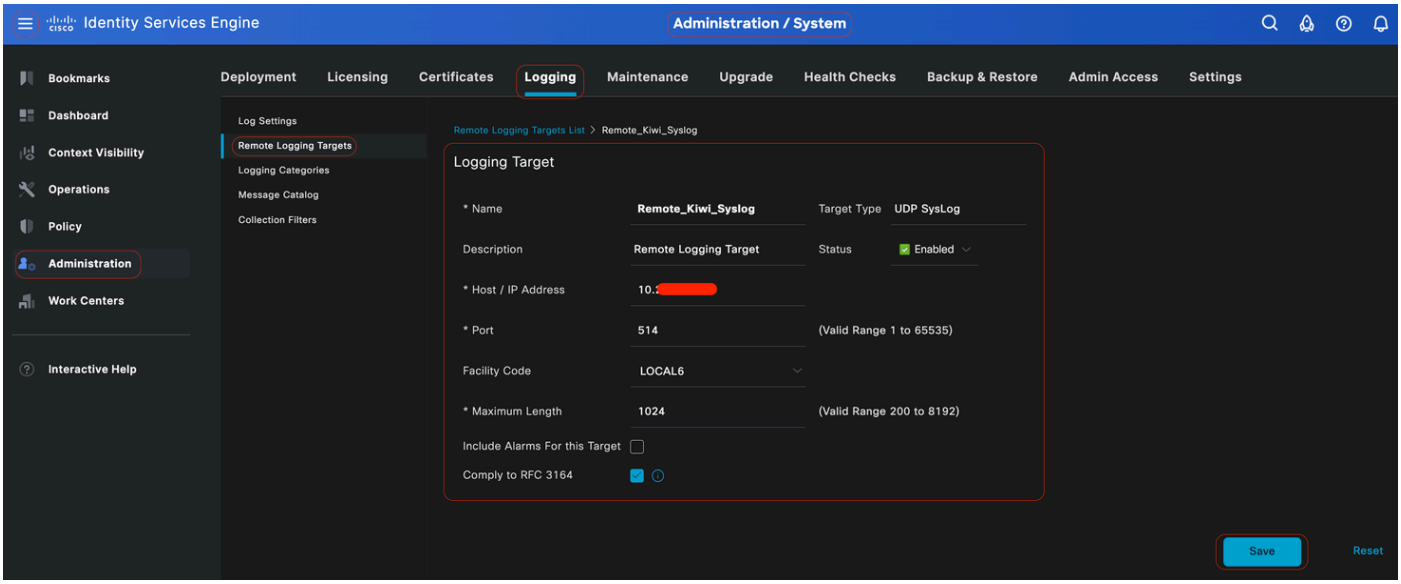
- **Compliance to RFC 3164**已選中，當您選中此覈取方塊時，即使使用了反斜線(\)，傳送到遠端伺服器的系統日誌消息中的分隔符(， ； {} \ \ \)也不會被轉義。

-

配置完成後，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？**，請按一下**Yes**。



設定遠端目標

配置日誌記錄類別下的遠端目標

思科ISE將可審計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**對映到所需的類別以轉發可審計的事件。

然後，日誌記錄目標可以對映到這些日誌記錄類別中的每一種。 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稽核

-

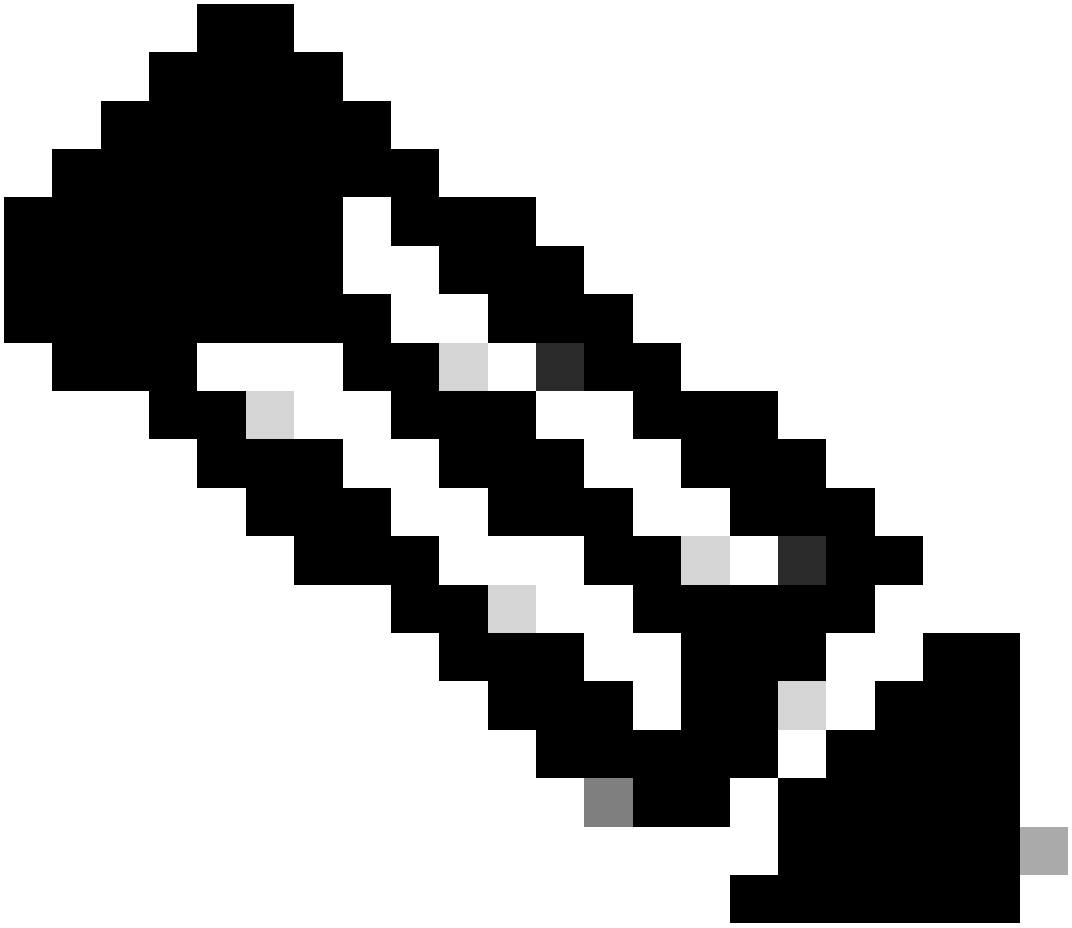
AAA診斷

- **計量**
- **外部MDM**
- **被動Id**
- **狀態和客戶端調配稽核**
- **狀態與使用者端布建診斷**
- **效能評測器**

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

- **行政和業務審計**
- **系統診斷**
- **系統統計資料**

在此配置示例中，您將在四個日誌記錄類別下配置遠端目標，這三個Logging Categories用於傳送身份驗證流量日誌：**Passed Authentications**、**Failed Attempts**和**Radius Accounting**，此類別用於ISE管理員日誌記錄流量：



注意：**此配置示例基於名為「配置遠端日誌記錄目標」的螢幕快照**

在思科ISE GUI中，**點選選單圖示(**

)並選擇**Administration>System>Logging>Logging Categories**，然後點選所需類別(**Passed Authentications**、**Failed Attempts**和**Radius Accounting)**。

步驟1-日誌嚴重性級別：事件消息與嚴重性級別相關聯，允許管理員過濾消息並排定其優先順序。 根據需要選擇日誌嚴重性級別。 對於某些日誌記錄類別，預設情況下會設定此值，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：

- **嚴重**：緊急程度。此級別意味著您不能使用Cisco ISE，您必須立即採取必要的操作。
- **錯誤**：此層次表示嚴重錯誤情況。
- **WARN**：此級別指示正常但重要的情況。這是為許多記錄類別設定的預設級別。
- **INFO**：此級別表示參考消息。

- **DEBUG**：此級別指示診斷錯誤消息。

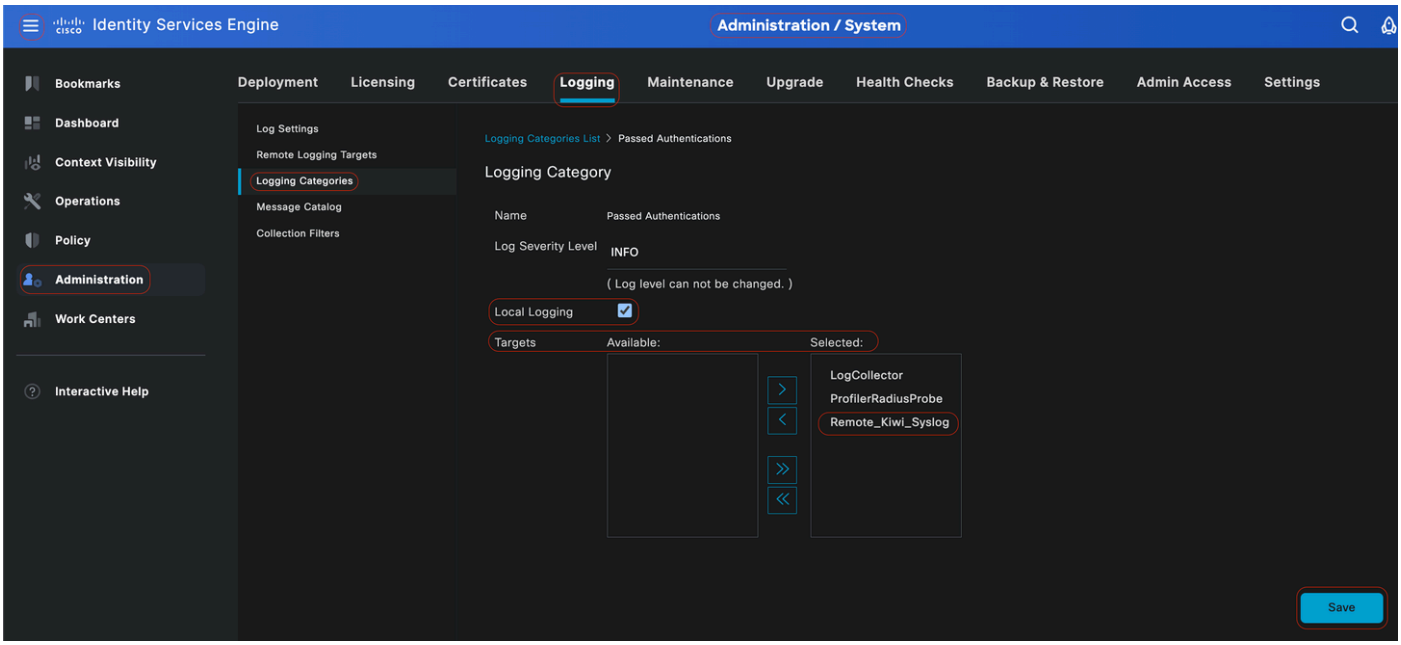
第2步- 本地日誌記錄：此覈取方塊用於啟用本地日誌生成。這意味著PSN生成的日誌也儲存在生成日誌的特定PSN上。我們建議保留預設配置

步驟3 -目標：此區域允許您選擇日誌記錄類別的目標，方法是使用左箭頭和右箭頭圖示在Availabledarea和Selectedarea之間傳輸目標。

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

Selectedarea （最初為空白）接著會顯示已為該類別選擇的目標。

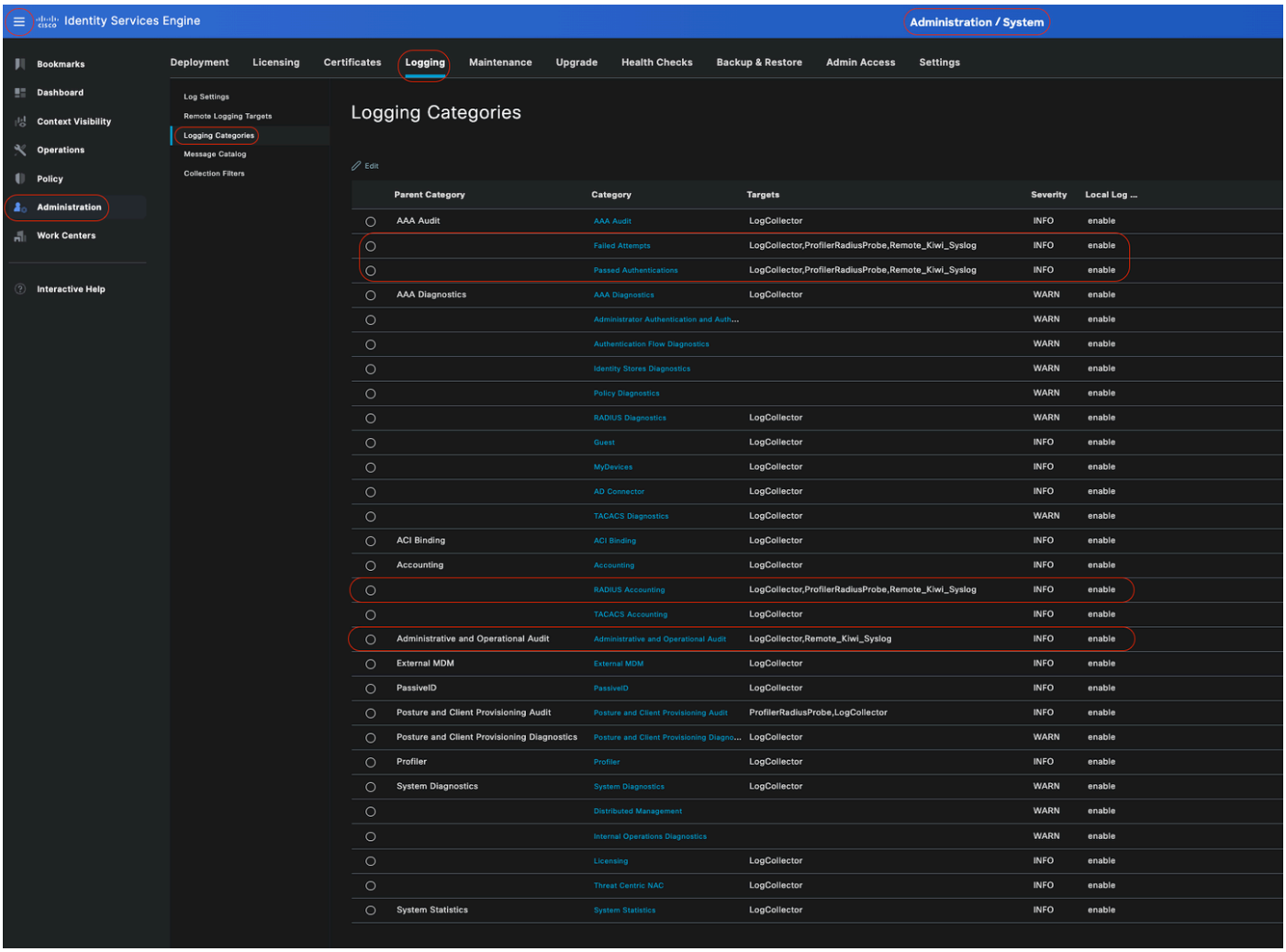
第4步-重複第1步到第3步，在**嘗試失敗和Radius記帳**類別下增加遠端目標。



將遠端目標對映到目標類別

第5步-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增加的遠端目標。

在此螢幕截圖中，您可以看到對映到所需類別的遠端目標**Remote_Kiwi_Syslog**。



驗證類別

瞭解類別

當事件發生時，會產生訊息。從多個工具（如核心、郵件、使用者級別等）生成了不同型別的事件消息。

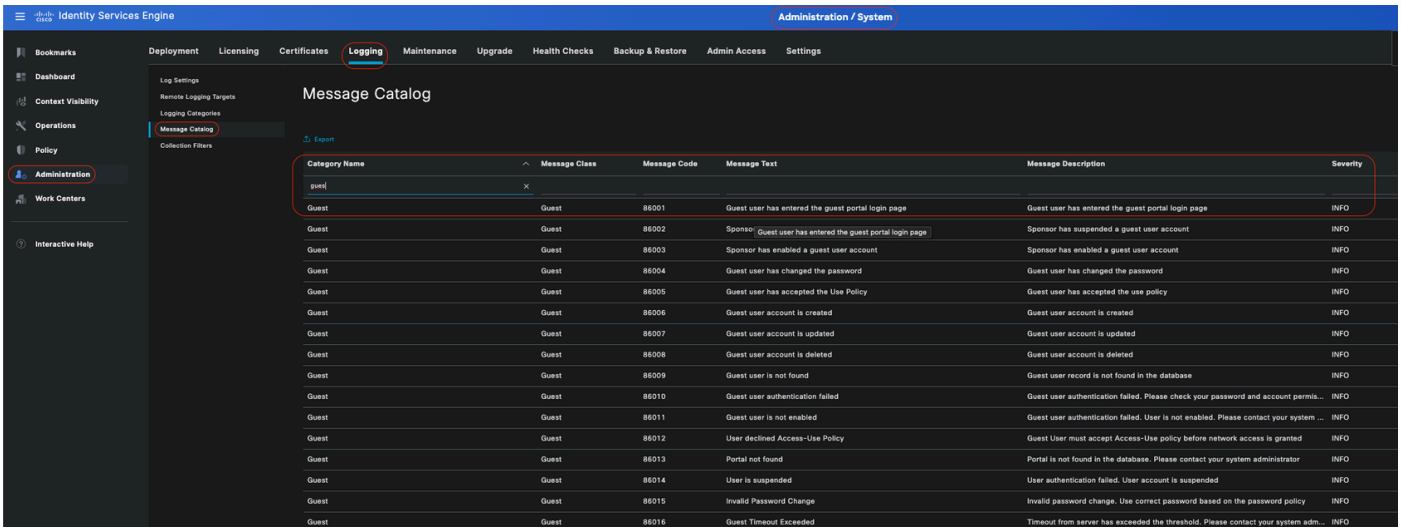
這些錯誤在報文目錄中進行了分類，並且這些事件也按層次進行了分類。

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稽核	AAA稽核 失敗的嘗試 透過驗證
AAA診斷	AAA診斷 管理員驗證與授權

	驗證流程診斷 辨識存放區診斷 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
狀態與使用者端布建診斷	狀態與使用者端布建診斷
效能評測器	效能評測器
系統診斷	系統診斷 分散式管理 內部作業診斷
系統統計資料	系統統計資料

在此螢幕截圖中，可以看到**Guest**是消息類並分類為**Guest**類別。 此訪客類別有一個稱為**AAA Diagnostics**的父類別。



訊息目錄

檢驗和故障排除

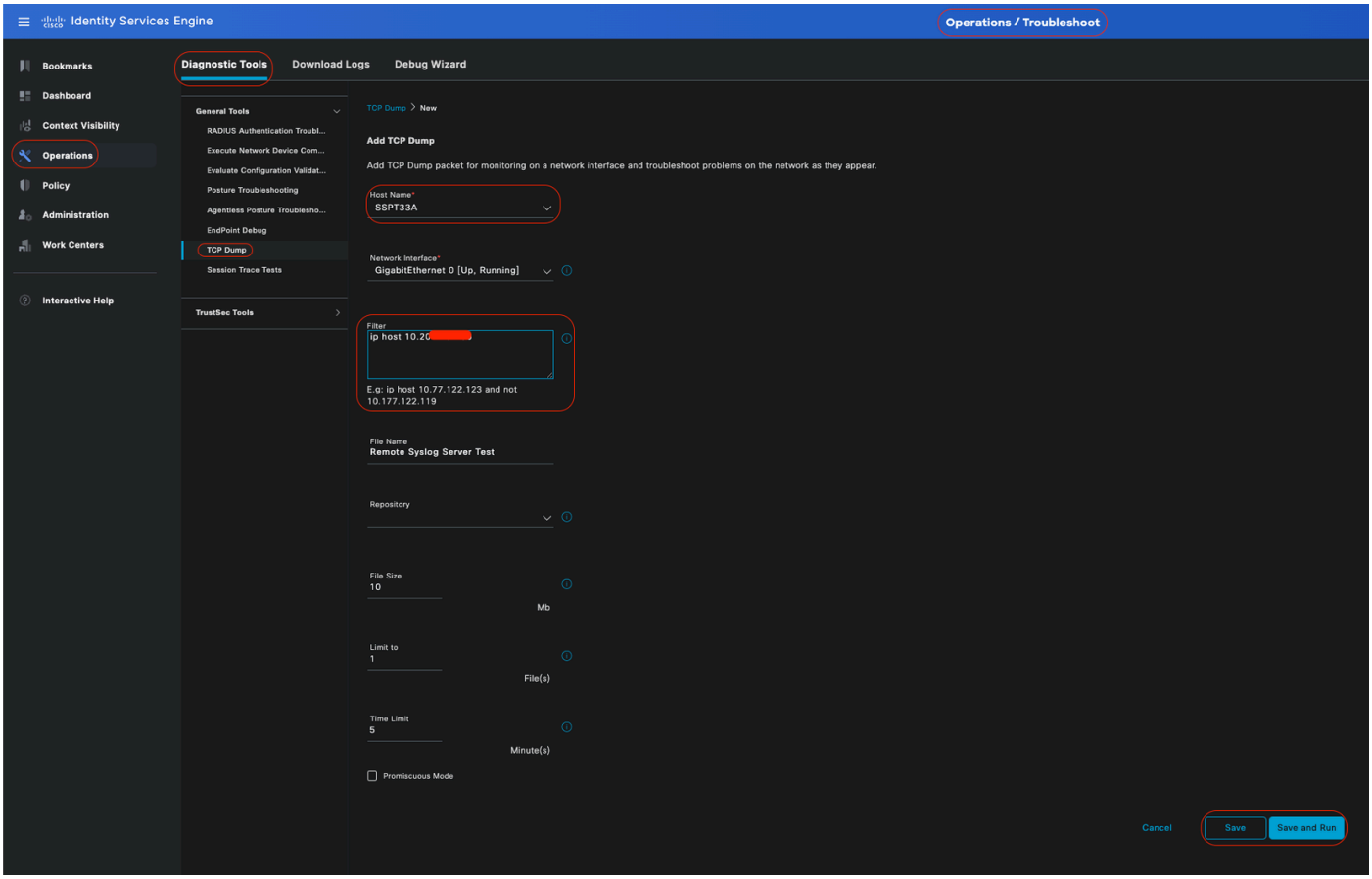
對遠端日誌記錄目標執行TCP轉儲是確認是否傳送日誌事件的最快的故障排除和驗證步驟。

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，並且這些消息將傳送到遠端目標

在思科ISE GUI中，點選選單圖示(
)，然後選擇**操作**>**故障排除**>**TCP轉儲**>點選**增加**。

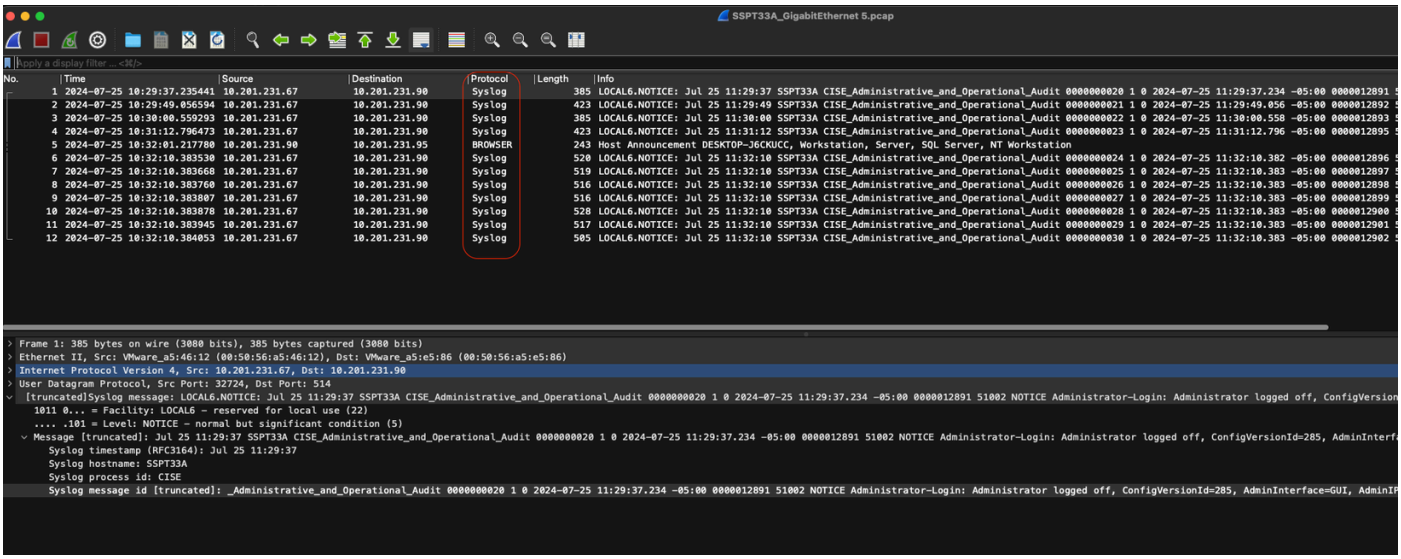
- 您必須過濾流量，請增加ip host <remote_target_IP_addres> filter欄位。

- 您必須從PSN獲取處理身份驗證的捕獲。



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。


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）。