使用Microsoft Server在安全Web裝置中配置SCP推送日誌

目錄

簡介

本文描述設定Secure Copy (SCP)以自動將Secure Web Appliance (SWA)中的記錄複製到其他伺服器的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- SCP的工作方式。
- SWA管理。
- Microsoft Windows或Linux作業系統的管理。

思科建議您：

- 已安裝物理或虛擬SWA。

- 許可證已啟用或已安裝。
- 安裝精靈已完成。

- 對SWA圖形使用者介面(GUI)的管理訪問。
- 已安裝Microsoft Windows (至少Windows Server 2019或Windows 10 （內部版本1809）)或Linux系統。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

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。

SCP

安全複製(SCP)的行為與遠端複製(RCP)類似，後者來自Berkeley r-tools套件（Berkeley大學自有的一組網路應用），不同之處在於SCP依賴安全外殼(SSH)來實現安全。此外，SCP要求配置身份驗證、授權和記帳(AAA)授權，以便裝置可以確定使用者是否具有正確的許可權級別

遠端伺服器上的SCP方法（相當於SCP推送）定期透過安全複製協定將日誌檔案推送到遠端SCP伺服器。此方法要求遠端電腦上使用SSH2協定的SSH SCP伺服器。該訂閱需要遠端電腦上的使用者名稱、SSH金鑰和目標目錄。系統會根據您設定的變換排程來傳輸記錄檔。

SWA日誌訂閱

您可以為每種型別的記錄檔建立多個記錄訂閱。訂用包括存檔和儲存的配置詳細資訊，包括：

- 變換設定，決定何時查扣記錄檔。
- 存檔日誌的壓縮設定。
- 存檔日誌的檢索設定，用於指定日誌是存檔到遠端伺服器上還是儲存在裝置上。

存檔記錄檔

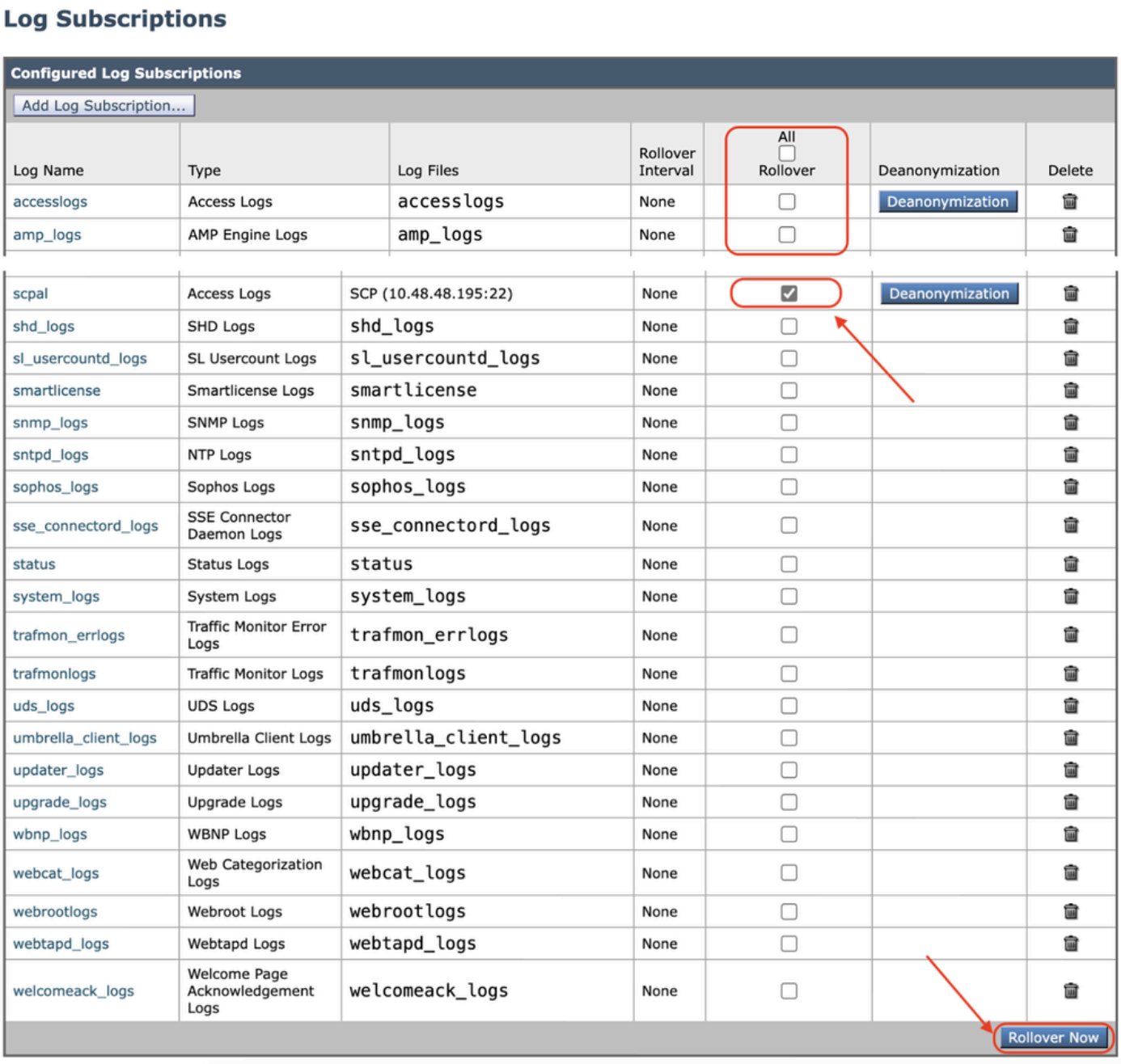
當當前日誌檔案達到使用者指定的最大檔案大小限制或自上次滾動以來的最長時間時，AsyncOS存檔（滾動）日誌訂閱。

日誌訂閱中包含以下存檔設定：

- 依檔案大小變換影像
- 按時間滾動更新
- 日誌壓縮
- 擷取方法

您也可以手動存檔（回滾）記錄檔。
步驟 1.選擇System Administration > Log Subscriptions。

步驟 2.選中要存檔的日誌訂閱的「變換」列中的覈取方塊，或選中全部覈取方塊以選擇所有訂閱。
第3步。點選立即滾動以存檔所選日誌。



影象-立即滑鼠指向效果GUI

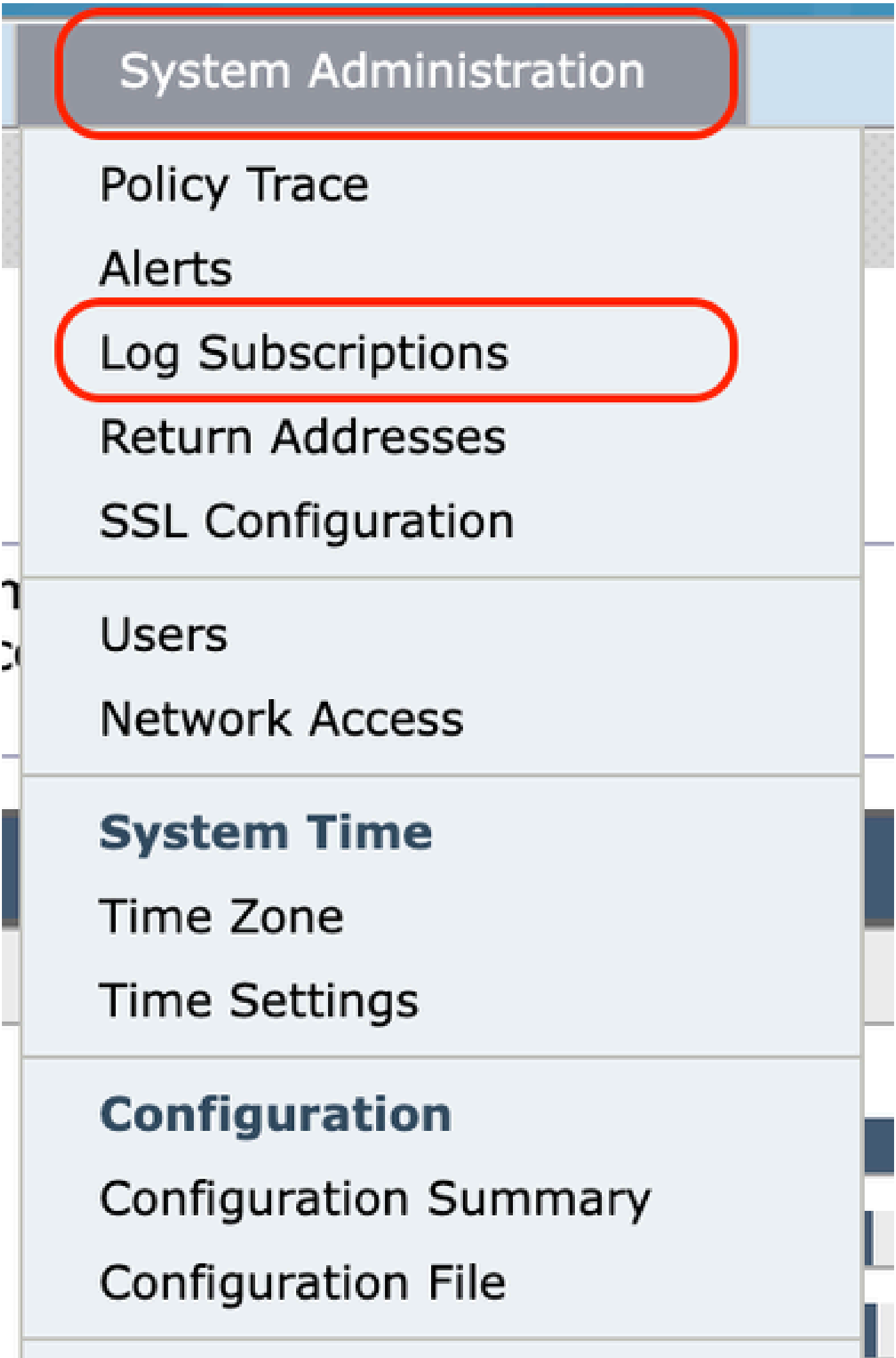
透過遠端伺服器上的SCP配置日誌檢索

從SWA使用SCP將日誌檢索到遠端伺服器有兩個主要步驟：

1. 配置SWA以推送日誌。
2. 設定遠端伺服器以接收記錄。

將SWA配置為從GUI將日誌傳送到SCP遠端伺服器

步驟 1.登入到SWA，然後從System Administration中選擇Log Subscriptions。


System Administration
Policy Trace
Alerts
Log Subscriptions
Return Addresses
SSL Configuration
Users
Network Access
System Time
Time Zone
Time Settings
Configuration
Configuration Summary
Configuration File

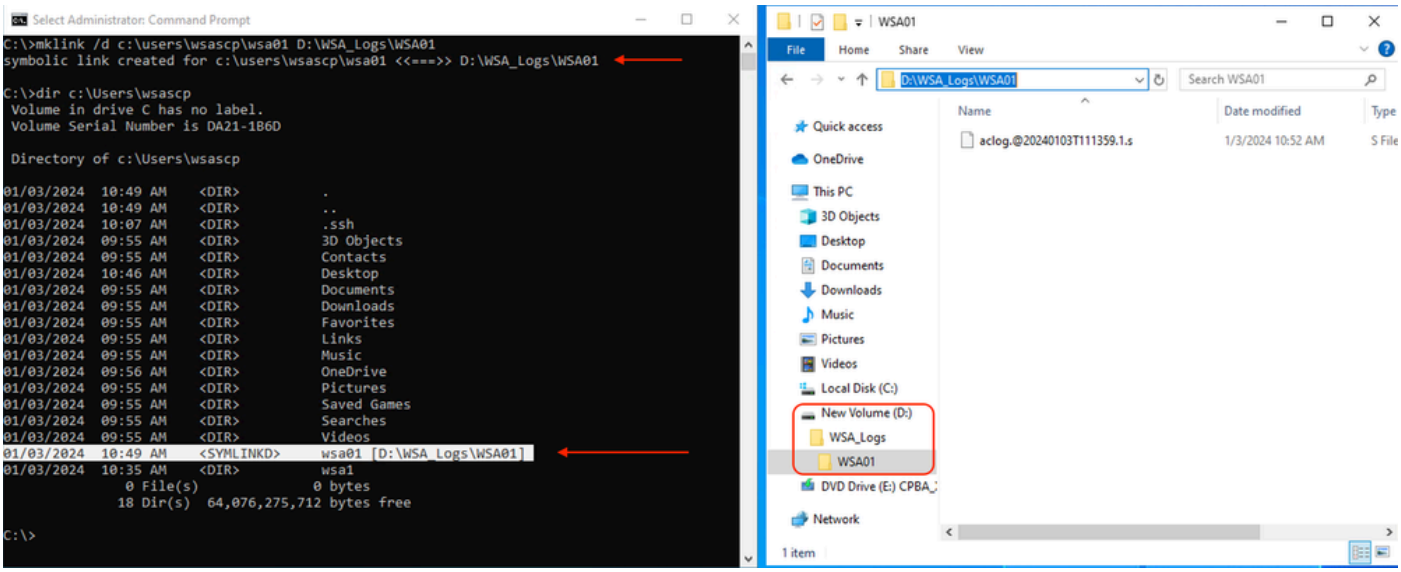
以外的其他磁碟機，請建立從使用者設定檔資料夾到所需磁碟機的連結。在本示例中，日誌被推送到D:\WSA_Logs\WSA01（這四個關鍵計數器以粗體顯示）。

步驟1.在所需驅動器中建立資料夾，如本示例所示

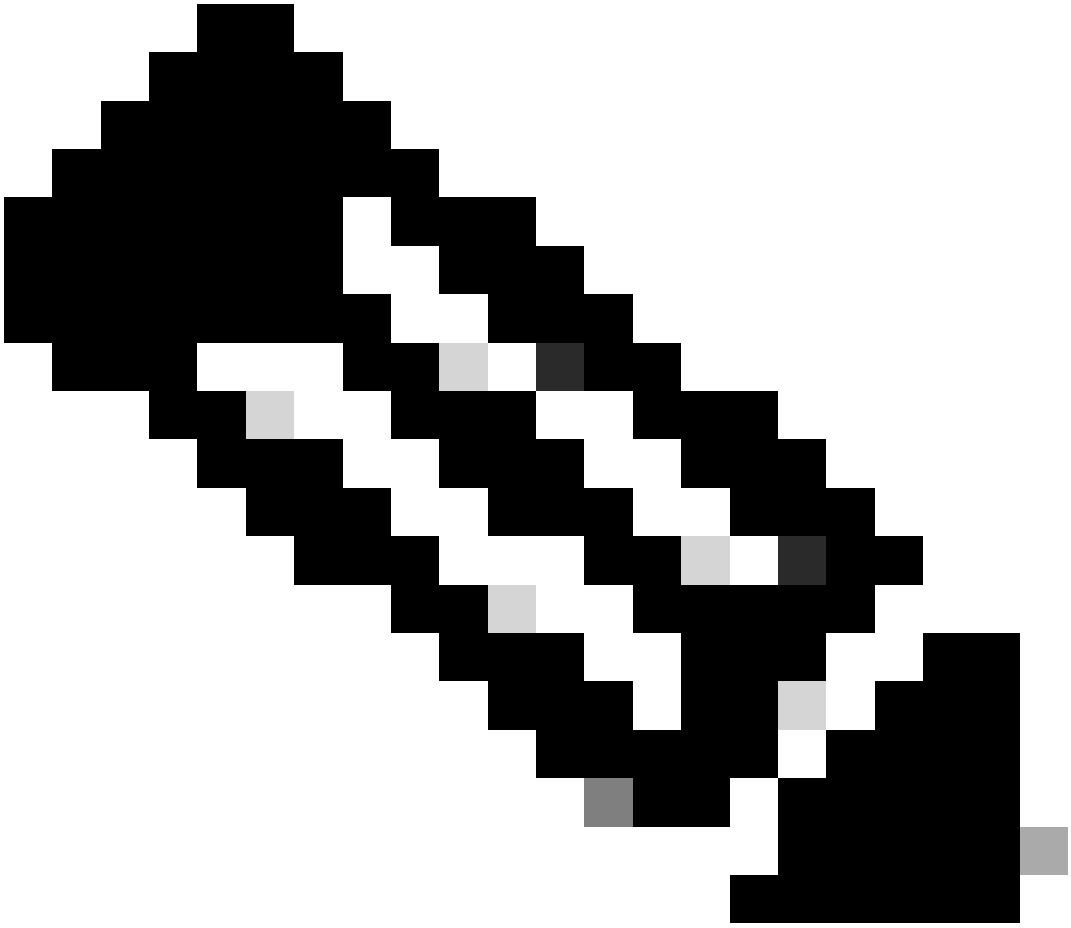
步驟 2.打開具有管理員許可權的命令提示符（以管理員身份運行）

步驟 3.執行此命令以建立連結：

```
mklink /d c:\users\wsascp\wsa01 D:\WSA_Logs\WSA01
```



影像-建立SYM連結



注意：在此示例中，SWA配置為將日誌推送到C:\Users\wsascp中的WSA01資料夾（在Cisco IOS軟體中），而SCP伺服器將資料夾WSA01作為指向D:\WSA_Logs\WSA01的符號連結

有關Microsoft Symbol連結的詳細資訊，請訪問：mklink | Microsoft學習

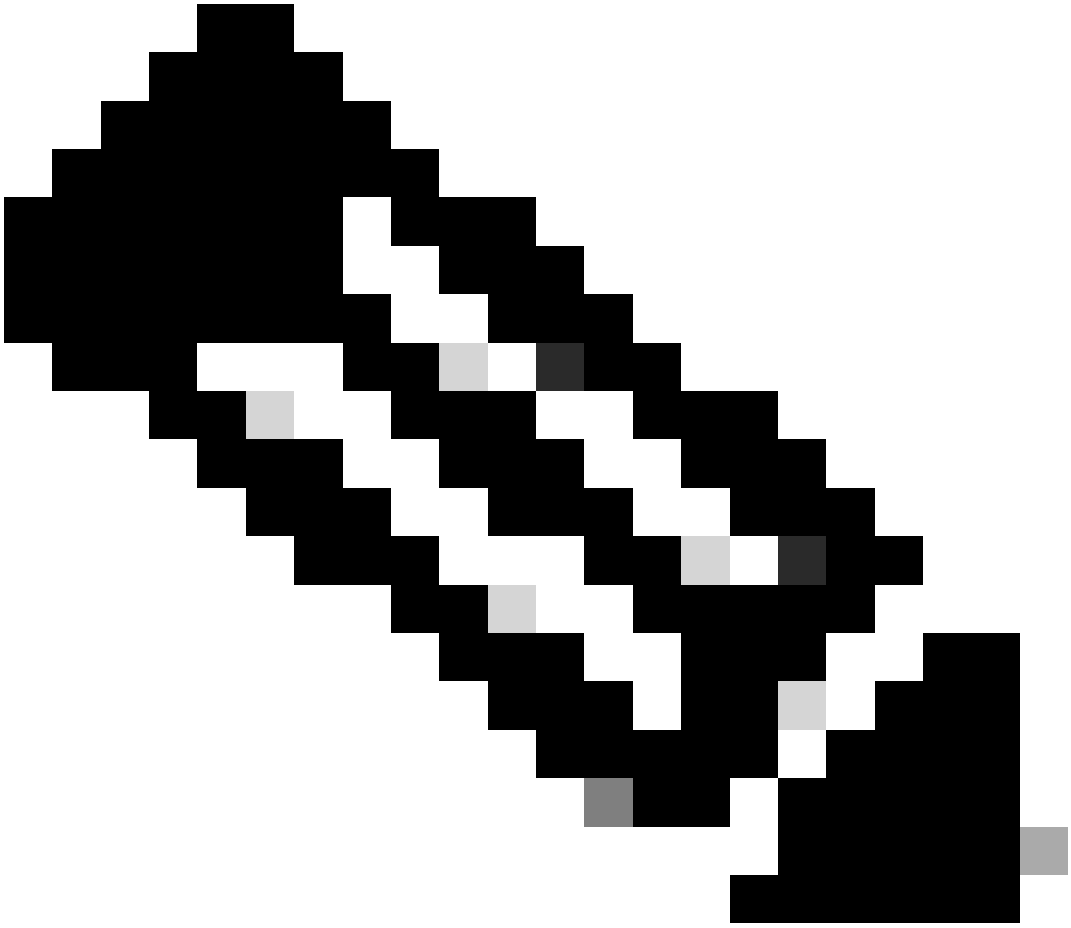
排除SCP日誌推送故障

在SWA中檢視記錄

要排除SCP日誌推送的故障，請在以下位置檢查錯誤：

1. CLI > displayalerts

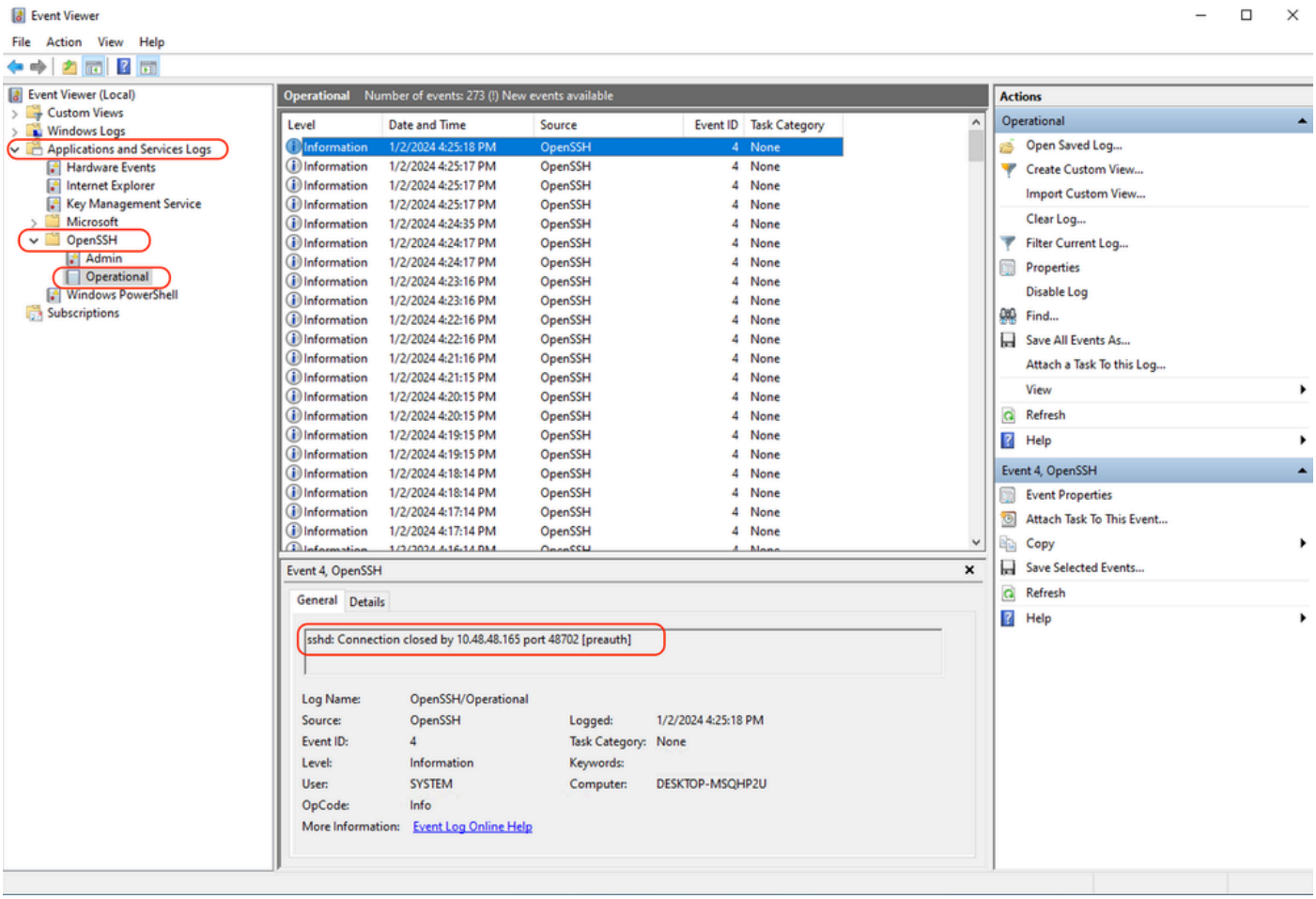
2. 系統日誌



註：要讀取system_logs，可在CLI中使用grep命令(在CLI中選擇與system_logs關聯的數字)，然後回答嚮導中的問題。

檢視SCP伺服器中的日誌

您可以在Microsoft事件檢視器中的應用程式和服務日誌 > OpenSSH > Operational中讀取SCP伺服器日誌



映像- PreAuth失敗

主機金鑰驗證失敗

此錯誤表示儲存在SWA中的SCP伺服器公鑰無效。

以下是CLI中displayalerts輸出的錯誤示例：

```
02 Jan 2024 16:52:35 +0100    Log Error: Push error for subscription scpal: SCP failed to transfer to 1
Last message occurred 68 times between Tue Jan  2 15:53:01 2024 and Tue Jan  2 16:52:31 2024.

Log Error: Push error for subscription scpal: SCP failed to transfer to 10.48.48.195:22: Host key verif
Last message occurred 46 times between Tue Jan  2 16:30:19 2024 and Tue Jan  2 16:52:31 2024.

Log Error: Push error for subscription scpal: SCP failed to transfer to 10.48.48.195:22: lost connectio
Last message occurred 68 times between Tue Jan  2 15:53:01 2024 and Tue Jan  2 16:52:31 2024.

Log Error: Push error for subscription scpal: SCP failed to transfer to 10.48.48.195:22: ssh: connect t
Last message occurred 22 times between Tue Jan  2 15:53:01 2024 and Tue Jan  2 16:29:18 2024.
```

以下是system_logs中一些錯誤的示例：

```
Tue Jan  2 19:49:50 2024 Critical: Log Error: Push error for subscription scp: SCP failed to transfer t
```

```
Tue Jan  2 19:49:50 2024 Critical: Log Error: Push error for subscription scp: SCP failed to transfer t
Tue Jan  2 19:49:50 2024 Critical: Log Error: Push error for subscription scp: SCP failed to transfer t
```

要解決此問題，可以從SCP伺服器複製主機，並將其貼上到SCP日誌訂閱頁面中。

請參閱配置SWA中的步驟7，從GUI將日誌傳送到SCP遠端伺服器，或者您可以聯絡Cisco TAC從後端刪除主機金鑰。

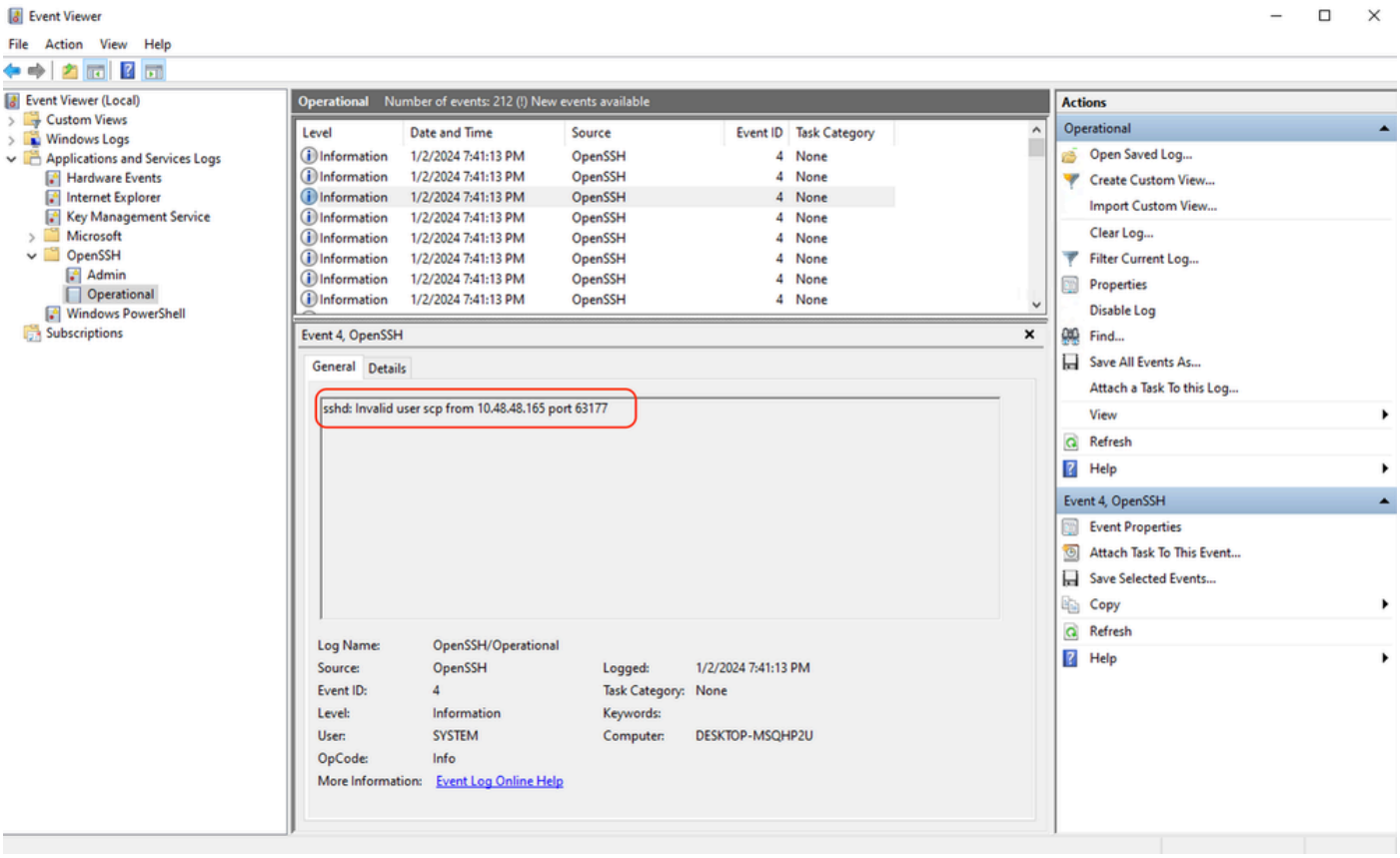
許可權被拒絕(publickey，password，keyboard-interactive)

此錯誤通常表示SWA中提供的使用者名稱無效。

以下是system_logs中的錯誤日誌示例：

```
Tue Jan  2 20:41:40 2024 Critical: Log Error: Push error for subscription scpal: SCP failed to transfer
Tue Jan  2 20:41:40 2024 Critical: Log Error: Push error for subscription scpal: SCP failed to transfer
Tue Jan  2 20:41:40 2024 Critical: Log Error: Push error for subscription scpal: SCP failed to transfer
```

以下是SCP伺服器的錯誤示例：<SWA_IP地址> port <TCP埠SWA連線到SCP伺服器>的使用者SCP無效



影象-無效使用者

要解決此錯誤，請檢查拼寫並驗證在SCP伺服器中啟用了使用者（在SWA中配置為推送日誌）。

沒有這樣的檔案或目錄

此錯誤表示SWA日誌訂閱區段中提供的路徑無效，

以下是system_logs的錯誤範例：

```
Tue Jan  2 20:47:18 2024 Critical: Log Error: Push error for subscription scpal: SCP failed to transfer
Tue Jan  2 20:47:18 2024 Critical: Log Error: Push error for subscription scpal: SCP failed to transfer
Tue Jan  2 20:47:18 2024 Critical: Log Error: Push error for subscription scpal: SCP failed to transfer
```

要解決此問題，請驗證拼寫，並確保路徑在SCP伺服器中正確有效。

SCP無法傳輸

此錯誤可能是通訊錯誤的指示。以下是錯誤範例：

```
03 Jan 2024 13:23:27 +0100    Log Error: Push error for subscription scp: SCP failed to transfer to 10.
```

要排除連線故障，請在SWA CLI中使用telnet命令：

```
SWA_CLI> telnet

Please select which interface you want to telnet from.
1. Auto
2. Management (10.48.48.187/24: SWA_man.csico.com)
[1]> 2

Enter the remote hostname or IP address.
[]> 10.48.48.195

Enter the remote port.
[23]> 22

Trying 10.48.48.195...
```

在本示例中，未建立連線。成功的連線輸出如下：

```
SWA_CLI> telnet

Please select which interface you want to telnet from.
1. Auto
2. Management (10.48.48.187/24: rishi2Man.calo.lab)
[1]> 2
Enter the remote hostname or IP address.
```

```
[]> 10.48.48.195
Enter the remote port.
[23]> 22

Trying 10.48.48.195...
Connected to 10.48.48.195.
Escape character is '^]'.
SSH-2.0-OpenSSH_for_Windows_SCP
```

如果telnet未連線：

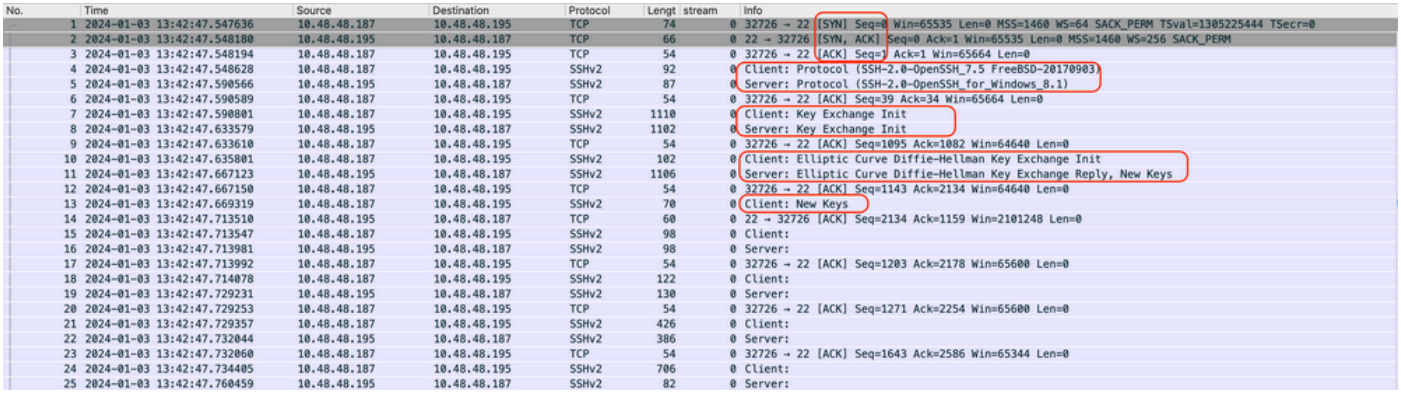
[1]檢查SCP伺服器防火牆是否阻止訪問。

[2]檢查從SWA到SCP伺服器的路徑中是否有防火牆阻止訪問。

[3]檢查SCP伺服器中的TCP埠22是否處於偵聽狀態。

[4]在兩個SWA和SCP伺服器中運行資料包捕獲以進行進一步分析。

以下是成功連線的封包擷取範例：



No.	Time	Source	Destination	Protocol	Lengt	stream	Info
1	2024-01-03 13:42:47.547636	10.48.48.187	10.48.48.195	TCP	74	0	32726 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM TSval=1305225444 TSecr=0
2	2024-01-03 13:42:47.548180	10.48.48.195	10.48.48.187	TCP	66	0	22 → 32726 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
3	2024-01-03 13:42:47.548194	10.48.48.187	10.48.48.195	TCP	54	0	32726 → 22 [ACK] Seq=1 Ack=1 Win=65664 Len=0
4	2024-01-03 13:42:47.548628	10.48.48.187	10.48.48.195	SSHv2	92	0	Client: Protocol (SSH-2.0-OpenSSH_7.5 FreeBSD-20170903)
5	2024-01-03 13:42:47.590566	10.48.48.195	10.48.48.187	SSHv2	87	0	Server: Protocol (SSH-2.0-OpenSSH_for_Windows_8.1)
6	2024-01-03 13:42:47.590589	10.48.48.187	10.48.48.195	TCP	54	0	32726 → 22 [ACK] Seq=39 Ack=34 Win=65664 Len=0
7	2024-01-03 13:42:47.590801	10.48.48.187	10.48.48.195	SSHv2	1110	0	Client: Key Exchange Init
8	2024-01-03 13:42:47.633579	10.48.48.195	10.48.48.187	SSHv2	1102	0	Server: Key Exchange Init
9	2024-01-03 13:42:47.633610	10.48.48.187	10.48.48.195	TCP	54	0	32726 → 22 [ACK] Seq=1095 Ack=1082 Win=64640 Len=0
10	2024-01-03 13:42:47.635801	10.48.48.187	10.48.48.195	SSHv2	102	0	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
11	2024-01-03 13:42:47.667123	10.48.48.195	10.48.48.187	SSHv2	1106	0	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys
12	2024-01-03 13:42:47.667150	10.48.48.187	10.48.48.195	TCP	54	0	32726 → 22 [ACK] Seq=1143 Ack=2134 Win=64640 Len=0
13	2024-01-03 13:42:47.669319	10.48.48.187	10.48.48.195	SSHv2	70	0	Client: New Keys
14	2024-01-03 13:42:47.713510	10.48.48.195	10.48.48.187	TCP	60	0	22 → 32726 [ACK] Seq=2134 Ack=1159 Win=2101248 Len=0
15	2024-01-03 13:42:47.713547	10.48.48.187	10.48.48.195	SSHv2	98	0	Client:
16	2024-01-03 13:42:47.713981	10.48.48.195	10.48.48.187	SSHv2	98	0	Server:
17	2024-01-03 13:42:47.713992	10.48.48.187	10.48.48.195	TCP	54	0	32726 → 22 [ACK] Seq=1203 Ack=2178 Win=65600 Len=0
18	2024-01-03 13:42:47.714078	10.48.48.187	10.48.48.195	SSHv2	122	0	Client:
19	2024-01-03 13:42:47.729231	10.48.48.195	10.48.48.187	SSHv2	130	0	Server:
20	2024-01-03 13:42:47.729253	10.48.48.187	10.48.48.195	TCP	54	0	32726 → 22 [ACK] Seq=1271 Ack=2254 Win=65600 Len=0
21	2024-01-03 13:42:47.729357	10.48.48.187	10.48.48.195	SSHv2	426	0	Client:
22	2024-01-03 13:42:47.732044	10.48.48.195	10.48.48.187	SSHv2	386	0	Server:
23	2024-01-03 13:42:47.732060	10.48.48.187	10.48.48.195	TCP	54	0	32726 → 22 [ACK] Seq=1643 Ack=2586 Win=65344 Len=0
24	2024-01-03 13:42:47.734405	10.48.48.187	10.48.48.195	SSHv2	706	0	Client:
25	2024-01-03 13:42:47.760459	10.48.48.195	10.48.48.187	SSHv2	82	0	Server:

映像-成功捕獲連線資料包

參考資料

思科網路安全裝置最佳實踐指南-思科

BRKSEC-3303 (ciscolive)

Cisco Secure Web Appliance的AsyncOS 14.5使用手冊- GD（常規部署）-連線、安裝和配置[Cisco Secure Web Appliance] -思科

開始使用OpenSSH for Windows | Microsoft學習

在Windows上配置SSH公鑰身份驗證 | Windows OS中心(woshub.com)

OpenSSH for Windows中的基於金鑰的身份驗證 | Microsoft學習

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）。