WSA日誌傳輸到遠端SCP伺服器

目錄

<u>簡介</u> <u>必要條件</u> <u>需採用元件</u> <u>驗</u>難 類 難 難解

簡介

本檔案介紹如何將日誌從思科網路安全裝置(WSA)傳輸到遠端安全複製(SCP)伺服器。您可以配置 WSA日誌,例如訪問日誌和身份驗證日誌,以便在日誌滾動或包裝時使用SCP協定將其轉發到外部 伺服器。

本文檔中的資訊介紹了如何配置日誌旋轉規則以及成功傳輸到SCP伺服器所需的安全外殼(SSH)金 鑰。

必要條件

需求

本文件沒有特定需求。

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。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

設定

完成以下步驟以配置WSA日誌,以便可以在遠端伺服器上使用SCP檢索這些日誌:

1. 登入到WSA Web GUI。

2. 導航到系統管理 > 日誌訂閱。

3. 選擇要為其配置此檢索方法的日誌的名稱,例如**訪問日誌**。

4. 在「檢索方法」欄位中,選擇Remote Server上的SCP。

5. 輸入SCP伺服器的SCP主機名或IP地址。

6. 輸入SCP埠號。

附註:預設設定為埠22。

- 7. 輸入要將日誌傳送到的SCP伺服器目標目錄的完整路徑名。
- 8. 輸入SCP伺服器驗證使用者的使用者名稱。
- 9. 如果要自動掃描主機金鑰或手動輸入主機金鑰,請啟用**主機金鑰檢查**。
- 10. 按一下「Submit」。您即將置入SCP伺服器authorized_keys檔案中的SSH金鑰現在應顯示在「編輯日誌訂閱」(Edit Log Subscription)頁面的頂部。以下是WSA中一條成功消息的示例:

Reporting	Web Security Manager	Security Services	Network	System Administration	
					Commit Changes =
Log Subscri	ptions				
Success - Log S	ubscription "accesslogs" was ch	anged.			
Pleas	a place the following SSH key(s)) into your authorized_key	s file on the remot	e host so that the log files can be uploaded.	
ssh-d AAAA root@	ss B3NzaC1kc3MAAACBAPL9nUx1 mgmt.s670j.lab	5KI7FL+YcsAeFKit833NKV	oW1tdndQdAVt2D	7aSmLoHOSFgrFqfrGvXPP18qUIYISUOQN7R7	kGlAvnIfAM7GwdG1vUdyyI7q14SL0UgOnElv

- 11. 按一下Commit Changes。
- 12. 如果SCP伺服器是Linux或Unix伺服器或Macintosh電腦,則從WSA將SSH金鑰貼上到SSH目 錄中的authorized_keys檔案中:

導航到Users > <username> > .ssh目錄。

將WSA SSH金鑰貼上到authorized_keys檔案中並儲存更改。 附註:如果SSH目錄中不存在authorized_keys檔案,則必須手動建立該檔案。

驗證

完成以下步驟,確認日誌是否成功傳輸到SCP伺服器:

- 1. 導航到WSA Log Subscriptions頁。
- 2. 在Rollover列中,選擇為SCP檢索配置的日誌。
- 3. 找到並按一下Rollover Now。
- 4. 導航到為日誌檢索配置的SCP伺服器資料夾,並驗證日誌是否已傳輸到該位置。

完成以下步驟,以監控從WSA到SCP伺服器的日誌傳輸:

- 1. 通過SSH登入WSA CLI。
- 2. 輸入grep命令。
- 3. 輸入要監控的日誌的相應編號。例如,從system_logs的grep清單中輸入31。
- 4. 在*Enter the regular expression to grep*提示符下輸入**scp**,以便過濾日誌,以便只監視SCP事務。
- 5. 在是否希望此搜尋不區分大小寫?提示。
- 6. 在Do you want to trail the logs?(是否要跟蹤日誌?)提示。
- 7. 在*Do you want to pagate the output?(是否要對輸出進行分頁?)處輸入*N提示。然後 WSA即時列出SCP事務。以下是來自WSA system_logs的成功SCP事務的示例:

Wed Jun 11 15:06:14 2014 Info: Push success for subscription <the name of the log>: Log aclog@20140611T145613.s pushed to remote host <IP address of the SCP Server>:22

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。