# 在安全工作負載上生成快照檔案(Tetration)

## 目錄



## 簡介

本文檔介紹如何在思科安全工作負載(Tetration)上為不同型別的日誌收集生成快照捆綁檔案。

## 必要條件

### 採用元件

思科建議您瞭解以下產品：

- 思科安全工作負載(Tetration)
- 思科整合式管理控制器(CIMC)

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。

> **附註**： 您必須具有客戶支援角色才能訪問快照工具。

> **警告**：本文檔中的說明適用於運行軟體版本3.4.1.x或更高版本的思科安全工作負載(Tetration)。

用於確定Tetration群集的硬體、軟體和整合的狀態的快照捆綁包包括：

- 經典快照捆綁包：收集 群集相關資料的日誌消息、配置資料、命令輸出、警報、時序資料庫(tsdb)等的收集。
- CIMC快照捆綁包：從統一計算系統(UCS)收集技術支援檔案，適用於硬體裝置(8RU、39RU)群

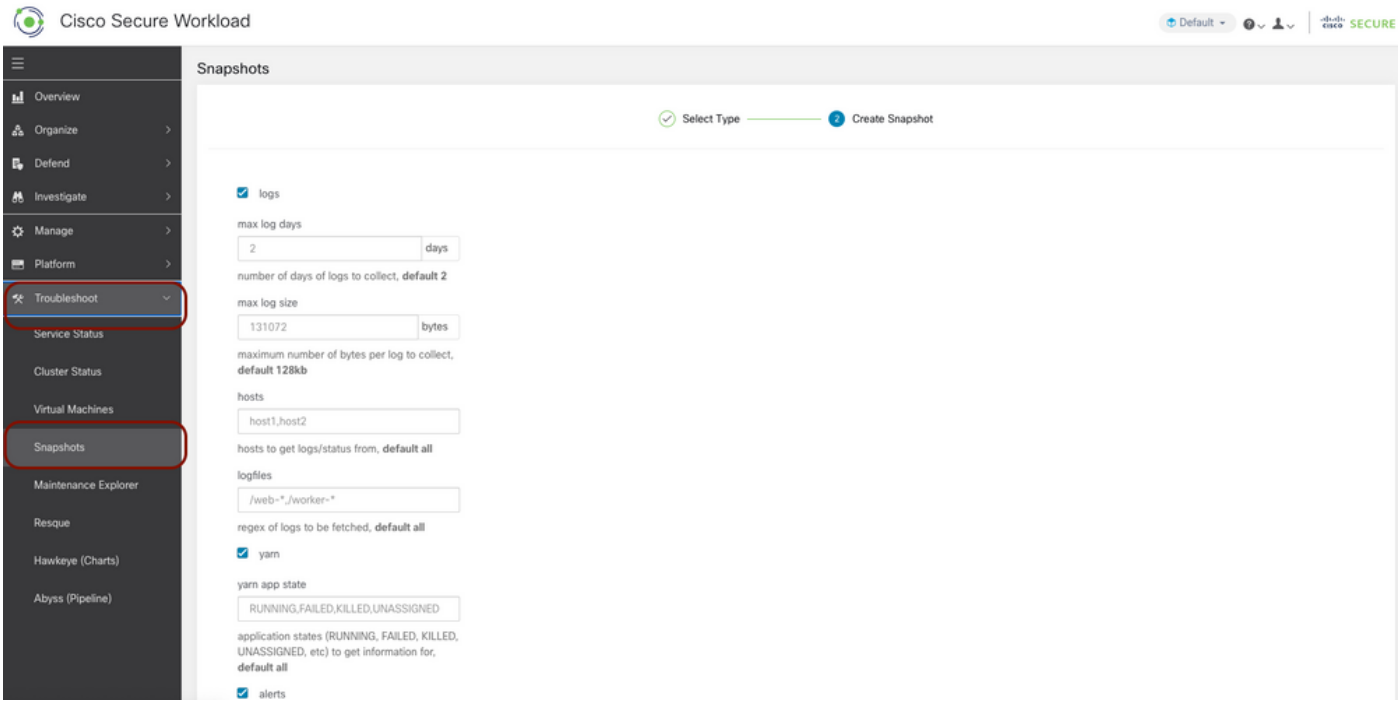
集。
- 軟體代理捆綁包：包含安裝在遙測資料收集終端系統上的Tetration代理的日誌。
- 虛擬裝置聯結器套件：包含來自Tetration Virtual裝置的日誌，該裝置支援流量擷取、資產豐富和警報通知。

如果思科工程師請求您從安全工作負載集群傳送快照捆綁包，則可以使用本文檔中提供的說明。

# 收集快照捆綁包

## 生成經典快照捆綁包

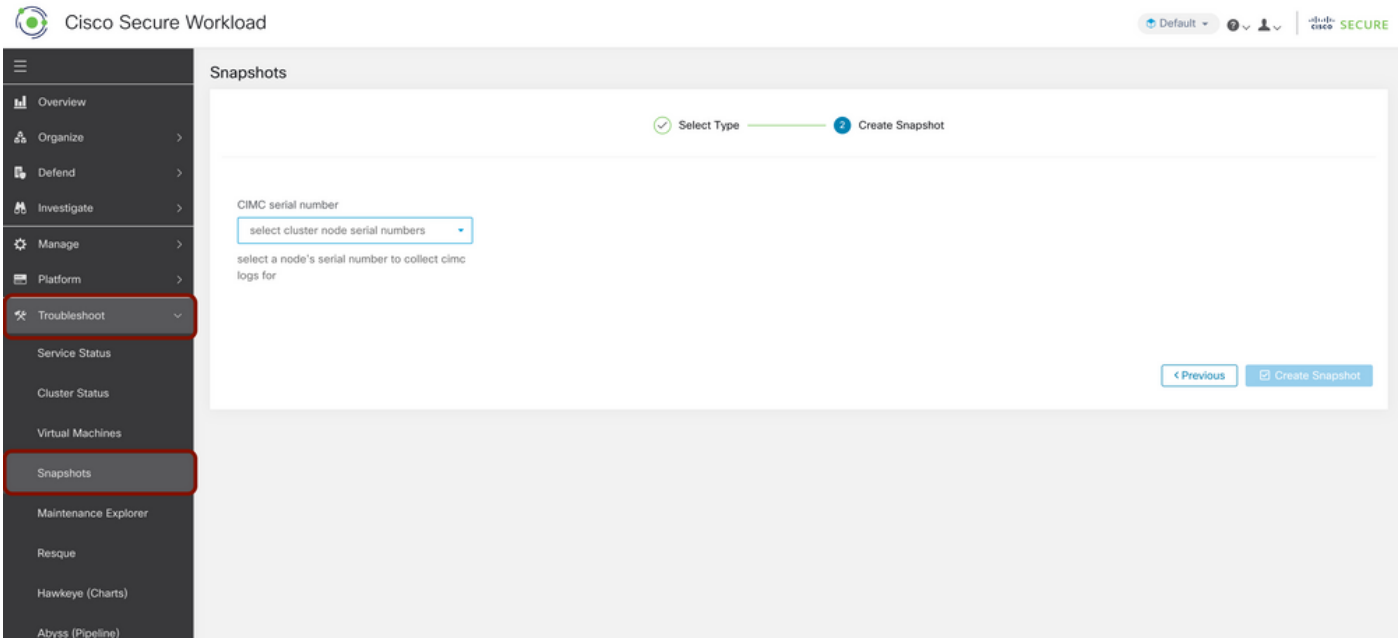
登入到安全工作負載使用者介面(UI)，導航到左側導航面板，然後選擇**故障排除>快照** [**維護>快照**（3.4.x或3.5.x）]選項。按一下**Create Snapshot**，然後選擇**Classic Snapshot**。此時將顯示帶有預設選項的快照頁面。如果Cisco TAC工程師明確要求您，則可覆寫預設選項。




向下滾動到頁面底部，並使用註釋部分指定案例編號或問題描述，然後按一下**建立快照**以啟動生成經典快照捆綁的過程。可能需要一段時間才能完成快照生成。一旦快照生成達到100%，請按一下**下載**以下載經典快照捆綁包。向下滾動以取得將檔案上傳到案件編號的選項。

## 生成CIMC捆綁包

登入到安全工作負載UI，導航到左側導航面板，然後選擇**故障排除>快照** [**維護>快照**（3.4.x或3.5.x）]。按一下**Create Snapshot**，然後選擇**CIMC Snapshot**。系統將顯示CIMC快照頁面，其中帶有用於選擇節點序列號的下拉選項。搜尋或選擇節點，然後按一下**建立快照**以啟動生成CIMC快照捆綁的過程。




可能需要一段時間才能完成快照生成。快照生成達到100%後，按一下**Download**下載CIMC快照捆綁包。向下滾動以取得將檔案上傳到案件編號的選項。

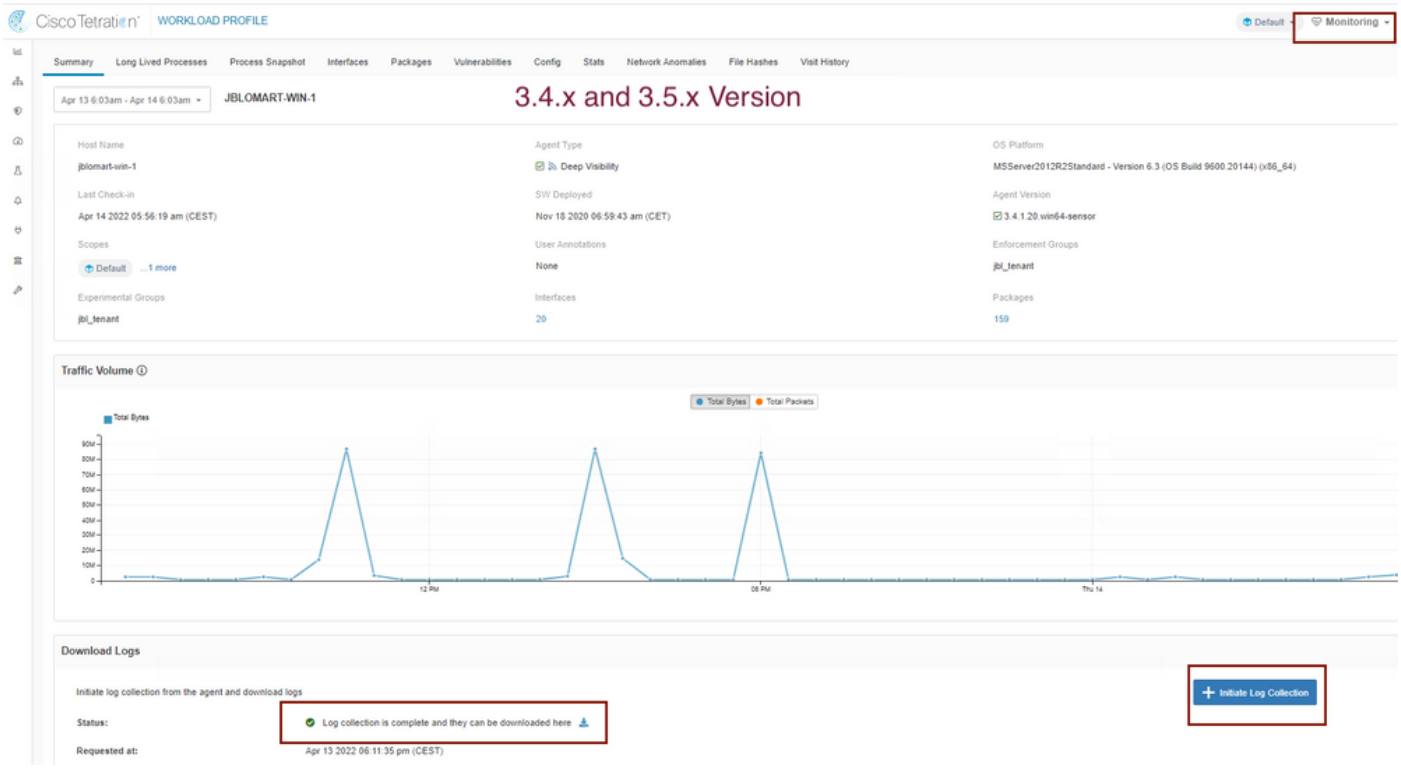
## 生成Tetration代理日誌聚結

為了收集日誌聚結，Tetration代理必須處於活動狀態。

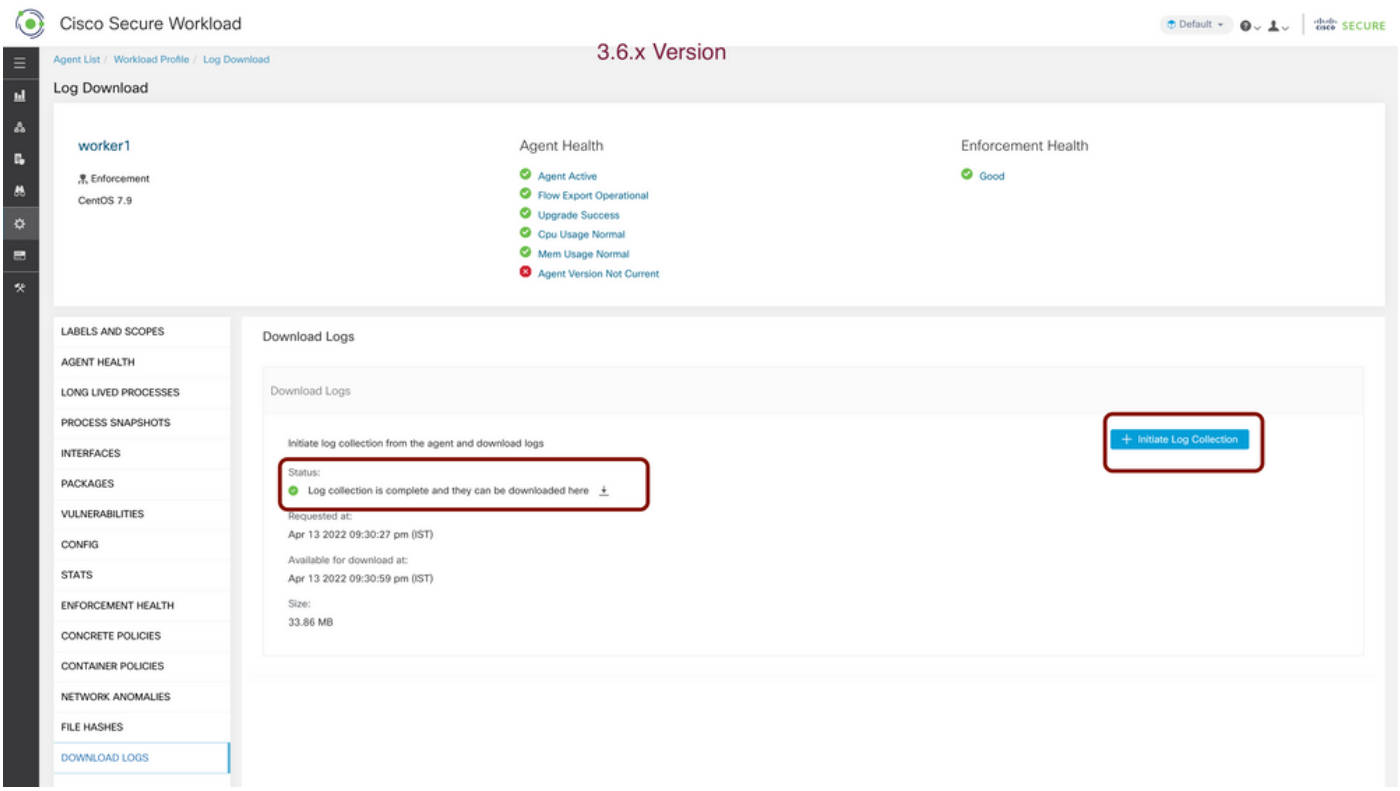
- 對於3.6.x版本，導航到左側導航面板，選擇**Manage > Agent**，然後點選**Agent List**。
- 對於3.4.x和3.5.x版本，從右上下拉選單導航到**Monitoring**，然後選擇**Agent List**。

使用過濾器選項搜尋代理，然後按一下**Agent**。它將您帶到代理的工作量配置檔案。您可以在此處找到有關代理配置、狀態等的詳細資訊。

在工作負載配置檔案頁面(3.6.x)的左側導航面板上，選擇**Download Logs**（在3.4.x和3.5.x中，並按照summary頁籤操作）。 按一下**Initiate Log Collection**，從Tetration Agent啟動日誌收集。可能需要一段時間才能完成日誌收集。日誌收集完成後，按一下**Download here**選項下載日誌。向下滾動以取得將檔案上傳到案件編號的選項。




*3.4.x和3.5.x版本*




*3.6.x版本*

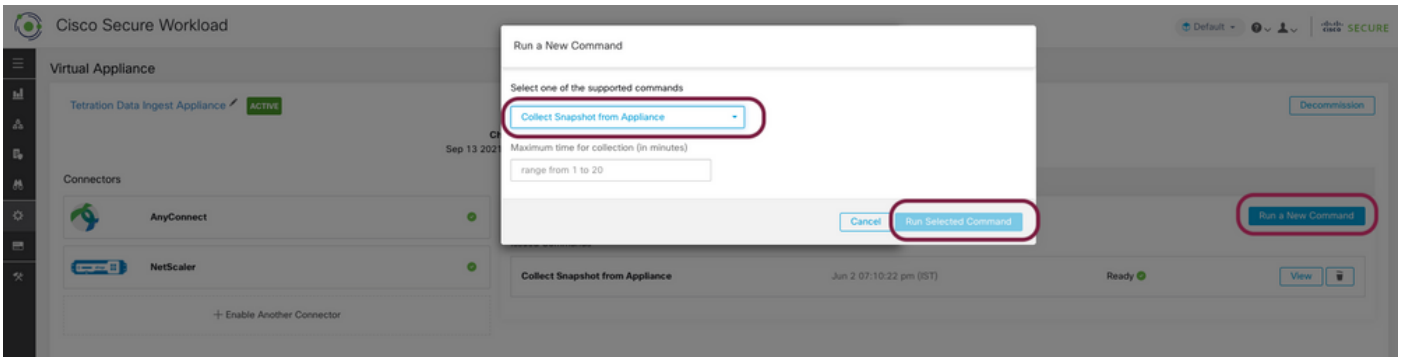
## 生成虛擬裝置聯結器快照捆綁包

要獲取虛擬裝置的快照捆綁包，您需要確保虛擬裝置處於Active狀態。

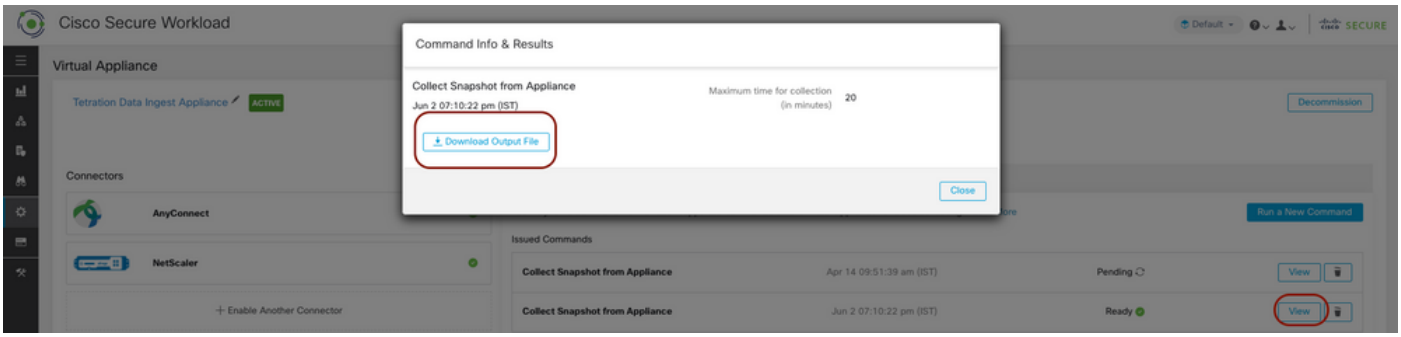
- 對於3.6.x版本，導航到左側導航面板，然後選擇**管理>虛擬裝置**。
- 對於3.4.x和3.5.x版本，導航到左側導航面板，然後選擇Connectors > Virtual Appliance。

選擇要為其生成快照捆綁包的虛擬裝置。按一下「Troubleshoot」，然後再次按一下「Troubleshoot」選項。按一下**運行新命令**，此時將開啟一個對話方塊。該對話方塊有一個下拉選單

來選擇命令。從下拉選單中，選擇**從裝置收集快照**並指定時間範圍（以分鐘為單位，例如，20分鐘），然後按一下**Run Selected Command**。它啟動從虛擬裝置收集快照捆綁的過程。從虛擬裝置收集日誌捆綁包可能需要一段時間。




快照捆綁包的收集完成後，按一下**檢視**以下載快照捆綁包。向下滾動以取得將檔案上傳到案件編號的選項。




# 將套件組合上傳到思科服務請求(SR)

有多種方法可將快照套件組合上傳到案件(SR)。 如需詳細資訊，請檢查Customer File Uploads to the Cisco Technical Assistance Center頁面。

- 思科安全工作負載(Tetration)
- Cisco Secure Workload(Tetration)產品概述
- **技術支援與文件 - Cisco Systems**