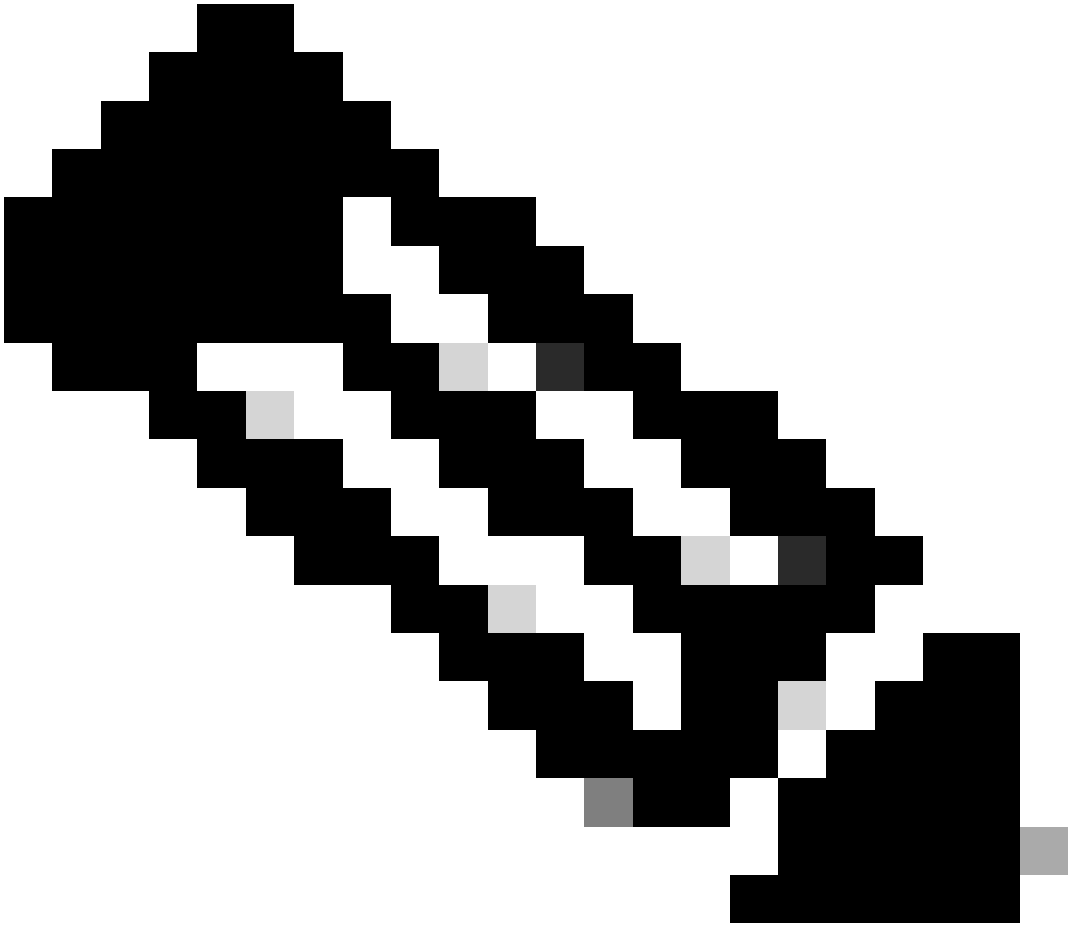
收集XDR調查分析模組的日誌

目錄

簡介

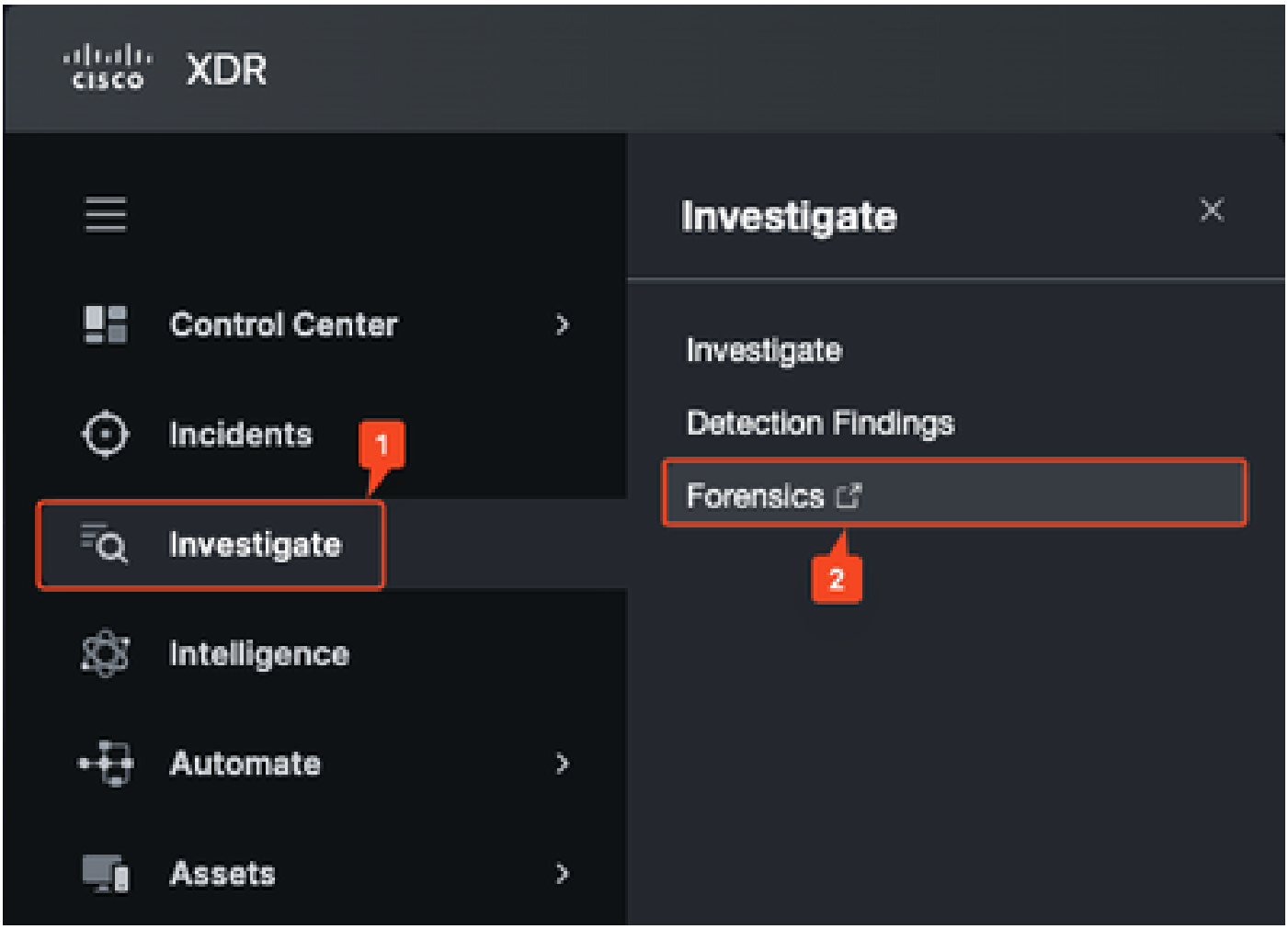
本文檔介紹如何遠端獲取診斷資料以排除XDR取證模組在其控制檯中的故障。

正在遠端獲取日誌



附註：目前，DART日誌不包含XDR取證日誌。

步驟1.開啟XDR並導航至Investigate > Forensics控制台。



步驟2.導航到Assets頁，驗證終端的主機名是否在Assets頁面可見。為此，請執行以下操作：

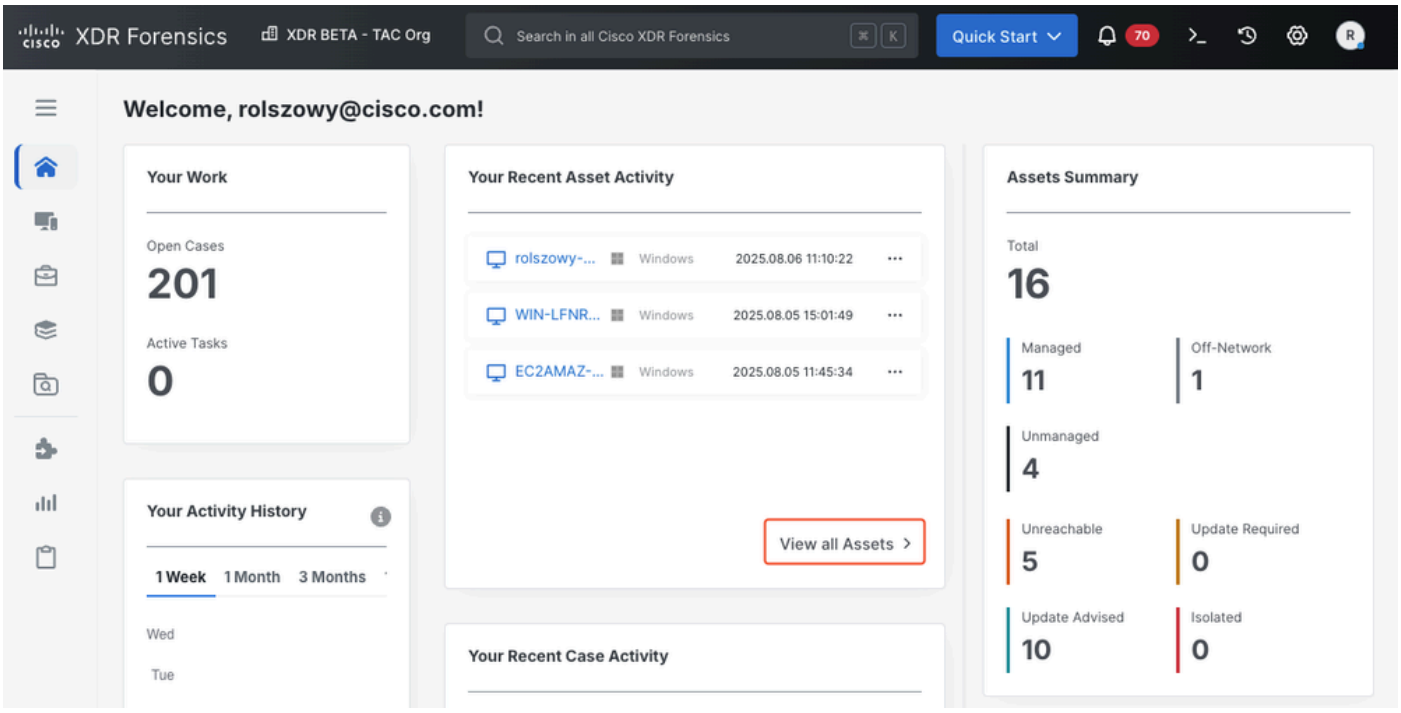
a)在給定電腦上開啟CMD並執行hostname命令。

<#root>

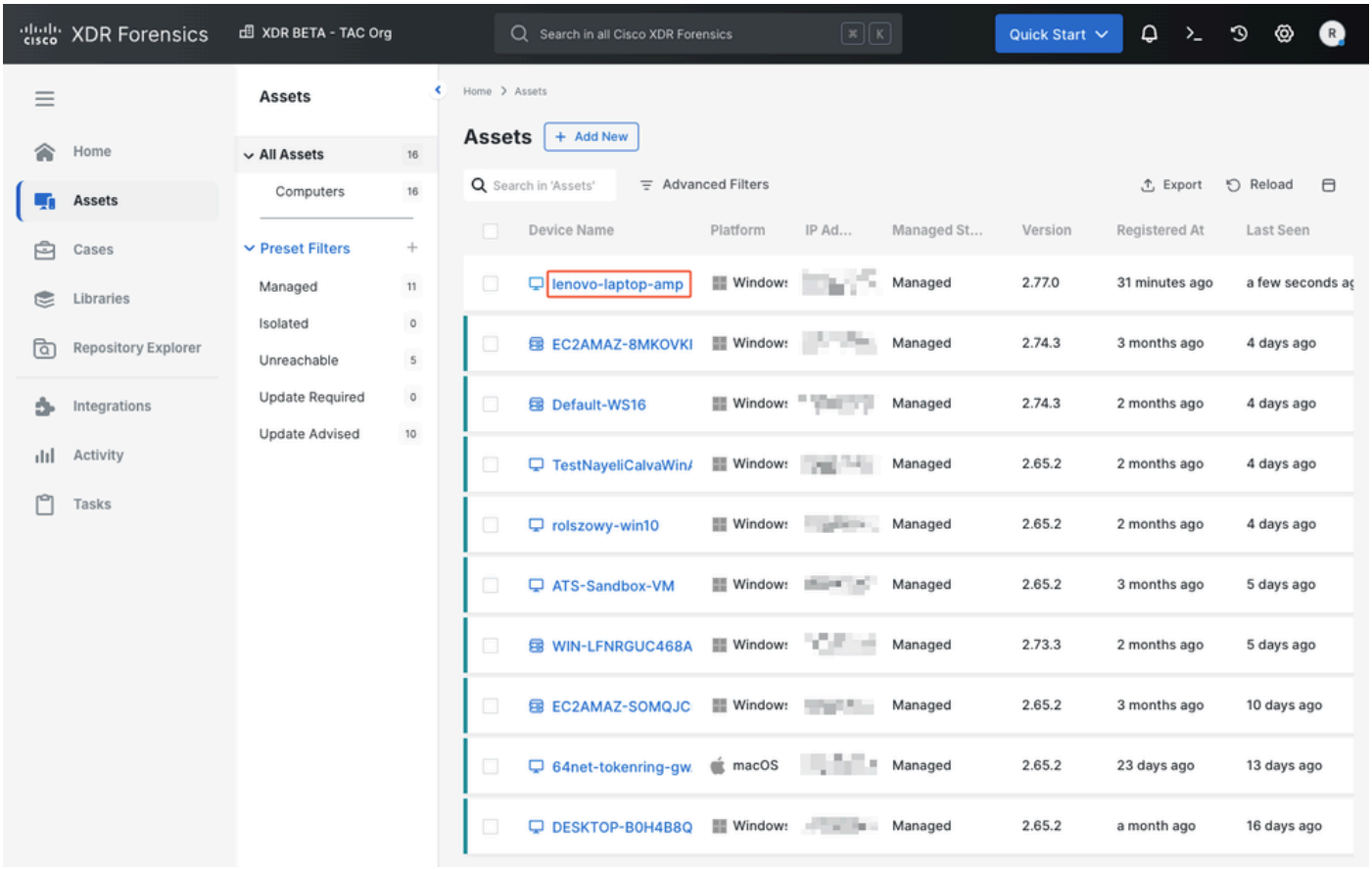
```
C:\Users\Admin\
hostname

lenovo-laptop-amp
```

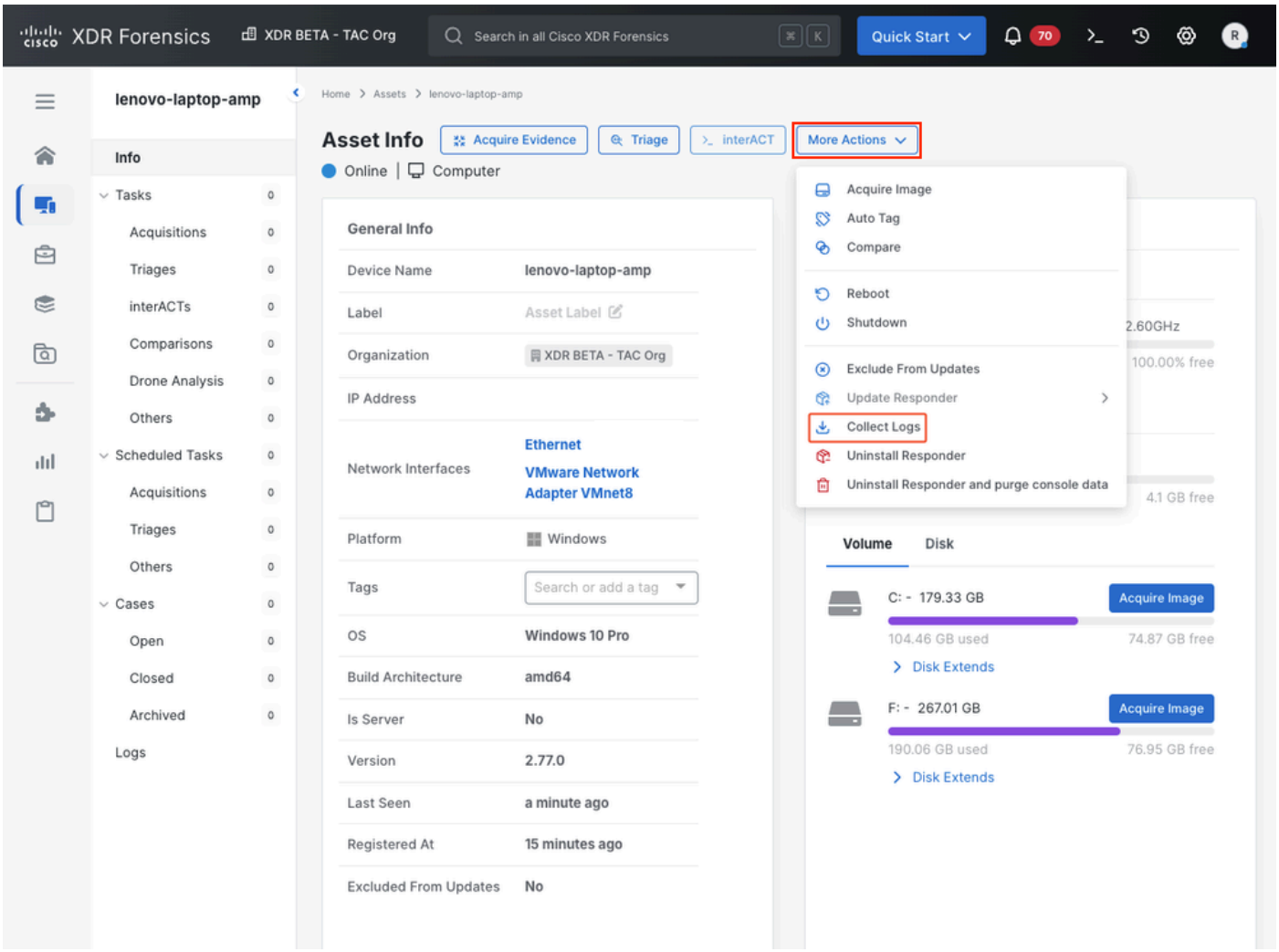
b)在XDR Forensics Console主頁中，按一下View all Assets(或使用左側的Assets選單)。

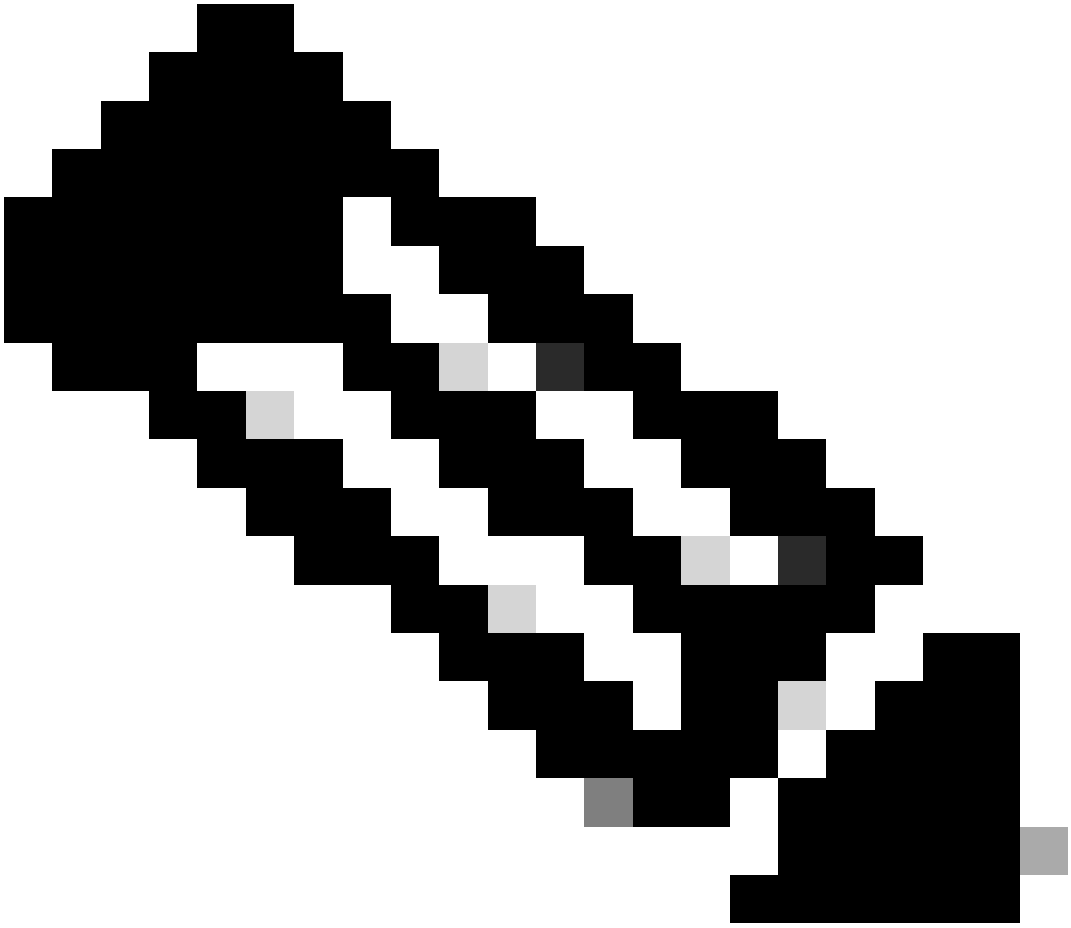


c)對清單中的終端進行本地化，然後按一下Device name以輸入其詳細資訊。



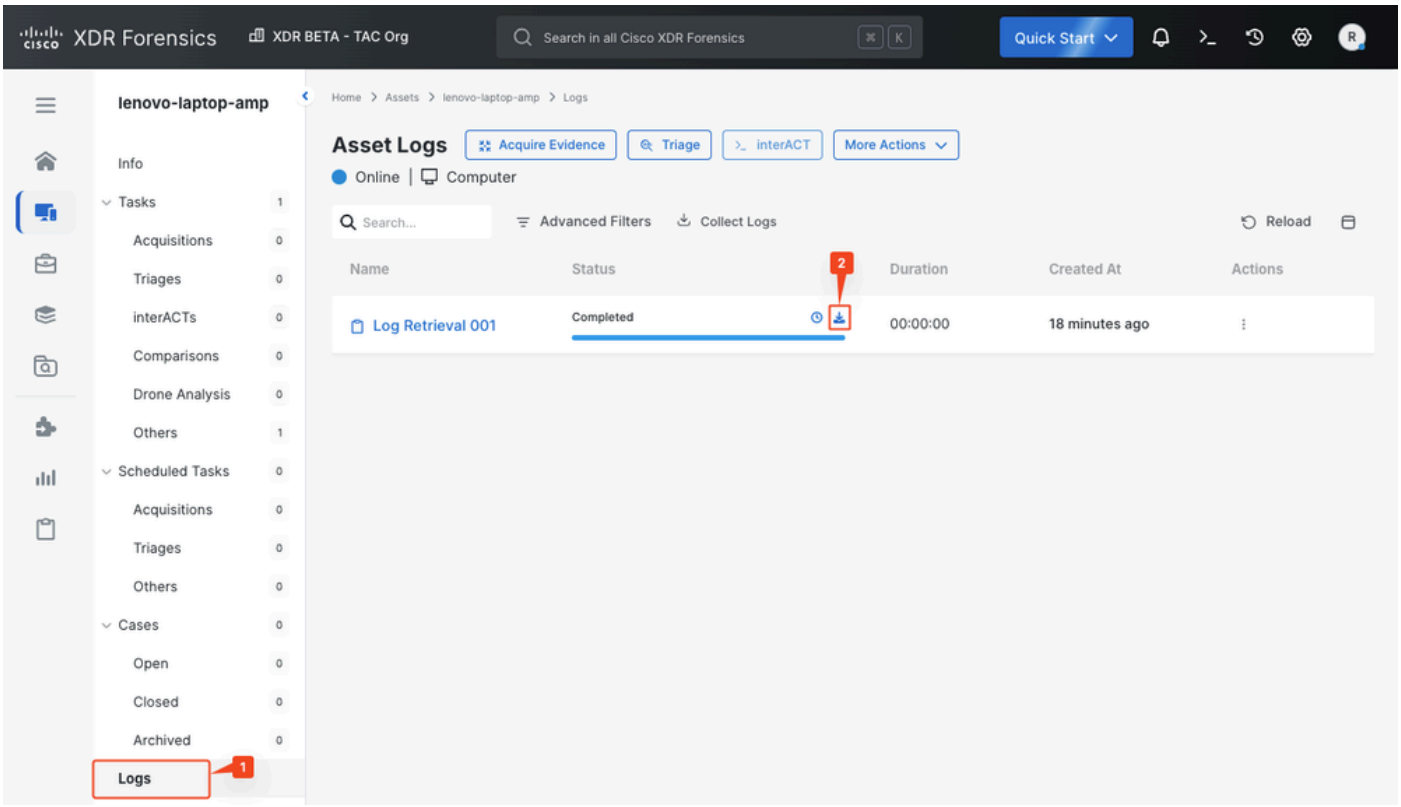
步驟3.在Asset info頁面中，按一下More Actions > Collect Logs，開始從端點收集資訊。


XDR Forensics
XDR BETA - TAC Org
Search in all Cisco XDR Forensics
Quick Start
70
lenovo-laptop-amp
Info
Tasks 0
Acquisitions 0
Triages 0
interACTs 0
Comparisons 0
Drone Analysis 0
Others 0
Scheduled Tasks 0
Acquisitions 0
Triages 0
Others 0
Cases 0
Open 0
Closed 0
Archived 0
Logs
Home > Assets > lenovo-laptop-amp
Asset Info
Acquire Evidence
Triage
interACT
More Actions
Online | Computer
General Info
Device Name lenovo-laptop-amp
Label Asset Label
Organization XDR BETA - TAC Org
IP Address
Network Interfaces Ethernet
VMware Network Adapter VMnet8
Platform Windows
Tags Search or add a tag
OS Windows 10 Pro
Build Architecture amd64
Is Server No
Version 2.77.0
Last Seen a minute ago
Registered At 15 minutes ago
Excluded From Updates No
Acquire Image
Auto Tag
Compare
Reboot
Shutdown
Exclude From Updates
Update Responder
Collect Logs
Uninstall Responder
Uninstall Responder and purge console data
2.60GHz
100.00% free
4.1 GB free
Volume
Disk
C: - 179.33 GB
Acquire Image
104.46 GB used
74.87 GB free
Disk Extends
F: - 267.01 GB
Acquire Image
190.06 GB used
76.95 GB free
Disk Extends



附註：如果資產處於聯機狀態，則此操作需要幾秒鐘才能完成。

步驟4.轉到日誌部分以檢視是否已收集日誌。在Asset Logs部分，按一下圖示開始下載日誌。

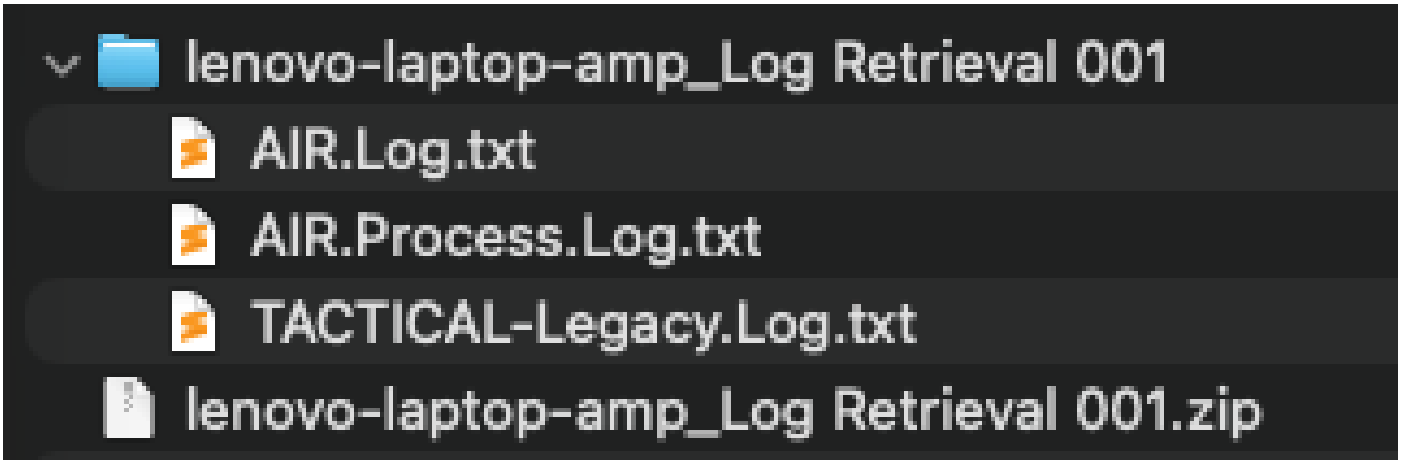


步驟5.獲得的*.zip檔案包含對模組進行故障排除所需的三個檔案：

-AIR.Log.txt

-AIR.Process.Log.txt

-TACTICAL-Legacy.Log.txt



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）。