鑑識
Data Infrastructure Insights

NetApp
January 17, 2025

目錄

鑑識

鑑識-所有活動

「所有活動」頁面可協助您瞭解在工作負載安全性環境中、對實體所執行的行動。

檢查所有活動資料

按一下「鑑識」>「活動鑑識」、然後按一下「所有活動」索引標籤以存取「所有活動」頁面。本頁提供租戶活動的概觀，並強調下列資訊：

- 顯示 _ 活動歷程記錄 _ 的圖表（根據所選的整體時間範圍）

  您可以在圖表中拖曳矩形來縮放圖表。將載入整個頁面以顯示縮放時間範圍。放大時、會顯示可讓使用者縮小的按鈕。

- _ 所有活動 _ 資料的清單。
- 群組依據下拉式清單將提供選項，可依使用者，路徑，實體類型等來分組活動
- 在表格上方會出現一個通用路徑按鈕，我們可以在表格上方取得內含實體路徑詳細資料的滑出面板。

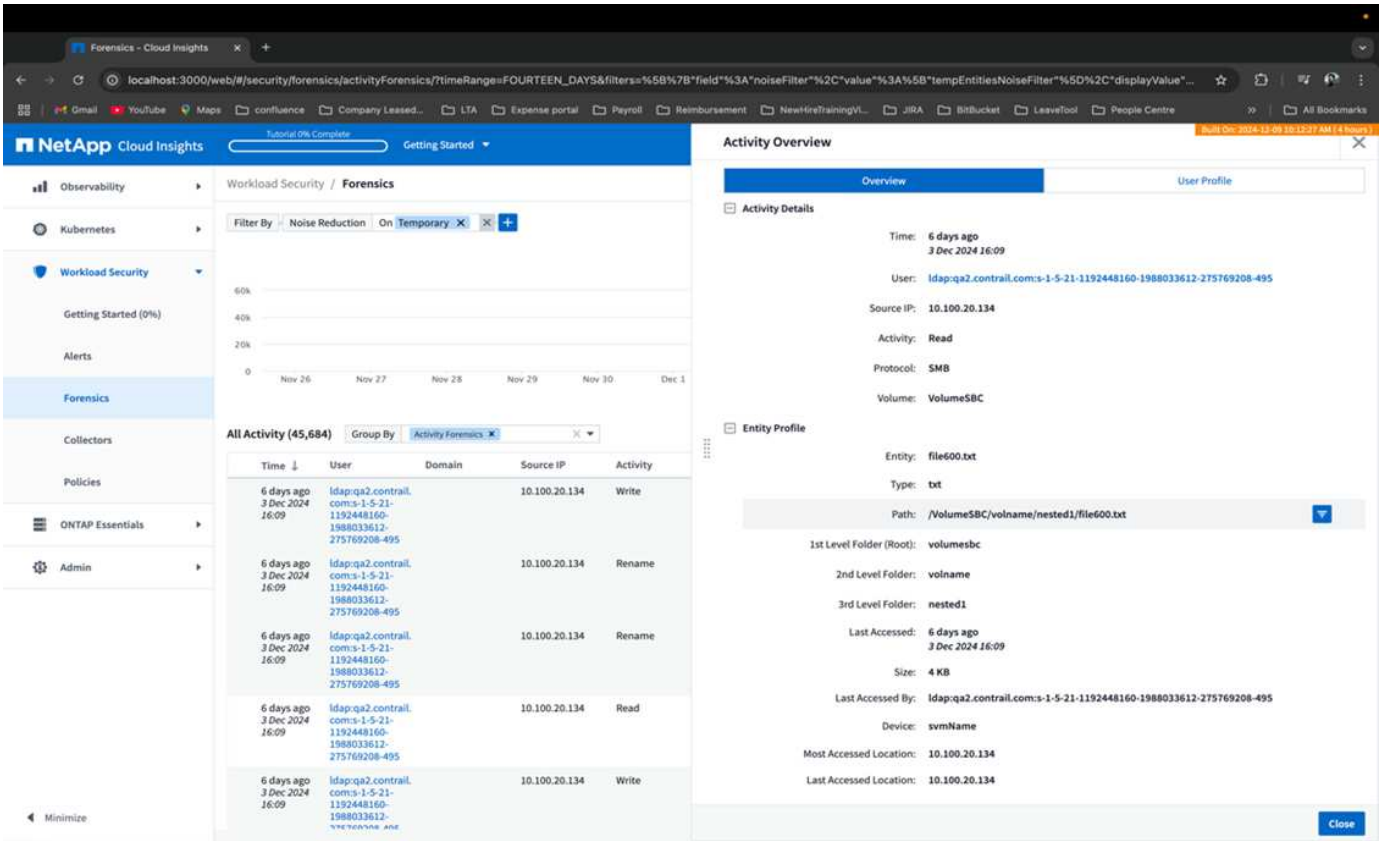
「_*所有活動*」表格顯示下列資訊。請注意、並非所有這些欄都會預設顯示。您可以按一下「齒輪」圖示來選取要顯示的欄。

- 存取實體的*時間*、包括上次存取的年、月、日和時間。
- 以滑出式面板連結存取實體的 * 使用者 * "使用者資訊"。
- 使用者執行的*活動*。支援的類型包括：
  - 變更群組擁有權：群組擁有權屬於檔案或資料夾。如需群組擁有權的詳細資訊，請參閱"此連結。"
  - 變更擁有者：檔案或資料夾的擁有權變更為其他使用者。
  - 變更權限-檔案或資料夾權限已變更。
  - 建立-建立檔案或資料夾。
  - 刪除-刪除檔案或資料夾。如果刪除資料夾、則會針對該資料夾和子資料夾中的所有檔案取得_DELETE _事件。
  - 讀取-檔案已讀取。
  - 讀取中繼資料：僅適用於啟用資料夾監控選項。將在Windows上開啟資料夾或在Linux資料夾內執行「ls」時產生。
  - 重新命名-重新命名檔案或資料夾。
  - 寫入-資料寫入檔案。
  - 寫入中繼資料-寫入檔案中繼資料、例如權限已變更。
  - 其他變更：上述未提及的任何其他事件。所有未對應的事件都會對應至「其他變更」活動類型。適用於檔案和資料夾。
- **Path** 是 *entity* 路徑。這應該是確切的實體路徑（例如「 */home/userX/nested1/nested2/abc.txt* 」），或是遞迴搜尋路徑的目錄部分（例如「 *_/home/userX/nested1/nested2/* 」）。注意：此處不允許 regex 路徑模

式（例如 *userX* ）。或者，也可以指定如下所述的個別路徑資料夾層級篩選器來進行路徑篩選。

- * 第一層資料夾（根目錄） * 是實體路徑的根目錄（小寫）。
- * 第二層資料夾 * 是實體路徑的第二層目錄（以較低的大小寫表示）。
- * 第三層資料夾 * 是實體路徑的第三層目錄（以較低的大小寫表示）。
- * 第四層資料夾 * 是實體路徑的第四層目錄（以較低的大小寫表示）。
- * 實體類型 * ，包括實體（例如檔案）副檔名（ .doc ， .docx ， .tmp 等）。
- 實體所在的 * 裝置 * 。
- 用於擷取事件的*傳輸協定*。
- 當原始檔案重新命名時、用於重新命名事件的*原始路徑*。根據預設、此欄在表格中不可見。使用欄選取器將此欄新增至表格。
- 實體所在的* Volume *。根據預設、此欄在表格中不可見。使用欄選取器將此欄新增至表格。

選取表格列會開啟滑出面板，其中一個索引標籤中會顯示使用者設定檔，另一個索引標籤則會顯示活動和實體總覽。



預設 _ 群組依據 _ 方法為 _ 活動鑑識 _ 。如果您選取不同的 _ 群組依據 _ 方法（例如，實體類型），則會顯示實體 _ 群組依據 _ 表格。如果沒有選擇，則會顯示 _Group by * all* 。

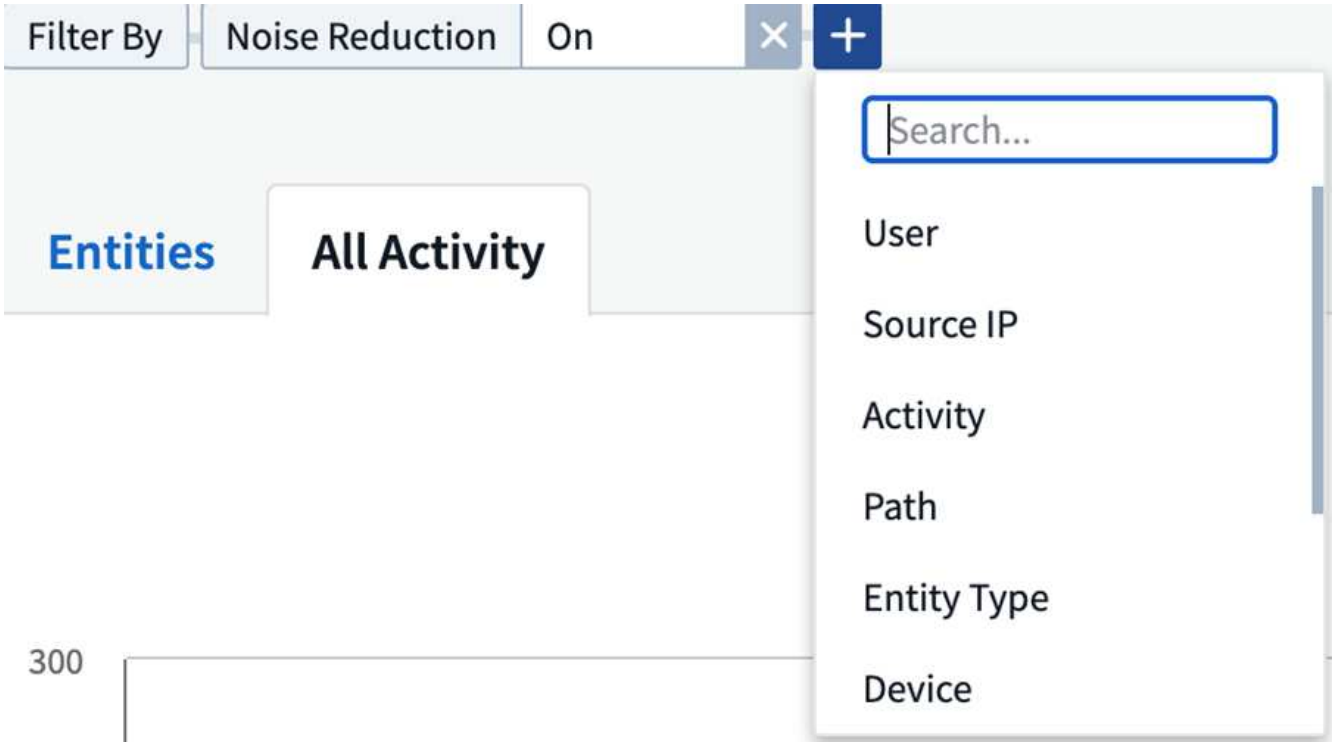
- 活動計數會顯示為超連結；選取此選項會將選取的群組新增為篩選。活動表會根據該篩選條件更新。
- 請注意，如果您變更篩選條件，變更時間範圍或重新整理畫面，則必須重新設定篩選條件，才能返回篩選結果。

篩選取證活動歷程記錄資料

您可以使用兩種方法來篩選資料。

- 可以從滑出面板新增篩選器。此值會新增至頂端_Filter by（篩選條件）清單中的適當篩選條件。
- 輸入「篩選條件」欄位以篩選資料：

  按一下「**+**」按鈕、從頂端的「篩選條件」小工具中選取適當的篩選條件：



  輸入搜尋文字

  按Enter或按一下篩選方塊外側以套用篩選條件。

您可以依下列欄位篩選取證活動資料：

- *活動*類型。
- 存取實體的來源**IP**。您必須以雙引號提供有效的來源IP位址、例如「10.1.1.1」。不完整的IP（例如"10.1.1. **"**、**"10.1.**.*"等）將無法運作。
- *傳輸協定*以擷取特定傳輸協定的活動。
- 執行活動的使用者名稱。您需要提供確切的使用者名稱以進行篩選。無法使用部分使用者名稱進行搜尋、或是以「*」為前置或後置的部分使用者名稱進行搜尋。
- *雜訊抑制*可篩選使用者在過去2小時內建立的檔案。它也可用來篩選使用者存取的暫存檔（例如、.tmp檔案）。
- * 執行活動之使用者的網域 * 。您需要提供 * 精確的網域 * 來進行篩選。搜尋部分網域、或以萬用字元（「 * 」）為前置或後置的部分網域將無法運作。_ 無 _ 可以指定來搜尋遺失的網域。

下列欄位必須遵守特殊篩選規則：

- * 實體類型 * 、使用實體（檔案）副檔名 - 最好在引號內指定確切的實體類型。例如 _ "txt" _ 。
- * 實體的 Path* ：這應該是確切的實體路徑（例如「 */home/userX/nested1/nested2/abc.txt* 」），或是遞歸搜尋路徑的目錄部分（例如「 */home/userX/nested1/nested2/* 」）。注意：此處不允許 regex 路徑模式（例如 * 使用者 X* ）。建議目錄路徑篩選器（以 / 結尾的路徑字串）最多 4 個目錄深，以獲得更快的結果。例如， "*/home/userX/nested1/nested2/*" 。如需詳細資訊、請參閱下表。
- 第一層資料夾（根目錄） - 實體路徑的根目錄作為篩選器。例如，如果實體路徑為 /home/userX/nested1/nested2/ ，則可使用 Home 或 Home 。
- 第二層資料夾 - 實體路徑篩選器的第二層目錄。例如，如果實體路徑為 /home/userX/nested1/nested2/ ，則可使用 userX 或「 userX 」。
- 第三層資料夾–實體路徑篩選器的第三層目錄。
- 例如，如果實體路徑為 /home/userX/nested1/nested2/ ，則可使用 nested1 或「 nested1 」。
- 第四層資料夾 - 實體路徑篩選器的目錄第四層目錄。例如，如果實體路徑為 /home/userX/nested1/nested2/ ，則可使用 nested2 或「 nested2 」。
- * 執行活動的使用者 * ：最好在報價中指定確切的使用者。例如、 _ 「管理員」 _ 。
- 實體所在的設備（SVM）
- *實體所在的Volume *
- 當原始檔案重新命名時、用於重新命名事件的*原始路徑*。

篩選時、上述欄位必須符合下列條件：

- 確切值應在引號內：範例：「searchtext」
- 萬用字元字串不得包含引號：範例：searchtext、*searchtext*會篩選任何包含「searchtext」的字串。
- 字串加上字首、例如：searchtext*、會搜尋以「searchtext」開頭的任何字串。

活動鑑識篩選器範例：

使用者套用的篩選運算式	預期成果	績效評估	留言
路徑 = "/home/userX/nested1/nested2/"	遞迴查詢指定目錄下的所有檔案和資料夾	快速	目錄搜尋最多 4 個目錄的速度很快。
路徑 = "/home/userX/nested1/"	遞迴查詢指定目錄下的所有檔案和資料夾	快速	目錄搜尋最多 4 個目錄的速度很快。
路徑 = 「 /home/userX/nested1/test 」	路徑值與 /home/userX/nested1/test 完全相符	慢一點	與目錄搜尋相比，搜尋的確切搜尋速度較慢。
路徑 = 「 /home/userX/nested1/nested2/nested3/"	遞迴查詢指定目錄下的所有檔案和資料夾	慢一點	搜尋超過 4 個目錄的速度較慢。

使用者套用的篩選運算式	預期成果	績效評估	留言
任何其他非路徑型篩選器。建議使用報價的使用者和實體類型篩選條件、例如、User="Administrator" Entity Type ="txt"		快速	

附註：

1. 當所選時間範圍超過 3 天時，「所有活動」圖示旁顯示的「活動」計數會四捨五入至 30 分鐘。例如， 9 月 1 日上午 10 ： 15 至 9 月 7 日上午 10 ： 15 的時間範圍將顯示 9 月 1 日上午 10 ： 00 至 9 月 7 日上午 10 ： 30 的活動計數。
2. 同樣地，當所選時間範圍超過 3 天時，「活動歷程記錄」圖表中顯示的計數度量會四捨五入至 30 分鐘。

排序取證活動記錄資料

您可以依 _ 時間，使用者，來源 IP ，活動， _ ， _ 實體類型 _ ，第一層資料夾（根目錄），第二層資料夾，第三層資料夾和第四層資料夾來排序活動記錄資料。根據預設、表格會依遞減的_Timed_順序排序、表示最新的資料會先顯示。「_Device」和「_Protocol」欄位的排序功能已停用。

非同步匯出使用者指南

總覽

儲存工作負載安全性中的非同步匯出功能是專為處理大型資料匯出而設計。

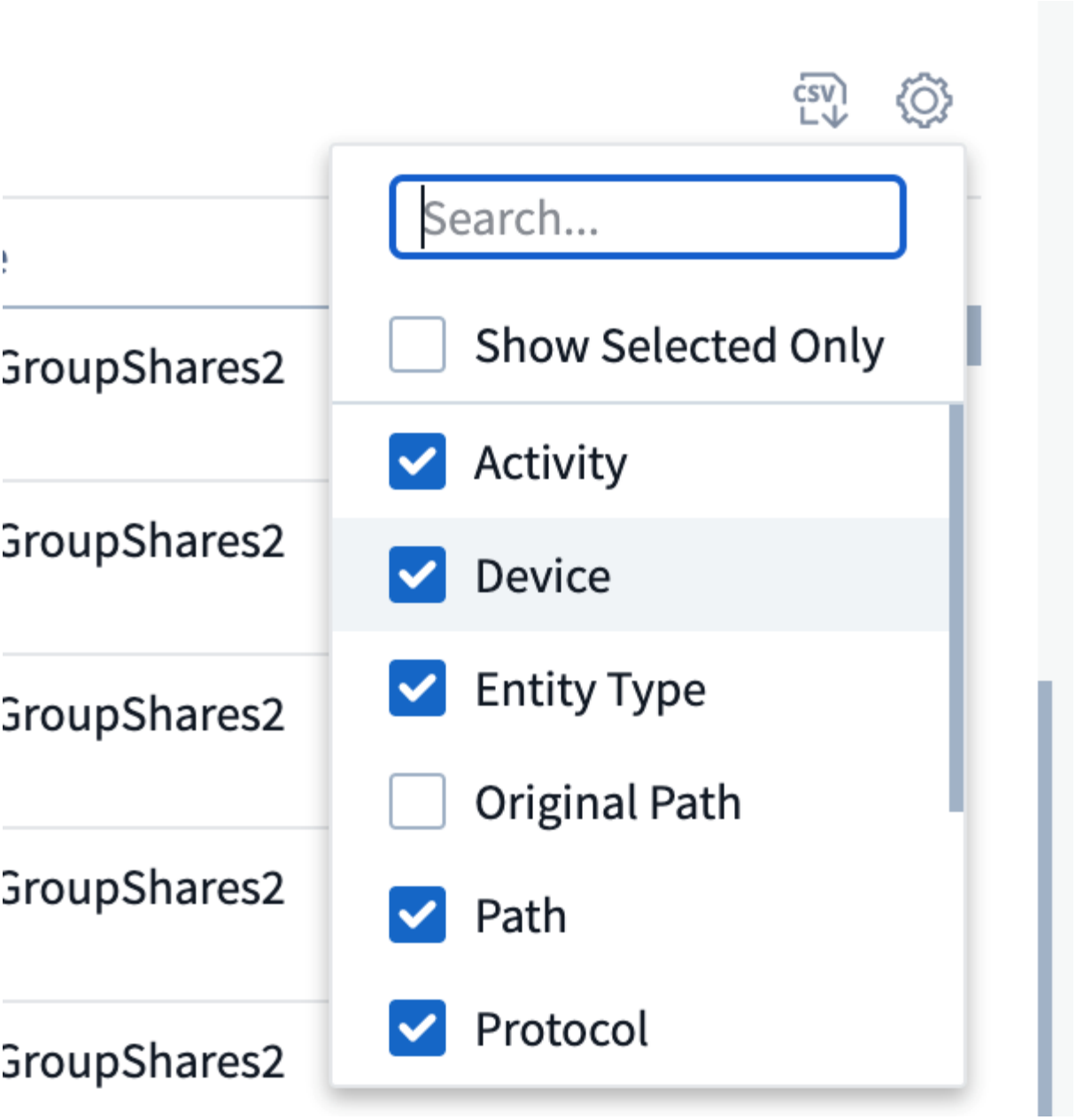
逐步指南：使用非同步匯出匯出資料

1. * 啟動匯出 * ：選取所需的匯出時間長度和篩選條件、然後按一下匯出按鈕。
2. * 等待匯出完成 * ：處理時間可從數分鐘到數小時不等。您可能需要重新整理鑑識頁面數次。匯出工作完成後、將會啟用「下載上次匯出 CSV 檔案」按鈕。
3. * 下載 * ：按一下「下載上次建立的匯出檔案」按鈕、以 .zip 格式取得匯出的資料。此資料將可供下載、直到使用者啟動另一個「非同步匯出」或已過 3 天（以先發生者為準）為止。此按鈕將保持啟用狀態、直到啟動另一個「非同步匯出」為止。
4. * 限制 * ：
    - 非同步下載的數量目前限制為每位使用者 1 次、每位租戶 3 次。
    - 匯出的資料上限為 100 萬筆記錄。

透過 API 擷取取鑑識資料的範例指令碼位於 NetApp 代理程式上的 /opt/oracle/cloudsecure/agent/Export 指令碼 // 。如需指令碼的詳細資訊、請參閱此位置的讀我檔案。

所有活動的欄選擇

「_All activity」（全部活動）表格預設會顯示選取欄。若要新增、移除或變更欄、請按一下表格右側的齒輪圖示、然後從可用欄清單中選取。



活動記錄保留

活動歷程記錄會保留13個月、適用於作用中的工作負載安全環境。

Forensics頁面中篩選器的適用性

篩選器	它的作用	範例	適用於這些篩選器	不適用於這些篩選器	結果
*（星號）	可讓您搜尋所有內容	Auto*03172022 如果搜尋文字包含連字號或底線、請在方括號中提供運算式、例如（ SVM* ）用於搜尋 SVM-123	使用者，實體類型，裝置， Volume ，原始路徑， 1stLevel 資料夾， 2ndLevel 資料夾， 3rdLevel 資料夾， 4thLevel 資料夾		傳回以「 Auto 」開頭並以「 03172022 」結尾的所有資源
？（問號）	可讓您搜尋特定字元數	AutoSabotageUser1_03172022？	使用者，實體類型，裝置， Volume ， 1stLevel 資料夾， 2ndLevel 資料夾， 3rdLevel 資料夾， 4thLevel 資料夾		傳回AutoSabotageUser1_03172022A、AutoSabotageUser1_03172022B、AutoSabotageUser1_031720225等
或	可讓您指定多個實體	AutoSabotageUser1_03172022 或AutoRansomUser4_03162022	使用者，網域，實體類型，原始路徑		傳回任何AutoSabotageUser1_03172022或AutoRansomUser4_03162022
不是	可讓您從搜尋結果中排除文字	非AutoRansomUser4_03162022	使用者，網域，實體類型，原始路徑， 1stLevel 資料夾， 2ndLevel 資料夾， 3rdLevel 資料夾， 4thLevel 資料夾	裝置	傳回所有開頭為「AutoRansomUser4_03162022」的項目
無	在所有欄位中搜尋空值	無	網域		傳回目標欄位為空白的結果

路徑搜尋

包含/不含/的搜尋結果會有所不同

"/AutoDir1/AutoFile03242022"	只能使用精確搜尋；會傳回所有具有正確路徑的活動，例如 /AutoDir1/AutoFile03242022 （不敏感的案例）
" / 自動直接 1/ "	有效；傳回與 AutoDir1 相符之第一層目錄的所有活動（案例不敏感）
"/AutoDir1/AutoFile03242022"	有效；傳回與 AutoDir1 相符的第一層目錄，以及與 AutoFile03242022 相符的第二層目錄的所有活動（案例不敏感）
/AutoDir1/AutoFile03242022 或/AutoDir1/AutoFile03242022	無法運作

不是/AutoDir1/AutoFile03242022	無法運作
不是/AutoDir1	無法運作
不是/AutoFile03242022	無法運作
*	無法運作

本機根 **SVM** 使用者活動變更

如果本機根 SVM 使用者正在執行任何活動、則安裝 NFS 共用的用戶端 IP 現在會納入使用者名稱中、在鑑識活動和使用者活動頁面中會顯示為 <ip-address-of-the-client> 。

例如：

- 如果 SVM-1 受到工作負載安全性的監控、且 SVM 的根使用者將共用裝載於 IP 位址為 10.197.12.40 的用戶端上、則取證活動頁面中顯示的使用者名稱將為 *root@10.197.12.40* 。
- 如果將同一個 SVM-1 裝載到另一個 IP 位址為 10.197.12.41 的用戶端、取證活動頁面中顯示的使用者名稱將為 *root@10.197.12.41* 。
- •這是為了依照 IP 位址來分隔 NFS 根使用者活動。以前、所有活動都只由 *root* 使用者執行、沒有 IP 區分。

疑難排解

問題	試試看
在「All Activities」（所有活動）表格的「User」（使用者）欄下、使用者名稱顯示為：「LDAP:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817”」或「LDAP:Default：80038003」。	可能的原因可能是：1.尚未設定使用者目錄收集器。若要新增一個、請前往 * 工作負載安全性 > 收集器 > 使用者目錄收集器 * 、然後按一下 *+ 使用者目錄收集器 * 。選擇_Active Directory或_LDAP Directory Server_。2.已設定使用者目錄收集器，但它已停止或處於錯誤狀態。請前往 * 收集器 > 使用者目錄收集器 * 、並檢查狀態。如需疑難排解秘訣，請參閱"使用者目錄收集器疑難排解"文件的一節。正確設定後、名稱將在24小時內自動解析。如果仍無法解決、請檢查是否已新增正確的使用者資料收集器。確定使用者確實是新增Active Directory / LDAP目錄伺服器的一部分。
UI中未顯示某些NFS事件。	請檢查下列項目：1.具有POSIX屬性集的AD伺服器之使用者目錄收集器應以從UI啟用的unixid屬性執行。2.從 UI 3 在使用者頁面中搜尋時，應該會看到任何執行 NFS 存取的使用者。NFS不支援原始事件（尚未探索使用者的事件）4。不會監控匿名存取NFS匯出。5.請確定 NFS4.1 版本低於 NFS4.1 。

在 Forensics *All Activity* 或 *Entity* 頁面的篩選器中輸入一些包含如星號（ * ）等萬用字元的字母後，頁面載入速度會非常緩慢。	搜尋字串中的星號（ * ）會搜尋所有項目。但是，諸如 <searchTerm> 或 <searchTerm> 等領先的通配符字符串將導致查詢速度緩慢。若要獲得更好的效能、請改用字首字串、格式為 <searchTerm> * （換句話說、在搜尋詞彙後加上星號（ * ）。範例：使用字串 _testvolume * 、而非 _*testvolume 或 _*test* Volume 。使用目錄搜尋，以遞歸方式查看指定資料夾下的所有活動（階層式搜尋）。例如，「 /path1/path2/path3// 」會在 /path1/path2/path3 下以遞歸方式列出所有活動。或者、也可以使用「 All Activity) 標籤下的「 Add to Filter 」（新增至篩選器）選項。
使用路徑篩選器時、我遇到「要求失敗、狀態碼 500/503 」錯誤。	請嘗試使用較小的日期範圍來篩選記錄。
取證使用者介面使用 *path* 篩選器時，資料載入速度緩慢。	目錄路徑篩選器（以 / 結尾的路徑字串）建議使用最多 4 個目錄深度，以獲得更快的結果。例如，如果目錄路徑為 /aaa/BBB/CCC/DDD ，請嘗試搜尋「 /AAA/BBB/CCC/DDD/」 ，以更快載入資料。

鑑識使用者總覽

每位使用者的資訊都會在「使用者總覽」中提供。使用這些檢視來瞭解使用者特性、相關實體及最近的活動。

使用者設定檔

使用者設定檔資訊包括聯絡資訊和使用者位置。設定檔提供下列資訊：

- 使用者名稱
- 使用者的電子郵件地址
- 使用者管理程式
- 使用者的電話聯絡人
- 使用者位置

使用者行為

使用者行為資訊可識別使用者最近執行的活動和作業。這些資訊包括：

- 最近的活動
  - 上次存取位置
  - 活動圖表
  - 警示
- 過去七天的營運
  - 作業數量

重新整理時間間隔

使用者清單每12小時重新整理一次。

保留政策

如果不再重新整理、使用者清單會保留13個月。13個月後、資料將會刪除。如果您的工作負載安全環境已刪除、則會刪除與環境相關的所有資料。

版權資訊

商標資訊