# 鑑識
# Cloud Insights

NetApp
April 16, 2024

# 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。本頁概述您環境中的活動、重點說明下列資訊：

- 顯示_ActivityHistory（活動記錄）的圖表（根據所選的整體時間範圍、每分鐘/每5分鐘/每10分鐘存取一次）

  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。

- 活動類型_的圖表。若要依活動類型取得活動記錄資料、請按一下對應的x軸標籤連結。
- 「實體類型」上的「活動」圖表。若要依實體類型取得活動記錄資料、請按一下對應的x軸標籤連結。
- 「所有活動」資料的清單

「_*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。
- 使用連結存取實體的*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。
- 實體的*路徑*、並連結至 "實體詳細資料"

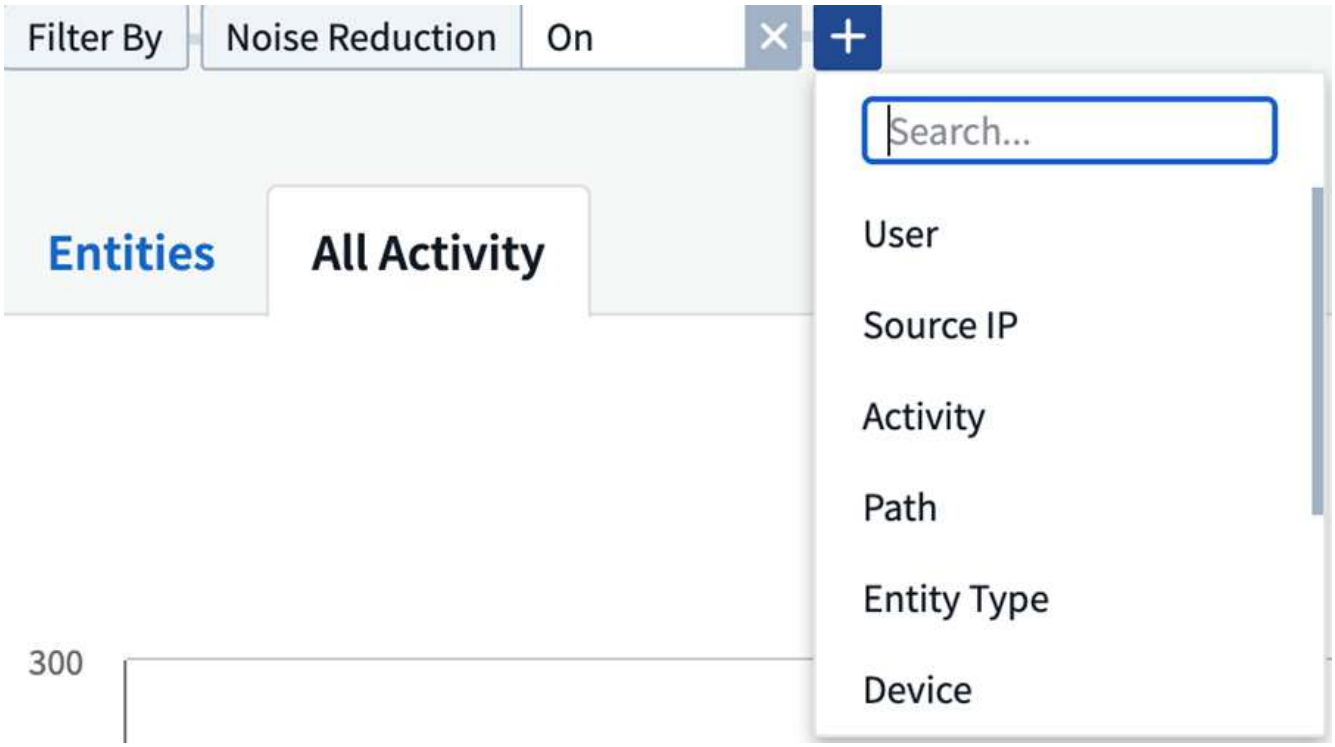
- 實體類型、包括實體（例如檔案）副檔名（.doc,.docx、.tmp,等等）
- 實體所在的*設備*
- 用於擷取事件的*傳輸協定*。
- 當原始檔案重新命名時、用於重新命名事件的*原始路徑*。根據預設、此欄在表格中不可見。使用欄選取器將此欄新增至表格。
- 實體所在的* Volume *。根據預設、此欄在表格中不可見。使用欄選取器將此欄新增至表格。

## 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。

1. 將游標暫留在表格中的欄位上、然後按一下出現的篩選圖示。此值會新增至頂端_Filter by（篩選條件）清單中的適當篩選條件。
2. 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）。

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
- 實體路徑
- 執行活動的使用者
- 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。

## 排序取證活動記錄資料

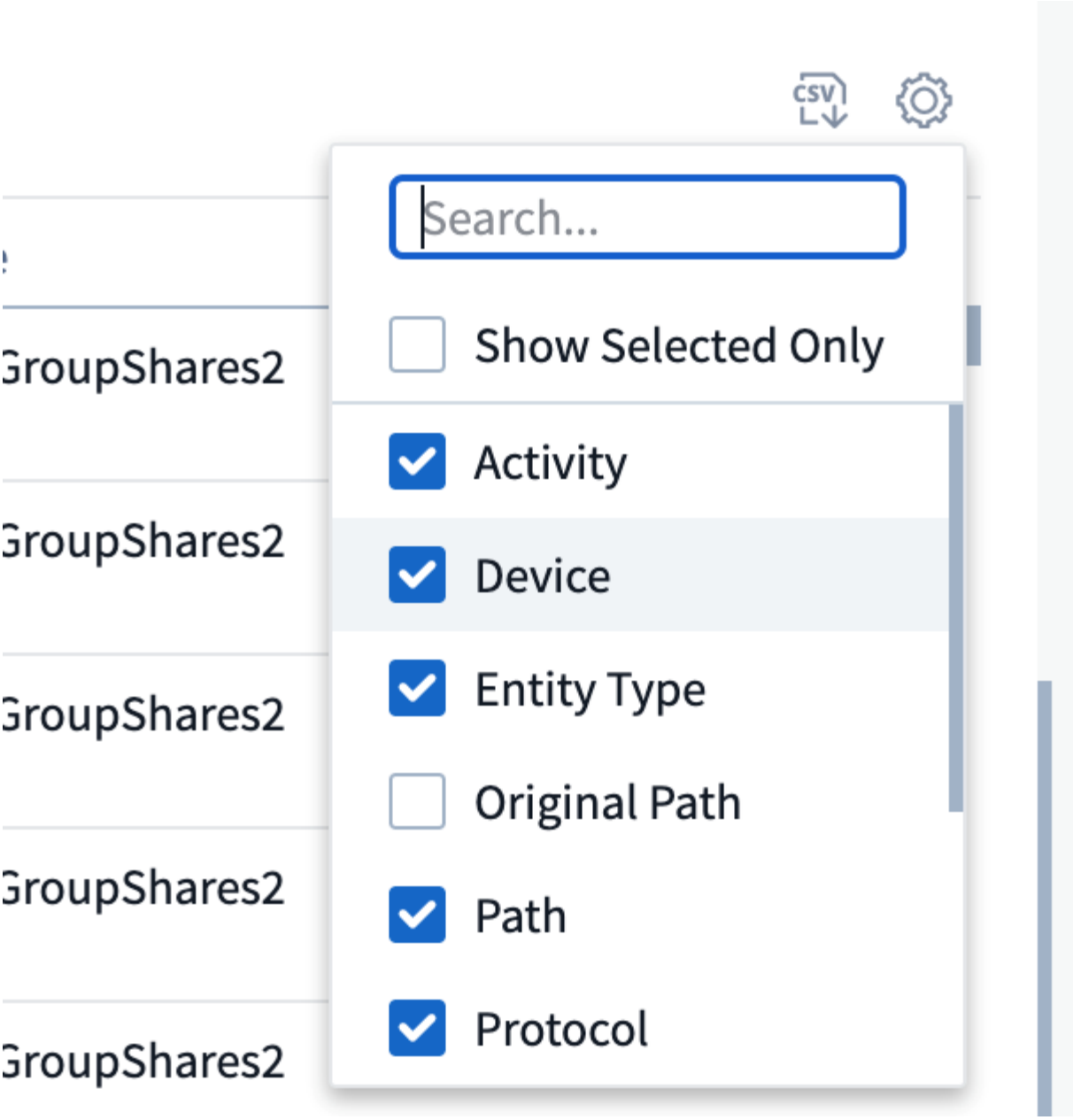
您可以依時間、使用者、來源IP、活動、路徑_和實體類型_來排序活動記錄資料。根據預設、表格會依遞減的_Timed_順序排序、表示最新的資料會先顯示。「_Device」和「_Protocol」欄位的排序功能已停用。

## 匯出所有活動

您可以按一下「活動記錄」表格上方的「_Export」（匯出）按鈕、將活動記錄匯出至.CSV檔案。請注意、只會匯出前 100 、 000 筆記錄。視資料量而定、匯出作業可能需要幾秒鐘到幾分鐘的時間才能完成。

## 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 | 適用於哪些篩選條件？ | 不適用於哪些篩選器 | 結果 |
|---|---|---|---|---|---|
| *（星號） | 可讓您搜尋所有內容 | Auto* 03172022 | 使用者、路徑、實體類型、裝置類型、Volume、原始路徑 | | 傳回以「Auto（自動）」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 | | 傳回AutoSabotageUser1_03172022A、AutoSabotageUser1_03172022AB、AutoSabotageUser1_031720225等 |
| 或 | 可讓您指定多個實體 | AutoSabotageUser1_03172022或AutoRansomUser4_03162022 | 使用者、網域、使用者名稱、路徑、實體類型、裝置、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、使用者名稱、路徑、實體類型、原始路徑、Volume | 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/原始路徑搜尋

包含/不含/的搜尋結果會有所不同

| | |
|---|---|
| /AutoDir1/AutoFile | 工作 |
| AutoDir1/AutoFile | 無法運作 |
| /AutoDir1/AutoFile（目錄1） | Dir1部分子字串無法運作 |
| "/AutoDir1/AutoFile03242022" | 完全正確的搜尋作業 |
| Auto* 03242022 | 無法運作 |
| AutoSabotageUser1_03172022？ | 無法運作 |
| /AutoDir1/AutoFile03242022<br>或/AutoDir1/AutoFile03242022 | 工作 |
| 不是/AutoDir1/AutoFile03242022 | 工作 |
| 非/AutoDir1 | 工作 |
| 不是/AutoFile03242022 | 無法運作 |
| * | 顯示所有項目 |

## 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：<br>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_。<br>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。請參閱 "使用者目錄收集器疑難排解" 說明文件中的一節、以取得疑難排解秘訣。<br>正確設定後、名稱將在24小時內自動解析。<br>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.在UI 3的使用者頁面中搜尋時、應該會看到執行NFS存取的任何使用者。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.確定NFS版本的使用版本低於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。<br>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（ * ）。<br>範例：使用字串 *testvolume* * 、而非 _**testvolume* 或 _**test** Volume* 。<br><br>使用以字首為基礎的搜尋、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* 或 _ "/path1/path2/path3"_ 將在 "*/path1/path2/path3* 下以遞歸方式列出所有活動。<br>或者、也可以使用「所有活動」索引標籤下的「新增至篩選」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。 |

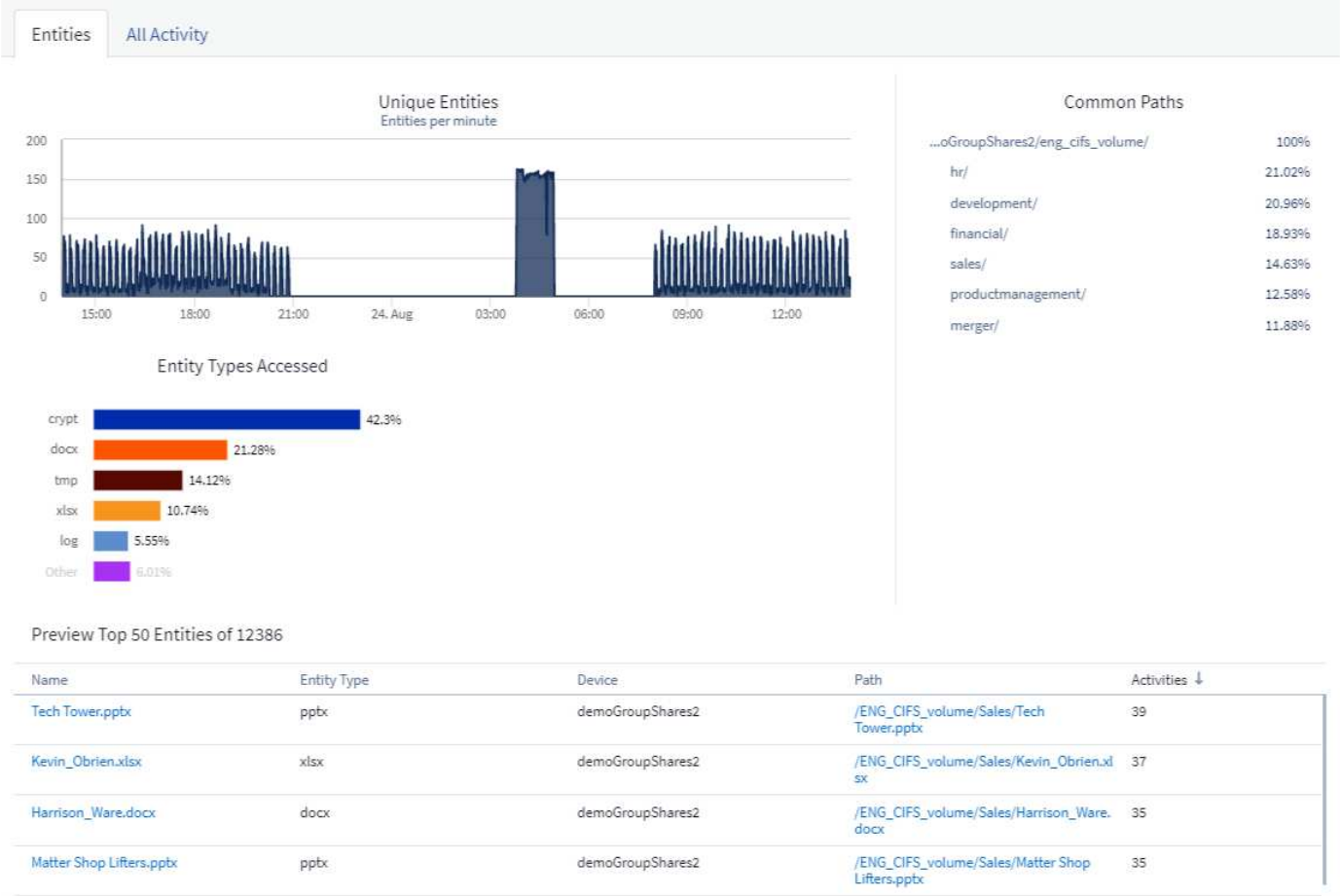
# 「鑑識實體」頁面

「鑑識實體」頁面提供您環境中實體活動的詳細資訊。

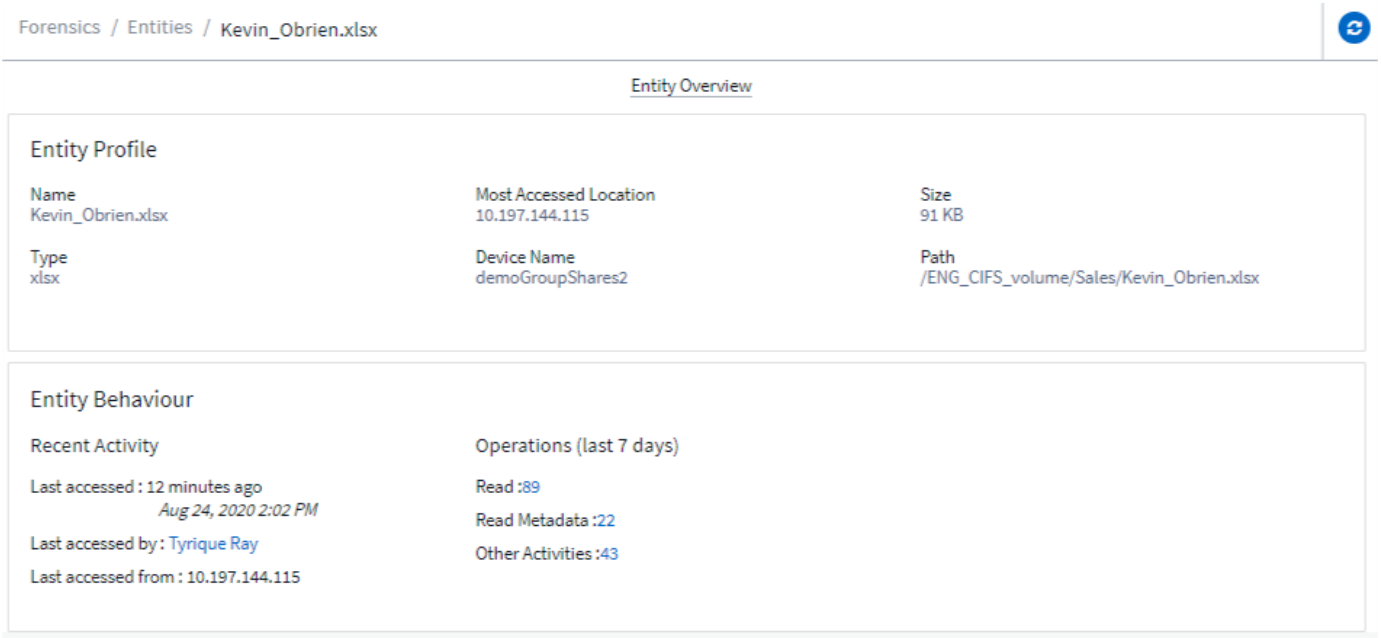
## 檢查實體資訊

按一下「鑑識」**>**「活動鑑識」、然後按一下「實體」索引標籤以存取「實體」頁面。

本頁概述您環境中的實體活動、重點說明下列資訊： *每分鐘存取的_獨特實體_圖表*存取的_實體類型_*公用路徑的明細表_*總共50個實體中的_前50個實體_清單




按一下清單中的實體、會開啟該實體的總覽頁面、顯示實體的設定檔、其中包含名稱、類型、裝置名稱、最常存取的位置IP和路徑、以及實體行為、例如使用者、IP、 以及上次存取實體的時間。




# 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。