法医

Data Infrastructure Insights

NetApp
February 03, 2026

目录

法医

取证 - 所有活动

“所有活动”页面可帮助您了解在工作负载安全环境中对实体执行的操作。

检查所有活动数据

单击“取证 > 活动取证”，然后单击“所有活动”选项卡以访问“所有活动”页面。此页面概述了租户上的活动，重点介绍了以下信息：

- 显示“活动历史”的图表（基于选定的全局时间范围）

  您可以通过在图形中拖出一个矩形来缩放图形。将加载整个页面以显示缩放的时间范围。放大时，会显示一个按钮让用户缩小。

- _所有活动_数据的列表。
- 分组下拉菜单将提供按用户、文件夹、实体类型等对活动进行分组的选项。
- 表格上方将出现一个常用路径按钮，单击该按钮我们可以获得带有实体路径详细信息的滑出面板。

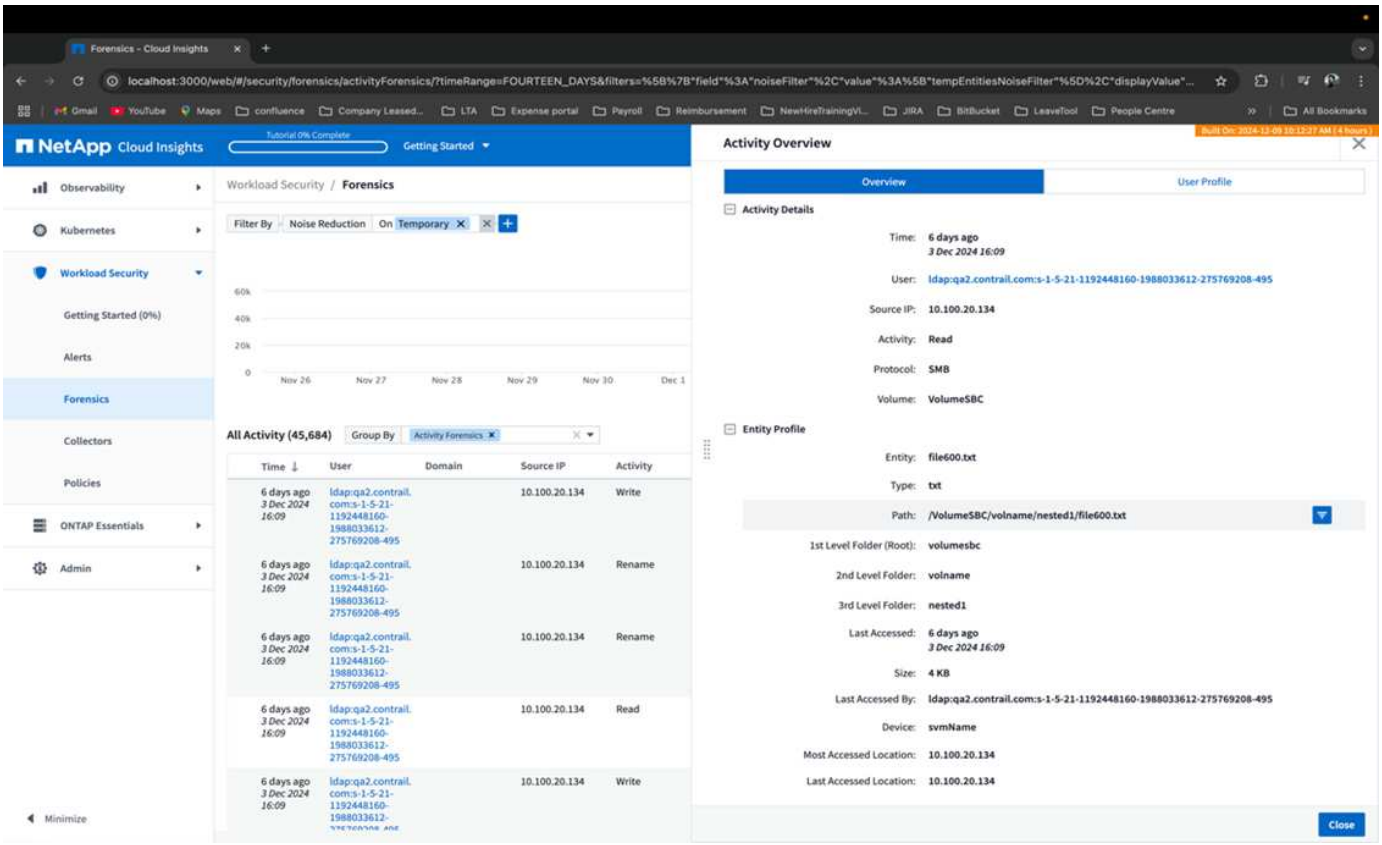
*所有活动*表显示以下信息。请注意，默认情况下并非所有这些列都会显示。您可以通过单击“齿轮”图标来选择要显示的列。

- 访问实体的*时间*，包括上次访问的年、月、日和时间。
- 通过链接访问实体的*用户*"用户信息"作为滑出面板。
- 用户执行的*活动*。支持的类型有：
  - 更改组所有权 - 文件或文件夹的组所有权已更改。有关团体所有权的更多详细信息，请参阅"此链接。"
  - 更改所有者 - 文件或文件夹的所有权更改为另一个用户。
  - 更改权限 - 文件或文件夹权限已更改。
  - 创建 - 创建文件或文件夹。
  - 删除——删除文件或文件夹。如果删除了一个文件夹，则会获取该文件夹及其子文件夹中所有文件的_delete_事件。
  - 读取-文件已读取。
  - 读取元数据 - 仅在启用文件夹监控选项时。将在 Windows 上打开文件夹或在 Linux 中的文件夹内运行“ls”时生成。
  - 重命名——重命名文件或文件夹。
  - 写入 - 数据写入文件。
  - 写入元数据 - 写入文件元数据，例如，权限更改。
  - 其他变化 - 任何其他未在上面描述的事件。所有未映射的事件都映射到“其他更改”活动类型。适用于文件和文件夹。
- **Path** 是_entity_路径。这应该是精确的实体路径（例如，“*/home/userX/nested1/nested2/abc.txt*”）或递归搜索路径的目录部分（例如，“*/home/userX/nested1/nested2/*”）。注意：这里不允许使用正则表达式路径模式

（例如，*nested*）。或者，也可以为路径过滤指定如下所述的单独路径文件夹级别过滤器。

- **1st Level Folder (Root)** 是小写的实体路径的根目录。
- **2nd Level Folder** 是小写的实体路径的二级目录。
- **3rd Level Folder** 是小写的实体路径的第三级目录。
- **4th Level Folder** 是小写的实体路径的第四级目录。
- 实体类型，包括实体（即文件）扩展名（.doc、.docx、.tmp 等）。
- 实体所在的*设备*。
- 用于获取事件的*协议*。
- 原始文件重命名时用于重命名事件的*原始路径*。默认情况下，此列在表中不可见。使用列选择器将此列添加到表中。
- 实体所在的*卷*。默认情况下，此列在表中不可见。使用列选择器将此列添加到表中。
- *实体名称*是实体路径的最后一个组成部分；对于文件类型的实体，它是文件名。

选择表格行将打开一个滑出面板，其中一个选项卡中显示用户配置文件，另一个选项卡中显示活动和实体概览。



默认的_Group by_方法是_Activity forensics_。如果您选择不同的“分组依据”方法（例如，实体类型），则会显示实体“分组依据”表。如果没有做出选择，则显示_Group By_ **all**。

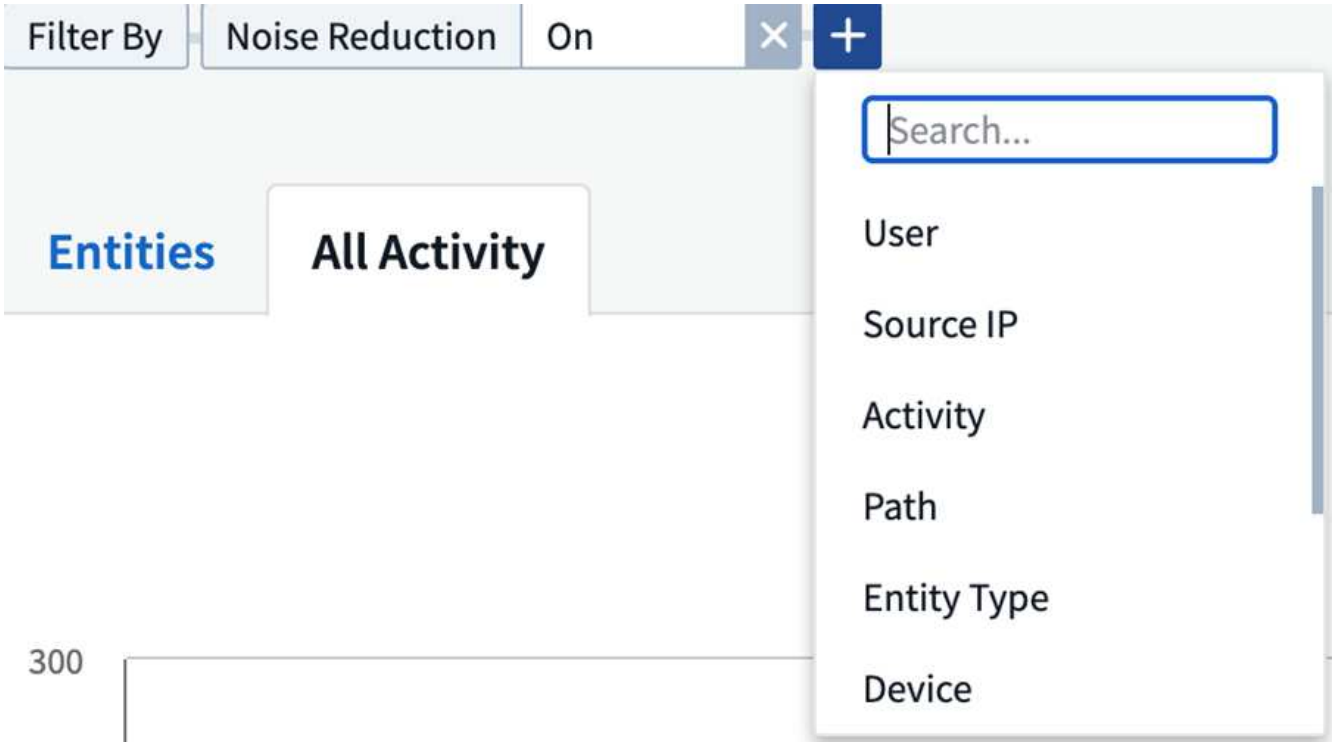
- 活动计数显示为超链接；选择此项将添加选定的分组作为过滤器。活动表将根据该过滤器进行更新。
- 请注意，如果您更改过滤器、改变时间范围或刷新屏幕，则必须再次设置过滤器才能返回过滤结果。
- 请注意，当选择实体名称作为过滤器时，分组依据下拉菜单将被禁用；此外，当用户已经在分组依据屏幕上时，实体名称作为过滤器将被禁用。

过滤取证活动历史数据

您可以使用两种方法来过滤数据。

- 可以从滑出面板添加过滤器。该值被添加到顶部“过滤依据”列表中的相应过滤器中。
- 通过在“筛选依据”字段中输入以下内容来筛选数据：

  通过单击 **[+]** 按钮，从顶部的“按条件过滤”小部件中选择适当的过滤器：



  输入搜索文本

  按 Enter 键或单击过滤器框外部即可应用过滤器。

您可以按以下字段过滤取证活动数据：

- *活动*类型。
- 协议 用于获取特定于协议的活动。
- 执行活动的用户的*用户名*。您需要提供准确的用户名来过滤。使用部分用户名或以“*”为前缀或后缀的部分用户名进行搜索将不起作用。
- 降噪 过滤用户在过去 2 小时内创建的文件。它还用于过滤用户访问的临时文件（例如 .tmp 文件）。
- 执行活动的用户的*域*。您需要提供*精确的域*来进行过滤。搜索部分域名，或以通配符（'*'）作为前缀或后缀的部分域名将不起作用。可以指定_None_来搜索缺失的域。

以下字段需遵守特殊过滤规则：

- 实体类型，使用实体（文件）扩展名 - 最好在引号内指定确切的实体类型。例如“txt”。
- 实体的*路径* - 这应该是精确的实体路径（例如，“*/home/userX/nested1/nested2/abc.txt*”）或递归搜索的路

径的目录部分（例如，“*/home/userX/nested1/nested2/*”）。注意：这里不允许使用正则表达式路径模式（例如，*nested*）。为了更快地获得结果，建议使用最多 4 个目录深度的目录路径过滤器（以 / 结尾的路径字符串）。例如，“*/home/userX/nested1/nested2/*”。请参阅下表以了解更多详细信息。

- 第一级文件夹（根） - 作为过滤器的实体路径的根目录。例如，如果实体路径是 /home/userX/nested1/nested2/，那么可以使用 home 或“home”。
- 第二级文件夹 - 实体路径过滤器的第二级目录。例如，如果实体路径是 /home/userX/nested1/nested2/，则可以使用 userX 或“userX”。
- 第三级文件夹 – 实体路径过滤器的第三级目录。
- 例如，如果实体路径是 /home/userX/nested1/nested2/，则可以使用 nested1 或“nested1”。
- 第四级文件夹 - 实体路径过滤器的目录第四级目录。例如，如果实体路径是 /home/userX/nested1/nested2/，那么可以使用 nested2 或“nested2”。
- *用户*执行活动 - 最好在引号内指定确切的用户。例如，“管理员”。
- 实体所在的*设备*（SVM）
- 实体所在的*体积*
- 原始文件重命名时用于重命名事件的*原始路径*。
- 访问实体的*源 IP*。
  - 您可以使用通配符 * 和 ?。例如：10.0.0.、**10.0.0.10**、**10.10**
  - 如果需要完全匹配，则必须提供双引号中有效的源 IP 地址，例如“10.1.1.1。”。带有双引号的不完整 IP（例如“10.1.1。”，“10.1..*”等）将不起作用。
- 实体名称 - 作为过滤器的实体路径的文件名。例如，如果实体路径是 /home/userX/nested1/testfile.txt，那么实体名称就是 testfile.txt。请注意，建议在引号内指定确切的文件名；尽量避免使用通配符搜索。例如“testfile.txt”。另请注意，建议在较短的时间范围内（最多 3 天）使用此实体名称过滤器。

以上字段在过滤时需要遵循以下原则：

- 确切值应放在引号内：例如：“searchtext”
- 通配符字符串不能包含引号：示例：searchtext，*searchtext*，将过滤任何包含“searchtext”的字符串。
- 带有前缀的字符串，例如：searchtext*，将搜索以“searchtext”开头的任何字符串。

请注意，所有过滤字段都是区分大小写的搜索。例如：如果应用的过滤器是实体类型，值为“searchtext”，它将返回实体类型为“searchtext”、“SearchText”、“SEARCHTEXT”的结果

活动取证过滤器示例：

用户应用的过滤表达式	预期结果	绩效评估	注释
路径 = “/home/userX/nested1/nested2/”	递归查找给定目录下的所有文件和文件夹	快	最多 4 个目录的目录搜索将会很快。
路径 = “/home/userX/nested1/”	递归查找给定目录下的所有文件和文件夹	快	最多 4 个目录的目录搜索将会很快。

用户应用的过滤表达式	预期结果	绩效评估	注释
路径 = “/home/userX/nested1/test”	路径值与 /home/userX/nested1/test 完全匹配	慢点	与目录搜索相比，精确搜索的速度较慢。
路径 = “/home/userX/nested1/nested2/nested3/”	递归查找给定目录下的所有文件和文件夹	慢点	超过 4 个目录的搜索速度较慢。
任何其他非基于路径的过滤器。建议将用户和实体类型过滤器放在引号中，例如，用户=“管理员”实体类型=“txt”		快	
实体名称 = “test.log”	文件名为 test.log 的精确匹配	快	因为它是完全匹配
实体名称 = *test.log	文件名以 test.log 结尾	慢	由于通配符，它可能会很慢。
实体名称 = test*.log	文件名以 test 开头，以 .log 结尾	慢	由于通配符，它可能会很慢。
实体名称 = test.lo	文件名以 test.lo 开头 例如：它将匹配 test.log 、test.log.1、test.log1	慢点	由于最后有通配符，所以速度可能会很慢。
实体名称 = 测试	文件名以 test 开头	最慢	由于末尾有通配符并且使用了更多通用值，因此速度可能最慢。

注:

1. 当选定的时间范围跨越 3 天以上时，“所有活动”图标旁边显示的活动计数将四舍五入为 30 分钟。例如，时间范围“9 月 1 日上午 10:15 至 9 月 7 日上午 10:15”将显示从 9 月 1 日上午 10:00 到 9 月 7 日上午 10:30 的活动计数。
2. 同样，当选定的时间范围跨越 3 天以上时，活动历史记录图表中显示的计数指标将四舍五入为 30 分钟。

对取证活动历史数据进行排序

您可以按时间、用户、源 IP、活动、实体类型、第一级文件夹（根）、第二级文件夹、第三级文件夹和第四级文件夹对活动历史数据进行排序。默认情况下，表格按时间降序排列，这意味着最新的数据将首先显示。*Device* 和 *Protocol* 字段的排序被禁用。

异步导出用户指南

概述

存储工作负载安全中的异步导出功能旨在处理大量数据导出。

分步指南：使用异步导出导出数据

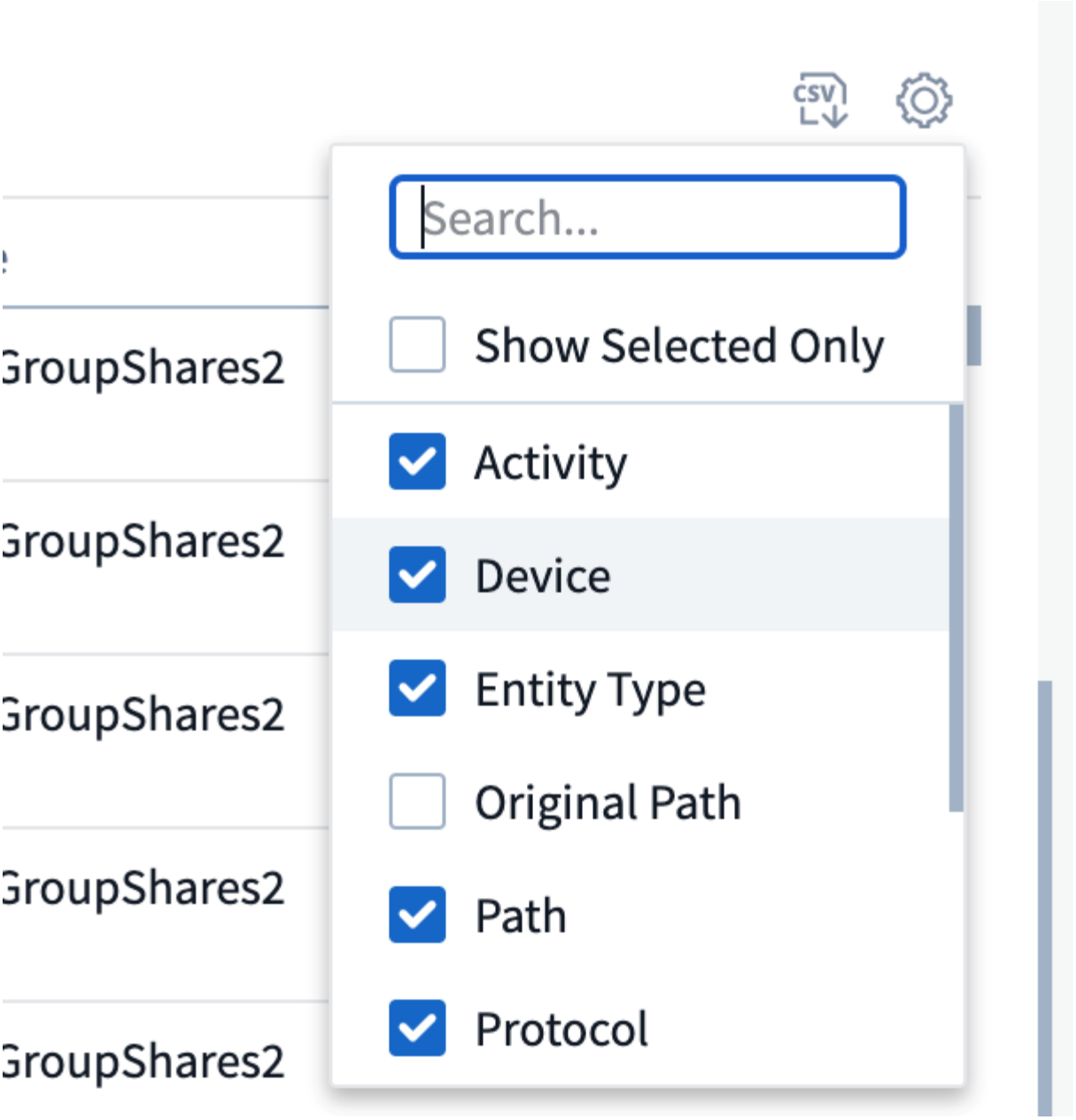
1. 启动导出：选择所需的导出时间长度和过滤器，然后单击导出按钮。

2. 等待导出完成：处理时间可能从几分钟到几个小时不等。您可能需要刷新取证页面几次。导出作业完成后，“下载最后导出的 CSV 文件”按钮将被启用。
3. 下载：单击“下载最后创建的导出文件”按钮以获取.zip格式的导出数据。这些数据将可供下载，直到用户启动另一个异步导出或 3 天过去（以先发生者为准）。该按钮将保持启用状态，直到启动另一个异步导出。
4. 限制：
    - 目前，每个用户每个活动和活动分析表的异步下载次数限制为 1 次，每个租户的异步下载次数限制为 3 次。
    - 对于活动表，导出的数据限制为最多 100 万条记录；而对于分组，限制为 50 万条记录。

代理上的 */opt/netapp/cloudsecure/agent/export-script/* 处有一个通过 API 提取取证数据的示例脚本。有关该脚本的更多详细信息，请参阅此处的自述文件。

所有活动的列选择

_所有活动_表默认显示选定列。要添加、删除或更改列，请单击表格右侧的齿轮图标，然后从可用列列表中进行选择。



活动历史记录保留

对于活跃的工作负载安全环境，活动历史记录将保留 13 个月。

取证页面中过滤器的适用性

筛选器	它的作用	示例	适用于这些过滤器	不适用于这些过滤器	结果
*（星号）	让您搜索一切	Auto*03172022 如果搜索文本包含连字符或下划线，请在括号中给出表达式。例如，(svm*) 用于搜索 svm-123	用户、实体类型、设备、卷、原始路径、第一级文件夹、第二级文件夹、第三级文件夹、第四级文件夹、实体名称、源 IP		返回所有以“Auto”开头并以“03172022”结尾的资源
？（问号）	使您能够搜索特定数量的字符	AutoSabotageUser1_03172022?	用户、实体类型、设备、卷、第一级文件夹、第二级文件夹、第三级文件夹、第四级文件夹、实体名称、源 IP		返回 AutoSabotageUser1_03172022A、AutoSabotageUser1_03172022B、AutoSabotageUser1_03172025 等等
或	使您能够指定多个实体	AutoSabotageUser1_03172022 或 AutoRansomUser4_03162022	用户、域、实体类型、原始路径、实体名称、源 IP		返回 AutoSabotageUser1_03172022 或 AutoRansomUser4_03162022 中的任一个
不是	允许您从搜索结果中排除文本	NOT AutoRansomUser4_03162022	用户、域、实体类型、原始路径、一级文件夹、二级文件夹、三级文件夹、四级文件夹、实体名称、源 IP	设备	返回所有不以“AutoRansomUser4_03162022”开头的内容
无	在所有字段中搜索 NULL 值	无	领域		返回目标字段为空的结果

路径搜索

带有和不带有 / 的搜索结果会有所不同

“/AutoDir1/AutoFile03242022”	仅精确搜索有效；返回所有具有精确路径为 /AutoDir1/AutoFile03242022 的活动（不区分大小写）
“/AutoDir1/”	有效；返回与 AutoDir1 匹配的第一级目录的所有活动（不区分大小写）
“/AutoDir1/AutoFile03242022/”	有效；返回与 AutoDir1 匹配的第一级目录和与 AutoFile03242022 匹配的第二级目录的所有活动（不区分大小写）

/AutoDir1/AutoFile03242022 或 /AutoDir1/AutoFile03242022	不起作用
不是/AutoDir1/AutoFile03242022	不起作用
不是/AutoDir1	不起作用
不是/AutoFile03242022	不起作用
*	不起作用

本地根 SVM 用户活动发生变化

如果本地根 SVM 用户正在执行任何活动，则现在将在用户名中考虑安装 NFS 共享的客户端的 IP，该 IP 将在取证活动和用户活动页面中显示为 root@<ip-address-of-the-client>。

例如：

- 如果 SVM-1 由 Workload Security 监控，并且该 SVM 的根用户在 IP 地址为 10.197.12.40 的客户端上挂载共享，则取证活动页面中显示的用户名将为 *root@10.197.12.40*。
- 如果将同一个 SVM-1 安装到 IP 地址为 10.197.12.41 的另一个客户端，则取证活动页面中显示的用户名将为 *root@10.197.12.41*。

*• 这样做是为了通过 IP 地址隔离 NFS 根用户活动。以前，所有活动都被认为仅由_root_用户完成，没有IP区别。

故障排除

问题	尝试一下
在“所有活动”表中的“用户”列下，用户名显示为：“ldap：HQ.COMPANYNAME.COM：S-1-5-21-3577637-1906459482-1437260136-1831817”或“ldap：default：80038003”	可能的原因有：1.尚未配置任何用户目录收集器。要添加一个，请转到*工作负载安全>收集器>用户目录收集器*，然后单击*+用户目录收集器*。选择“Active Directory”或“LDAP 目录服务器”。2.已配置用户目录收集器，但它已停止或处于错误状态。请转到*收集器>用户目录收集器*并检查状态。请参阅"用户目录收集器故障排除"文档部分提供了故障排除提示。正确配置后，名称将在 24 小时内自动解析。如果仍然没有解决，请检查您是否添加了正确的用户数据收集器。确保该用户确实是所添加的 Active Directory/LDAP 目录服务器的一部分。
某些 NFS 事件在 UI 中看不到。	检查以下内容：1.应运行设置了 POSIX 属性的 AD 服务器的用户目录收集器，并从 UI 启用 unixid 属性。2.从 UI 3 在用户页面中搜索时，应该可以看到任何进行 NFS 访问的用户。 NFS 4 不支持原始事件（尚未发现用户的事件）。对 NFS 导出的匿名访问将不会受到监控。5.确保使用的 NFS 版本为 4.1 或更低版本。 （请注意， ONTAP 9.15 或更高版本支持 NFS 4.1。）

在取证_所有活动_或_实体_页面的过滤器中输入一些包含通配符（如星号 (*)）的字母后，页面加载速度非常慢。	搜索字符串中的星号 (*) 可搜索所有内容。但是，以 *<*searchTerm*> 或 *<*searchTerm*>* 等为首的通配符字符串将导致查询速度变慢。为了获得更好的性能，请改用前缀字符串，格式为 <*searchTerm*>*（换句话说，在搜索词后面附加星号 (*)）。示例：使用字符串 *testvolume**，而不是 **testvolume* 或 **test*volume*。使用目录搜索以递归方式查看给定文件夹下的所有活动（分层搜索）。例如，“/path1/path2/path3/”将以递归方式列出 /path1/path2/path3 下的所有活动。或者使用“所有活动”选项卡下的“添加到过滤器”选项。”
使用路径过滤器时遇到“请求失败，状态代码 500/503”错误。	尝试使用较小的日期范围来过滤记录。
使用 *path* 过滤器时，Forensic UI 加载数据的速度很慢。	目录路径过滤器（以 / 结尾的路径字符串）建议深度最多为 4 个目录，以便更快地获得结果。例如，如果目录路径是 /Aaa/Bbb/Ccc/Ddd，请尝试搜索“/Aaa/Bbb/Ccc/Ddd/”以更快地加载数据。
使用实体名称过滤器时，Forensics UI 加载数据缓慢且遇到失败。	请尝试使用较小的时间范围并使用双引号进行精确值搜索。例如，如果 entityPath 是“/home/userX/nested1/nested2/nested3/testfile.txt”，则尝试使用“testfile.txt”作为实体名称过滤器。

法医用户概述

用户概览中提供了每个用户的信息。使用这些视图来了解用户特征、关联实体和最近的活动。

用户配置文件

用户资料信息包括用户的联系信息和位置。该配置文件提供以下信息：

- 用户姓名
- 用户的电子邮件地址
- 用户管理器
- 用户的电话联系方式
- 用户位置

用户行为

用户行为信息识别用户最近的活动和执行的操作。这些信息包括：

- 近期活动
  - 最后访问位置
  - 活动图
  - 警报
- 过去七天的运营情况

- 操作次数

刷新间隔

用户列表每 12 小时刷新一次。

保留政策

如果没有再次刷新，用户列表将保留 13 个月。 13个月后，数据将被删除。如果您的工作负载安全环境被删除，则与该环境相关的所有数据也将被删除。

版权信息

商标信息