Ciencia forense

Data Infrastructure Insights

NetApp
December 19, 2024

Tabla de contenidos

Ciencia forense

Análisis forenses: Toda la actividad

La página All Activity permite comprender las acciones que se realizan en las entidades del entorno Workload Security.

Examen de todos los datos de actividad

Haga clic en **Forensics > Activity Forensics** y haga clic en la ficha **All Activity** para acceder a la página All Activity. Esta página proporciona una descripción general de las actividades de su inquilino, destacando la siguiente información:

- Un gráfico que muestra *Activity History* (basado en el rango de tiempo global seleccionado)

  Puede ampliar el gráfico arrastrando un rectángulo del gráfico. Se cargará toda la página para mostrar el intervalo de tiempo ampliado. Cuando se amplía, se muestra un botón que permite al usuario alejar el zoom.

- Una lista de los datos *All Activity*.
- Una lista desplegable GROUP BY proporcionará la opción de agrupar la actividad por usuarios, ruta, tipo de entidad, etc.
- Un botón de ruta común estará disponible sobre la tabla en clic del que podemos obtener el panel deslizante con detalles de ruta de la entidad.

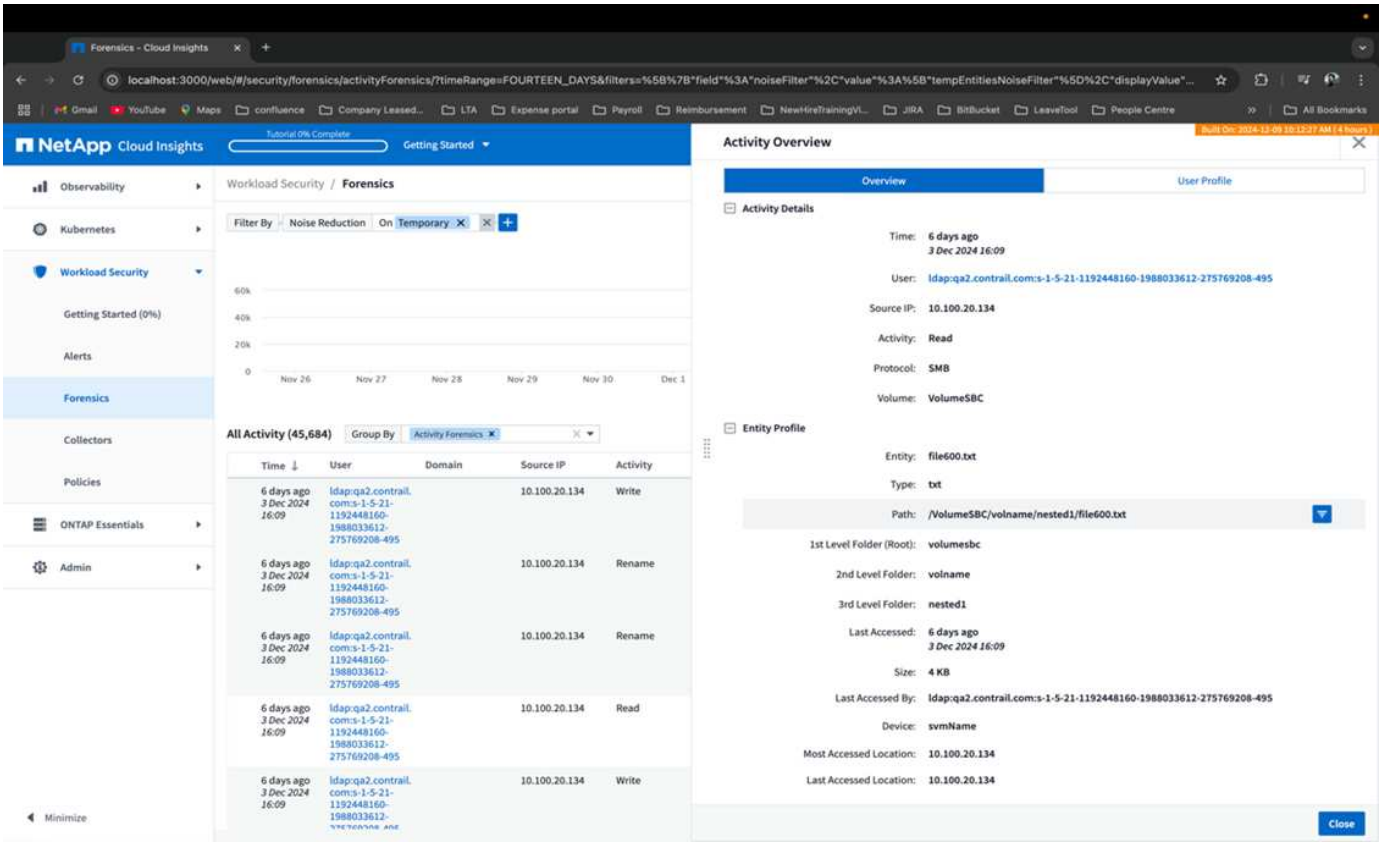
La tabla **All Activity** muestra la siguiente información. Tenga en cuenta que no todas estas columnas se muestran de forma predeterminada. Puede seleccionar las columnas que desea mostrar haciendo clic en el icono de engranaje.

- El **tiempo** se accedió a una entidad incluyendo el año, mes, día y hora del último acceso.
- El **usuario** que accedió a la entidad con un enlace a la "Información del usuario" como un panel deslizante.
- La **actividad** que realizó el usuario. Los tipos admitidos son:
  - **Cambiar propiedad de grupo**: La propiedad de grupo es de archivo o carpeta que se cambia. Para obtener más detalles sobre la propiedad del grupo, consulte "este enlace."
  - **Cambiar propietario**: La propiedad del archivo o carpeta se cambia a otro usuario.
  - **Permiso de cambio**: Se ha cambiado el permiso de archivo o carpeta.
  - **Crear** - Crear archivo o carpeta.
  - **Eliminar**: Permite eliminar archivos o carpetas. Si se elimina una carpeta, se obtienen eventos *delete* para todos los archivos de esa carpeta y subcarpetas.
  - **Leer**: Se lee el archivo.
  - **Leer metadatos**: Sólo para activar la opción de supervisión de carpetas. Se generará al abrir una carpeta en Windows o al ejecutar “ls” dentro de una carpeta en Linux.
  - **Renombrar**: Permite cambiar el nombre del archivo o carpeta.
  - **Escribir**: Los datos se escriben en un archivo.
  - **Escribir metadatos** - los metadatos del archivo se escriben, por ejemplo, el permiso cambiado.

- **Otro Cambio** - cualquier otro evento que no se describe anteriormente. Todos los eventos no asignados se asignan al tipo de actividad “otros cambios”. Aplicable a archivos y carpetas.

- El **Path** es *entity* path.
- La carpeta de nivel **1st (root)** es el directorio raíz de la ruta de la entidad en minúscula.
- La carpeta de nivel **2nd** es el directorio de segundo nivel de la ruta de la entidad en minúscula.
- La carpeta de nivel **3rd** es el directorio de tercer nivel de la ruta de la entidad en minúsculas.
- La carpeta de nivel **4th** es el directorio de nivel cuarto de la ruta de la entidad en minúscula.
- El **Tipo de entidad**, incluyendo la extensión de entidad (es decir, archivo) (.doc, .docx, .tmp, etc.).
- El **Dispositivo** donde residen las entidades.
- El **Protocolo** utilizado para obtener eventos.
- La **Ruta original** se utiliza para cambiar el nombre de los eventos cuando se cambió el nombre del archivo original. Esta columna no está visible de forma predeterminada en la tabla. Utilice el selector de columna para agregar esta columna a la tabla.
- El **volumen** donde residen las entidades. Esta columna no está visible de forma predeterminada en la tabla. Utilice el selector de columna para agregar esta columna a la tabla.

Al seleccionar una fila de tabla, se abre un panel desplegable con el perfil de usuario en una pestaña y la vista general de actividad y entidad en otra pestaña.



El método *Group by* por defecto es *Activity forsics*. Si selecciona un método *Group by* distinto—por ejemplo, Tipo de entidad—se mostrará la tabla *Group by* de entidad. Si no se realiza ninguna selección, se muestra *Agrupar por* **Todo**.

- El recuento de actividades se muestra como un hipervínculo; al seleccionarlo, se agregará la agrupación

seleccionada como filtro. La tabla de actividad se actualizará en función de ese filtro.

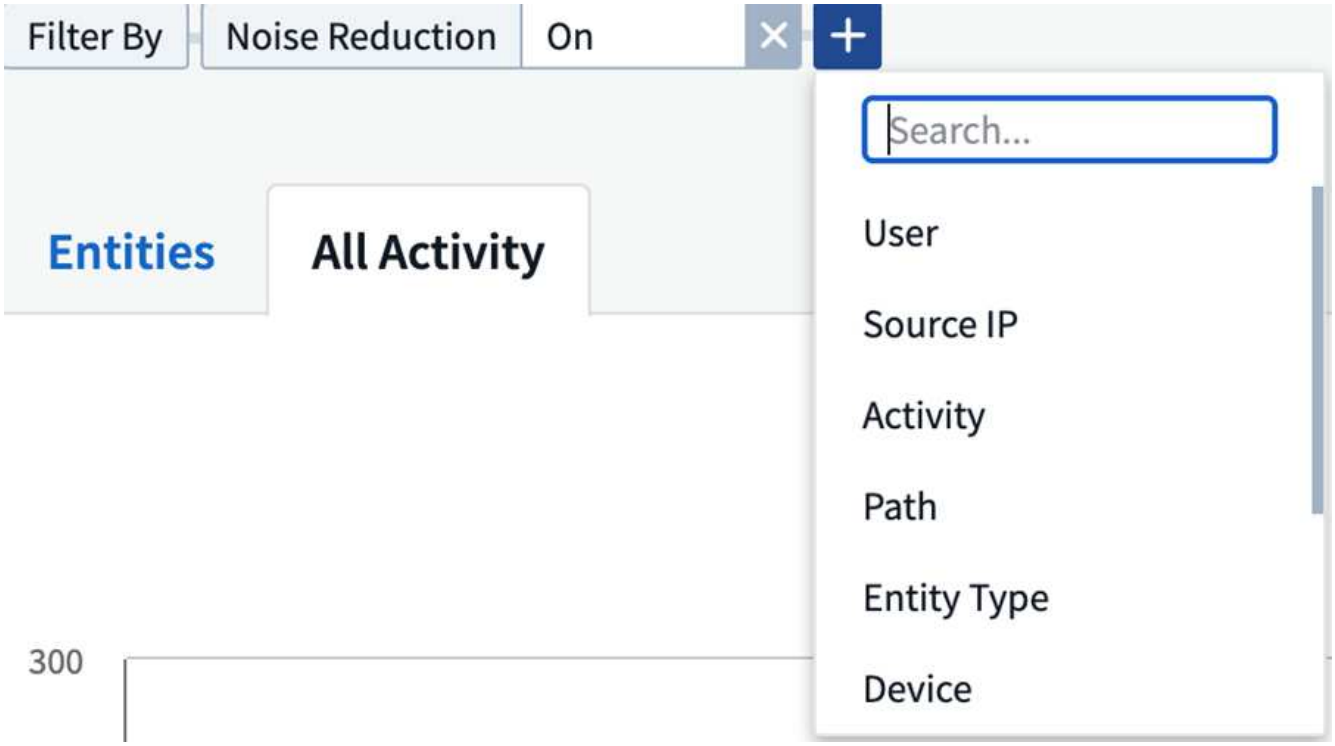
- Tenga en cuenta que si cambia el filtro, modifica el intervalo de tiempo o actualiza la pantalla, no podrá volver a los resultados filtrados sin volver a configurar el filtro.

Filtrado de datos del historial de actividades forenses

Existen dos métodos que se pueden utilizar para filtrar datos.

- El filtro se puede añadir desde el panel deslizante. El valor se agrega a los filtros apropiados en la lista Top *Filter by*.
- Filtre los datos escribiendo en el campo *Filter by*:

  Seleccione el filtro adecuado en el widget "Filtrar por" superior haciendo clic en el botón **[+]**:



  Introduzca el texto de búsqueda

  Pulse Intro o haga clic fuera del cuadro de filtro para aplicar el filtro.

Puede filtrar los datos de la actividad forense por los siguientes campos:

- El tipo **actividad**.
- **IP de origen** desde la que se accedió a la entidad. Debe proporcionar una dirección IP de origen válida entre comillas dobles, por ejemplo “10.1.1.1”. Los IP incompletos, como “10.1.1.**”, “10.1.**.*”, etc., no funcionarán.
- **Protocolo** para obtener actividades específicas del protocolo.
- **Nombre de usuario** del usuario que realiza la actividad. Debe proporcionar el nombre de usuario exacto para filtrar. La búsqueda con nombre de usuario parcial o nombre de usuario parcial con prefijo o sufijo ‘*’ no funcionará.
- **Reducción de ruido** para filtrar los archivos que el usuario crea en las últimas 2 horas. También se utiliza

para filtrar archivos temporales (por ejemplo, archivos .tmp) a los que accede el usuario.

- **Dominio** del usuario que realiza la actividad. Debe proporcionar el **dominio exacto** para filtrar. La búsqueda de dominio parcial, o dominio parcial con prefijo o sufijo con comodín ('*'), no funcionará. *None* se puede especificar para buscar el dominio que falta.

Los siguientes campos están sujetos a reglas de filtrado especiales:

- **Tipo de entidad**, usando la extensión de entidad (archivo) - es preferible especificar el tipo de entidad exacto dentro de las comillas. Por ejemplo *“txt”*.
- **Ruta** de la entidad - Los filtros de ruta de directorio (cadena de ruta que termina con /) hasta 4 directorios de profundidad se recomiendan para obtener resultados más rápidos. Por ejemplo, *”/home/userX/nested1/nested2/”*. Consulte la siguiente tabla para obtener más información.
- Carpeta de nivel 1st (raíz) - Directorio raíz de la ruta de la entidad como filtros. Por ejemplo, si la ruta de acceso de la entidad es /home/userX/nested1/nested2/, se puede utilizar home O home.
- Carpeta de nivel 2nd - Directorio de nivel 2nd de los filtros de ruta de la entidad. Por ejemplo, si la ruta de acceso de la entidad es /home/userX/nested1/nested2/, entonces userX O “userX” se puede utilizar.
- Carpeta de nivel 3rd: Directorio de nivel 3rd de los filtros de ruta de la entidad.
- Por ejemplo, si la ruta de acceso de la entidad es /home/userX/nested1/nested2/, entonces nested1 O “nested1” se pueden utilizar.
- Carpeta de nivel 4th - Directorio de nivel 4th de los filtros de ruta de la entidad. Por ejemplo, si la ruta de acceso de la entidad es /home/userX/nested1/nested2/, entonces nested2 O “nested2” se pueden utilizar.
- **Usuario** realizando la actividad - es preferible especificar el usuario exacto dentro de las comillas. Por ejemplo, _ “Administrador”_.
- **Dispositivo** (SVM) donde residen las entidades
- **Volumen** donde residen las entidades
- La **Ruta original** se utiliza para cambiar el nombre de los eventos cuando se cambió el nombre del archivo original.

Los campos anteriores están sujetos a lo siguiente al filtrar:

- El valor exacto debe estar entre comillas: Ejemplo: "searchtext"
- Las cadenas con caracteres comodín no deben contener comillas: Ejemplo: searchtext, *searchtext*, filtrará las cadenas que contengan ‘reconfigurar texto’.
- Cadena con un prefijo, ejemplo: searchtext* , buscará cualquier cadena que comience por ‘reconfigurar texto’.

Ejemplos de filtros forenses de actividades:

Expresión de filtro aplicada por el usuario	Resultado esperado	Evaluación del rendimiento	Comentar
Path = «/home/userX/nested1/nested2/»	Búsqueda recursiva de todos los archivos y carpetas en el directorio dado	Y rápido	Las búsquedas en directorios de hasta 4 directorios serán rápidas.

Expresión de filtro aplicada por el usuario	Resultado esperado	Evaluación del rendimiento	Comentar
Ruta = «/home/userX/nested1/»	Búsqueda recursiva de todos los archivos y carpetas en el directorio dado	Y rápido	Las búsquedas en directorios de hasta 4 directorios serán rápidas.
Path = “/home/userX/nested1/test”	Búsqueda recursiva de todos los archivos y carpetas bajo la ruta de acceso regex (prueba* podría significar archivo O directorio O ambos)	Más lento	La búsqueda de directorio+archivo regex será más lenta en comparación con las búsquedas de directorio.
Path = «/home/userX/nested1/nested2/nested3/»	Búsqueda recursiva de todos los archivos y carpetas en el directorio dado	Más lento	Más de 4 búsquedas de directorios son más lentas para realizar búsquedas.
Cualquier otro filtro no basado en ruta. Filtros de tipo de usuario y entidad recomendados para estar entre comillas, por ejemplo, User= “Administrator” Entity Type= “txt”		Y rápido	

NOTA:

1. El recuento de actividades que se muestra junto al icono Todas las actividades se redondea a 30 minutos cuando el intervalo de tiempo seleccionado abarca más de 3 días. Por ejemplo, un intervalo de tiempo de *sept 1st 10:15 am a sept 7th 10:15 am* mostrará recuentos de actividades desde sept 1st 10:00 am hasta sept 7th 10:30 am.
2. Del mismo modo, las métricas de recuento que se muestran en el gráfico Historial de actividades se redondean a 30 minutos cuando el intervalo de tiempo seleccionado abarca más de 3 días.

Ordenar datos del historial de actividades forenses

Puede ordenar los datos del historial de actividades por *Tiempo, Usuario, IP de origen, Actividad,*, *Tipo de entidad*, Carpeta de 1st niveles (raíz), Carpeta de 2nd niveles, Carpeta de 3rd niveles y Carpeta de 4th niveles. De forma predeterminada, la tabla se ordena por orden *time* descendente, lo que significa que los datos más recientes se mostrarán primero. La ordenación está desactivada para los campos *Device* y *Protocol*.

Guía de usuario para exportaciones asíncronas

Descripción general

La función de exportaciones asíncronas de Storage Workload Security está diseñada para gestionar grandes exportaciones de datos.

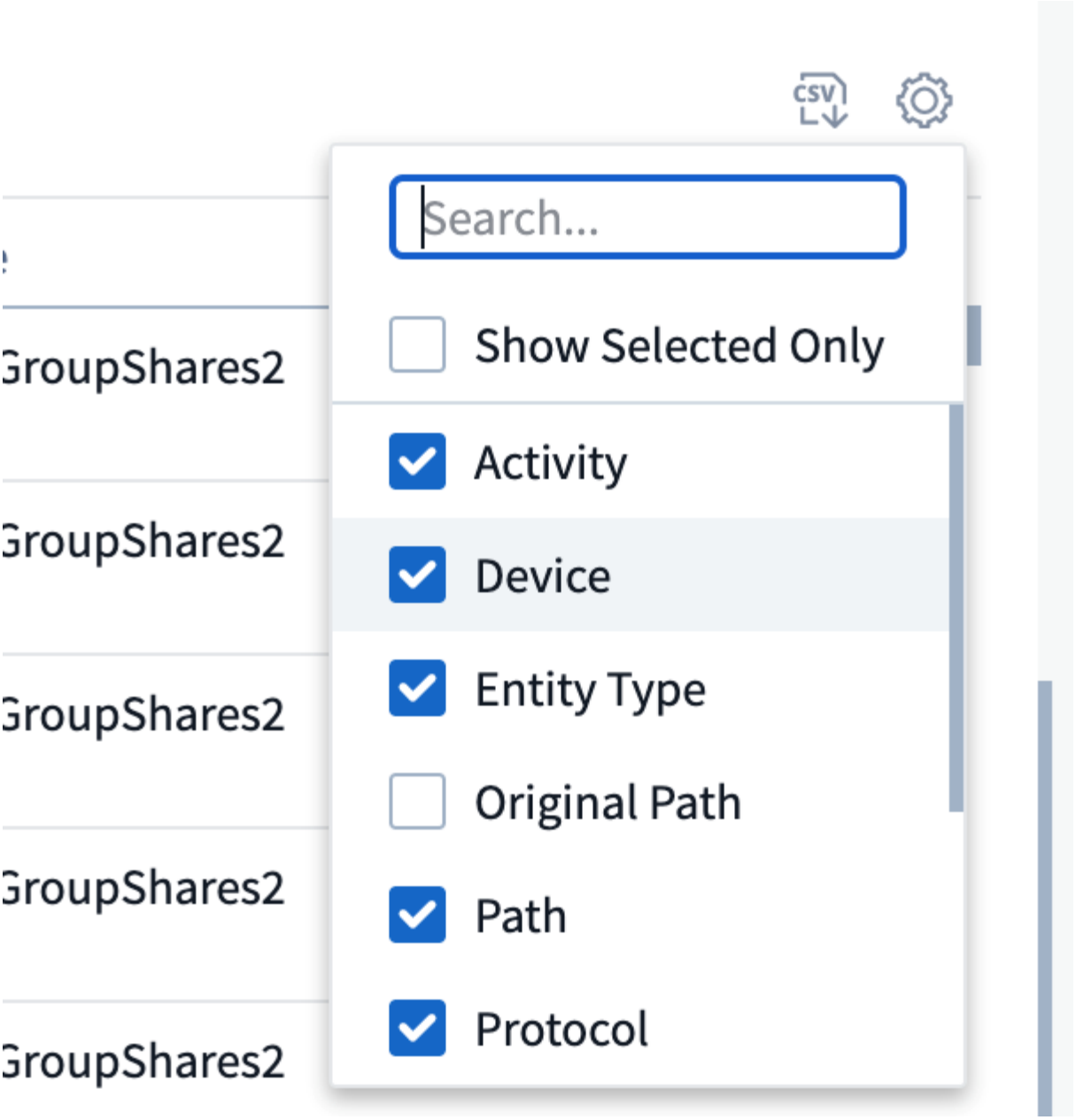
Guía paso a paso: Exportación de datos con exportaciones asíncronas

1. **Iniciar exportación**: Seleccione la duración de tiempo y los filtros deseados para la exportación y haga clic en el botón de exportación.
2. **Espere a que se complete la exportación**: El tiempo de procesamiento puede variar de unos minutos a unas pocas horas. Es posible que tenga que actualizar la página de análisis forense unas cuantas veces. Una vez finalizado el trabajo de exportación, se activará el botón Descargar último archivo CSV de exportación.
3. **Descargar**: Haga clic en el botón “Descargar último archivo de exportación creado” para obtener los datos exportados en un formato .zip. Estos datos estarán disponibles para su descarga hasta que el usuario inicie otra exportación asíncrona o hayan transcurrido 3 días, lo que ocurra primero. El botón permanecerá activado hasta que se inicie otra exportación asíncrona.
4. **Limitaciones**:
    - El número de descargas asíncronas está limitado actualmente a 1 por usuario y 3 por inquilino.
    - Los datos exportados están limitados a un máximo de 1 millones de registros.

Un script de ejemplo para extraer datos forenses a través de API está presente en */opt/NetApp/cloudsecure/agent/export-script/* en el agente. Consulte el archivo Léame en esta ubicación para obtener más información sobre el script.

Selección de columna para toda la actividad

La tabla *All Activity* muestra las columnas SELECT de forma predeterminada. Para agregar, eliminar o cambiar las columnas, haga clic en el icono de engranaje situado a la derecha de la tabla y seleccione una de las columnas disponibles.



Retención del historial de actividades

El historial de actividad se conserva durante 13 meses para entornos de seguridad de carga de trabajo activa.

Aplicabilidad de los filtros en la página Forensics

Filtro	Qué hace	Ejemplo	Aplicable a estos filtros	No aplicable a estos filtros	Resultado
* (Asterisk)	le permite buscar todo	Auto*03172022 Si el texto de búsqueda contiene guiones o guiones bajos, dar expresión entre paréntesis, por ejemplo, (svm*) para buscar svm-123	Usuario, Tipo de entidad, Dispositivo, Volumen, Ruta original, Carpeta 1stLevel, Carpeta 2ndLevel, Carpeta 3rdlevel, Carpeta 4thLevel		Devuelve todos los recursos que comienzan con “Auto” y terminan con “03172022”
? (signo de interrogación)	le permite buscar un número específico de caracteres	AutoSabotageUser1_03172022?	Usuario, Tipo de entidad, Dispositivo, Volumen, Carpeta 1stLevel, Carpeta 2ndLevel, Carpeta 3rdlevel, Carpeta 4thLevel		Devuelve AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022B, AutoSabotageUser1_031720225, etc.
O.	permite especificar varias entidades	AutoSabotageUser1_03172022 o AutoRansomUser4_03162022	Usuario, Dominio, Tipo de entidad, Ruta de acceso original		Devuelve cualquiera de los valores de AutoSabotageUser1_03172022 O AutoRansomUser4_03162022
NO	permite excluir el texto de los resultados de la búsqueda	NO es AutoRansomero4_03162022	Usuario, Dominio, Tipo de entidad, Ruta original, Carpeta 1stLevel, Carpeta 2ndLevel, Carpeta 3rdlevel, Carpeta 4thLevel	Dispositivo	Devuelve todo lo que no empieza con"AutoRansomUser4_03162022"
Ninguno	Busca valores NULL en todos los campos	Ninguno	Dominio		devuelve los resultados en los que el campo de destino está vacío

Ruta / Búsqueda de ruta original

Los resultados de búsqueda con y sin / serán diferentes

"/AutoDir1/Autofile03242022"	Solo funciona la búsqueda exacta; devuelve todas las actividades con la ruta exacta como /AutoDir1/AutoFile03242022 (caso insensible)
«/AutoDir1/ »	Funciona; devuelve todas las actividades con un directorio de 1st niveles que coincide con AutoDir1 (caso insensible)
«/AutoDir1/AutoFile03242022/ »	Funciona; devuelve todas las actividades con un directorio de 1st niveles que coincide con el directorio de AutoDir1 y 2nd niveles que coincide con AutoFile03242022 (sin sensibilidad)
/AutoDir1/AutoFile03242022 O /AutoDir1/AutoFile03242022	No funciona
NO /AutoDir1/AutoFile03242022	No funciona
NO /AutoDir1	No funciona
NO /Autofile03242022	No funciona
*	No funciona

Cambios en la actividad de un usuario raíz SVM local

Si un usuario de SVM raíz local realiza alguna actividad, la IP del cliente en el que se monta el recurso compartido de NFS ahora se considera en el nombre de usuario, que se mostrará como root@<ip-address-of-the-client> tanto en las páginas de actividad forense como de actividad del usuario.

Por ejemplo:

- Si SVM-1 se supervisa mediante Workload Security, y el usuario raíz de esa SVM monta el recurso compartido en un cliente con la dirección IP 10.197.12.40, el nombre de usuario que se muestra en la página de actividad forense será *root@10.197.12.40*.
- Si se monta el mismo SVM-1 en otro cliente con la dirección IP 10.197.12.41, el nombre de usuario que se muestra en la página de actividad forense será *root@10.197.12.41*.

*• Esto se hace para segregar la actividad del usuario raíz NFS por dirección IP. Anteriormente, toda la actividad se consideraba realizada únicamente por *root* usuario, sin distinción de IP.

Resolución de problemas

Problema	Pruebe esto

En la tabla "todas las actividades", bajo la columna "Usuario", el nombre de usuario se muestra como: "ldap:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817” o "ldap:default:80038003"	Las posibles razones pueden ser: 1. Aún no se ha configurado ningún colimador de directorios de usuarios. Para agregar uno, vaya a **Workload Security > Collectors > User Directory Collectors** y haga clic en **+User Directory Collector**. Seleccione *Active Directory* o *LDAP Directory Server*. 2. Se ha configurado un recopilador de directorios de usuario, sin embargo, se ha detenido o está en estado de error. Vaya a **Colectores > Colectores de directorios de usuarios** y compruebe el estado. Consulte "Solución de problemas del recopilador de directorios de usuarios"la sección de la documentación para obtener consejos sobre solución de problemas. Una vez configurada correctamente, el nombre se resolverá automáticamente en 24 horas. Si todavía no se resuelve, compruebe si ha agregado el recopilador de datos de usuario correcto. Asegúrese de que el usuario forma parte del servidor de directorio de Active Directory/LDAP agregado.
Algunos eventos de NFS no se ven en la interfaz de usuario de.	Compruebe lo siguiente: 1. Se debe ejecutar un recopilador de directorios de usuarios para el servidor AD con el conjunto de atributos POSIX con el atributo unixid habilitado desde la interfaz de usuario. 2. Cualquier usuario que haga acceso a NFS debe verse cuando se busque en la página de usuario desde UI 3. Los eventos sin formato (los eventos para los que aún no se ha detectado el usuario) no son compatibles con NFS 4. El acceso anónimo a la exportación de NFS no se supervisará. 5. Asegúrese de que la versión de NFS se utiliza en menos de NFS4,1.
Después de escribir algunas letras que contienen un carácter comodín como asterisco (*) en los filtros de las páginas Forensics *All Activity* o *entities*, las páginas se cargan muy lentamente.	Un asterisco (*) en la cadena de búsqueda busca todo. Sin embargo, las cadenas comodín iniciales como **<searchTerm>* o **<searchTerm>** resultarán en una consulta lenta. Para obtener un mejor rendimiento, utilice cadenas de prefijo en su lugar, en el formato *<searchTerm>** (en otras palabras, agregue el asterisco (*) *after* un término de búsqueda). Ejemplo: Utilice la cadena *testvolume**, en lugar de **testvolume* o **test*volume*. Utilice una búsqueda de directorio para ver todas las actividades debajo de una carpeta dada de forma recursiva (búsqueda jerárquica). Por ejemplo, “/path1/path2/path3/” enumerará todas las actividades de forma recursiva en /path1/path2/path3. Alternativamente, use la opción “Agregar a filtro” en la pestaña Todas las actividades.”
Encuentro un error de solicitud fallida con el código de estado 500/503 al utilizar un filtro de ruta.	Intente utilizar un rango de fechas más pequeño para filtrar registros.

La interfaz de usuario forense carga los datos lentamente cuando se utiliza el filtro *PATH*.	Se recomiendan filtros de ruta de directorio (cadena de ruta que termina con /) de hasta 4 directorios de profundidad para obtener resultados más rápidos. Por ejemplo, si la ruta de directorio es /AAA/BBB/CCC/DDD, intente buscar "/AAA/BBB/CCC/DDD/" para cargar datos más rápido.

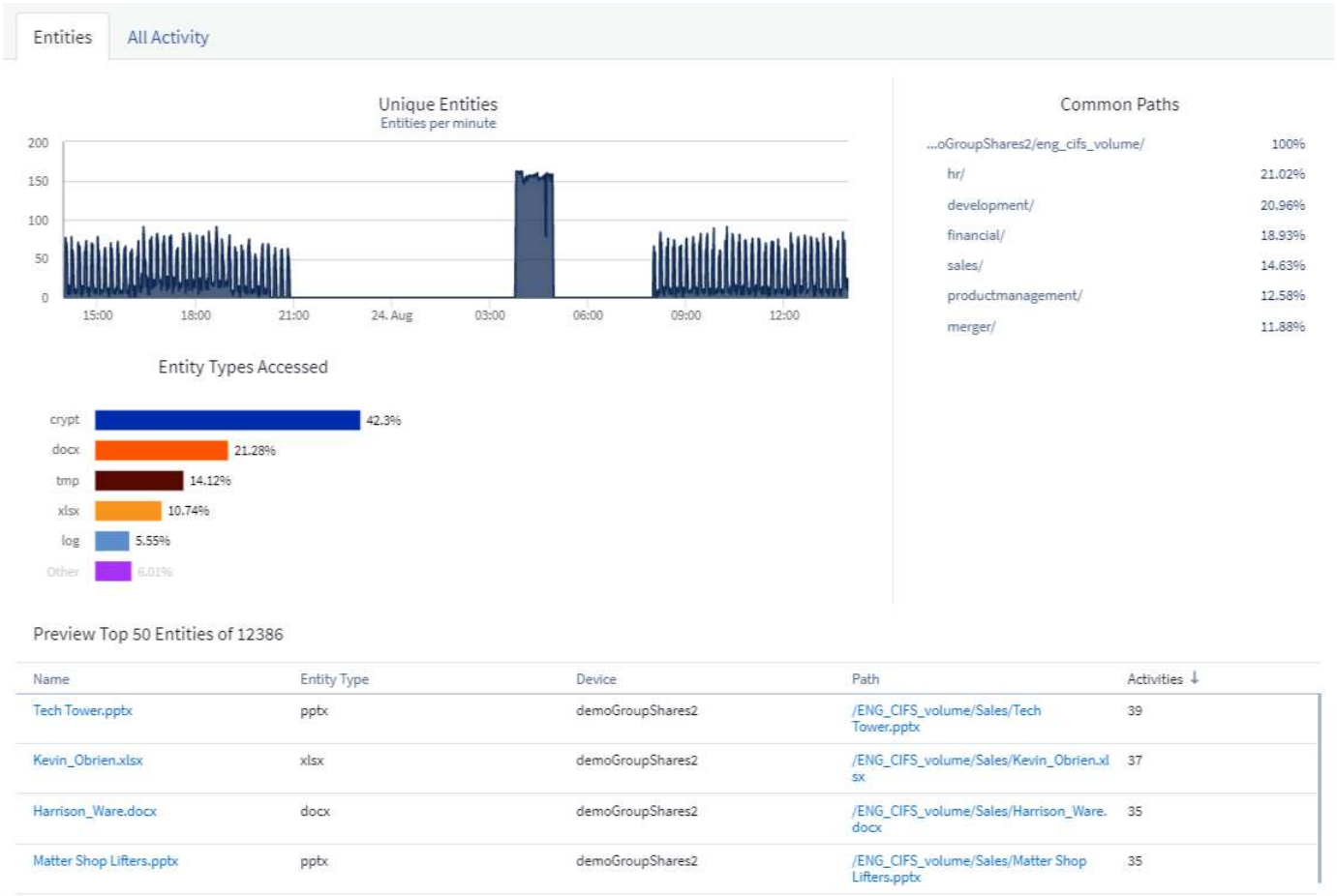
Página de entidades forenses

La página Entidades de Forensics proporciona información detallada sobre la actividad de la entidad en su arrendatario.

Examen de la Información de entidad

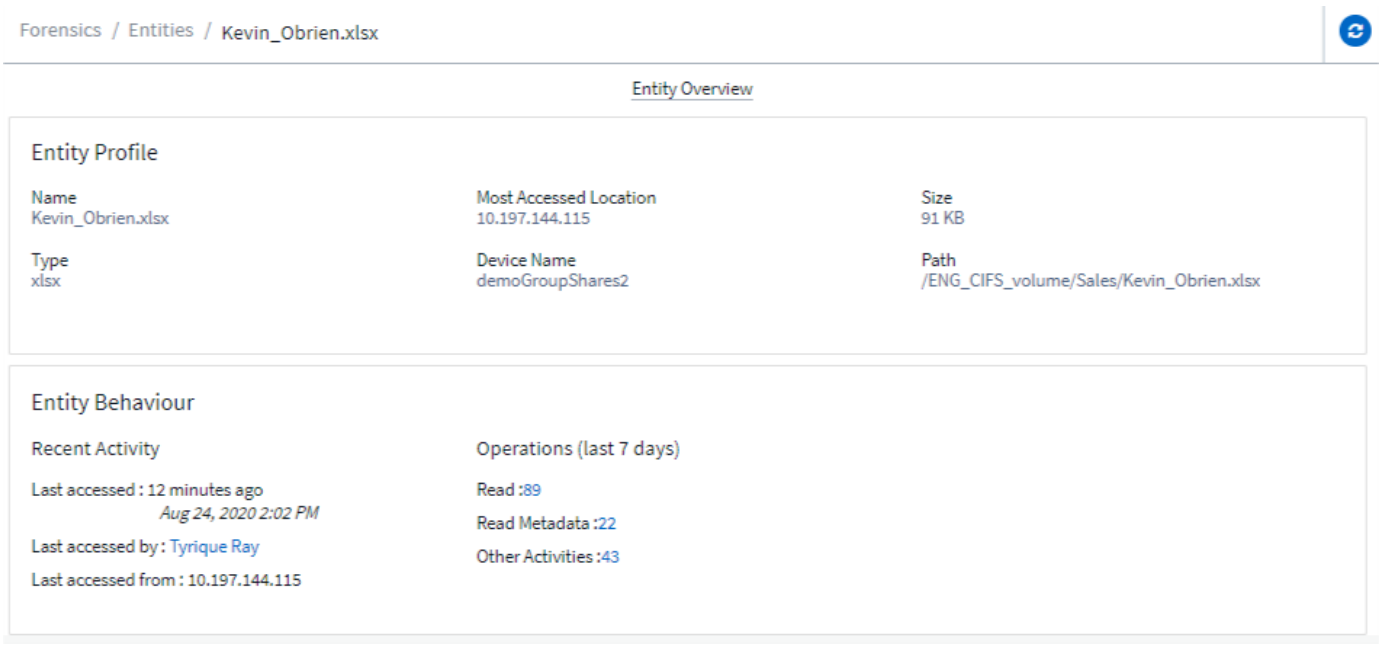
Haga clic en **Forensics > Activity Forensics** y haga clic en la ficha *Entities* para acceder a la página de entidades.

Esta página proporciona una descripción general de la actividad de la entidad en su arrendatario, resaltando la siguiente información: * Un gráfico que muestra *Entidades únicas* accedidas por minuto * Un gráfico de *Tipos de Entidad accedidos* * Un desglose de las *Rutas comunes* * Una lista de las *50 entidades principales* del número total de entidades



Al hacer clic en una entidad de la lista se abre una página de resumen de la entidad, mostrando un perfil de la entidad con detalles como nombre, tipo, nombre del dispositivo, dirección IP de la ubicación y ruta de acceso a los que se accede más, así como el comportamiento de la entidad, como el usuario, la dirección IP, y hora a

la que se accedió por última vez a la entidad.



Descripción general del usuario forense

La información de cada usuario se proporciona en la sección Información general del usuario. Utilice estas vistas para comprender las características del usuario, las entidades asociadas y las actividades recientes.

Perfil de usuario

La información del perfil de usuario incluye la información de contacto y la ubicación del usuario. El perfil proporciona la siguiente información:

- Nombre del usuario
- Dirección de correo electrónico del usuario
- Administrador del usuario
- Contacto telefónico para el usuario
- Ubicación del usuario

Comportamiento del usuario

La información sobre el comportamiento del usuario identifica las actividades y operaciones recientes realizadas por el usuario. Esta información incluye:

- Actividad reciente
  - Última ubicación de acceso
  - Gráfico de actividades
  - Alertas
- Operaciones de los últimos siete días

- Cantidad de operaciones

Actualizar intervalo

La lista de usuarios se actualiza cada 12 horas.

Política de retención

Si no se vuelve a actualizar, la lista de usuarios se conserva durante 13 meses. Después de 13 meses, los datos se eliminarán. Si se elimina el entorno Workload Security, se eliminan todos los datos asociados con el entorno.

Información de copyright

Información de la marca comercial