Seguridad de cargas de trabajo

Data Infrastructure Insights

NetApp
December 19, 2024

Tabla de contenidos

Seguridad de cargas de trabajo

Acerca de la seguridad de carga de trabajo de almacenamiento

Información de la infraestructura de datos Seguridad de cargas de trabajo del almacenamiento (anteriormente Cloud Secure) ayuda a proteger sus datos con inteligencia procesable sobre amenazas internas. Proporciona control y visibilidad centralizados de todos los accesos a datos corporativos en los entornos de cloud híbrido para garantizar la consecución de los objetivos de seguridad y cumplimiento de normativas.

Visibilidad

Obtenga una visibilidad y control centralizados del acceso del usuario a los datos corporativos más importantes almacenados en sus instalaciones o en el cloud.

Sustituye herramientas y procesos manuales que no ofrecen una visibilidad precisa y puntual del acceso a los datos y el control. Workload Security funciona de forma única en sistemas de almacenamiento en la nube y en las instalaciones para proporcionar alertas en tiempo real sobre el comportamiento de los usuarios malintencionados.

Protección

Proteja los datos de su organización frente a un uso inadecuado por parte de usuarios malintencionados o en riesgo mediante el aprendizaje automático avanzado y la detección de anomalías.

Le avisa de cualquier acceso anormal a los datos mediante el aprendizaje automático avanzado y la detección de anomalías en el comportamiento del usuario.

Cumplimiento de normativas

Garantice el cumplimiento de normativas de la empresa mediante la auditoría del acceso de los usuarios a los datos confidenciales de la empresa almacenados en las instalaciones o en el cloud.

Primeros pasos

Introducción a Workload Security

Hay tareas de configuración que se deben completar antes de empezar a utilizar Workload Security para supervisar la actividad del usuario.

El sistema Workload Security utiliza un agente para recopilar datos de acceso de los sistemas de almacenamiento e información de usuario de los servidores de Directory Services.

Es necesario configurar lo siguiente para poder comenzar a recoger datos:

Tarea	Información relacionada

Configure un agente	"Requisitos del agente" "Agregar agente" "**Video**: Implementación del agente"
Configurar un conector de directorio de usuarios	"Agregar conector de directorio de usuario" "**Vídeo**: Conexión a Active Directory"
Configurar recopiladores de datos	Haga clic en **Workload Security > Collectors** en el recopilador de datos que desea configurar. Consulte la sección de referencia del proveedor del recopilador de datos de la documentación. "**Vídeo**: Conexión ONTAP SVM"
Crear cuentas de usuarios	"Gestionar cuentas de usuario"
Resolución de problemas	"**Vídeo**: Solución de problemas"

La seguridad de la carga de trabajo también se puede integrar con otras herramientas. Por ejemplo, "consulte esta guía" en la integración con Splunk.

Requisitos del agente de seguridad de cargas de trabajo

Debe "Instale un agente"adquirir información de sus recopiladores de datos. Antes de instalar el agente, debe asegurarse de que su entorno cumple con los requisitos de sistema operativo, CPU, memoria y espacio en disco.

Componente	Requisitos de Linux
De NetApp	Un equipo que ejecute una versión con licencia de uno de los siguientes: * CentOS 64 64 64 24,04 11 9,4 Stream (64 9,2 15 SP3 20,04 64 64 64 bits), CentOS 9 9,4 15 SP5 22,04 10 9,3 Stream, SELinux * OpenSUSE Leap 8,8 a 64 (64 bits) * Oracle Linux 8,6 - 8,8, 9,1 a 9,4 (15,5 bits) * Red Hat Enterprise Linux 8,6 a 15,3, 9,1 a 9,4 (8 bits) Se recomienda un servidor dedicado.
Comandos	para la instalación es necesario descomprimir. Además, se requiere el comando 'efectuar su –' para la instalación, la ejecución de scripts y la desinstalación.
CPU	4 núcleos de CPU
Memoria	16 GB DE MEMORIA RAM

Componente	Requisitos de Linux
Espacio disponible en disco	El espacio en disco se debe asignar de esta manera: /Opt/NetApp 36 GB (mínimo 35 GB de espacio libre después de la creación del sistema de archivos) Nota: Se recomienda asignar un poco de espacio adicional en disco para permitir la creación del sistema de archivos. Asegúrese de que hay al menos 35 GB de espacio libre en el sistema de archivos. Si /opt es una carpeta montada de un almacenamiento NAS, asegúrese de que los usuarios locales tengan acceso a esta carpeta. Es posible que el agente o el recopilador de datos no se puedan instalar si los usuarios locales no tienen permiso para esta carpeta. Consulte "resolución de problemas"la sección para obtener más información.
Red	Conexión Ethernet de 100 Mbps a 1 Gbps, dirección IP estática, conectividad IP con todos los dispositivos y un puerto requerido para la instancia de seguridad de carga de trabajo (80 o 443).

Tenga en cuenta que el agente de seguridad de carga de trabajo se puede instalar en el mismo equipo que una unidad de adquisición y/o agente de Data Infrastructure Insights. Sin embargo, es una mejor práctica instalar estos en máquinas independientes. En el caso de que se instalen en el mismo equipo, asigne espacio en disco como se muestra a continuación:

Espacio disponible en disco	50-55 GB para Linux, el espacio en disco se debe asignar de esta manera: /Opt/netapp 25-30 GB /var/log/netapp 25 GB

Recomendaciones adicionales

- Se recomienda encarecidamente sincronizar el tiempo tanto en el sistema ONTAP como en la máquina del agente mediante **Protocolo de tiempo de red (NTP)** o **Protocolo simple de tiempo de red (SNTP)**.

Reglas de acceso a la red de cloud

Para entornos de seguridad de cargas de trabajo **basados en EE.UU.**:

Protocolo	Puerto	Origen	Destino	Descripción
TCP	443	Agente de Seguridad de Carga de Trabajo	<site_name>.cs01.cloudinsights.netapp.com <site_name>.c01.cloudinsights.netapp.com <site_name>.c02.cloudinsights.netapp.com	Acceso a Información sobre la infraestructura de datos
TCP	443	Agente de Seguridad de Carga de Trabajo	gateway.c01.cloudinsights.netapp.com agentlogin.cs01.cloudinsights.netapp.com	Acceso a los servicios de autenticación

Para entornos de seguridad de cargas de trabajo * basados en Europa:

Protocolo	Puerto	Origen	Destino	Descripción
TCP	443	Agente de Seguridad de Carga de Trabajo	<site_name>.cs01-eu-1.cloudinsights.netapp.com <site_name>.c01-eu-1.cloudinsights.netapp.com <site_name>.c02-eu-1.cloudinsights.netapp.com	Acceso a Información sobre la infraestructura de datos
TCP	443	Agente de Seguridad de Carga de Trabajo	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-eu-1.cloudinsights.netapp.com	Acceso a los servicios de autenticación

Para entornos de seguridad de cargas de trabajo * basados en APAC*:

Protocolo	Puerto	Origen	Destino	Descripción
TCP	443	Agente de Seguridad de Carga de Trabajo	<site_name>.cs01-ap-1.cloudinsights.netapp.com <site_name>.c01-ap-1.cloudinsights.netapp.com <site_name>.c02-ap-1.cloudinsights.netapp.com	Acceso a Información sobre la infraestructura de datos
TCP	443	Agente de Seguridad de Carga de Trabajo	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-ap-1.cloudinsights.netapp.com	Acceso a los servicios de autenticación

Reglas dentro de la red

Protocolo	Puerto	Origen	Destino	Descripción
TCP	389(LDAP) 636 (LDAPS / start-tls)	Agente de Seguridad de Carga de Trabajo	URL del servidor LDAP	Conéctese a LDAP

Protocolo	Puerto	Origen	Destino	Descripción
TCP	443	Agente de Seguridad de Carga de Trabajo	Dirección IP de gestión del clúster o de SVM (según la configuración del recopilador SVM)	Comunicación API con ONTAP
TCP	35000 - 55000	Direcciones IP de LIF de datos de SVM	Agente de Seguridad de Carga de Trabajo	Comunicación de ONTAP al agente de seguridad de carga de trabajo para eventos de Fpolicy. Estos puertos deben abrirse hacia el agente de seguridad de carga de trabajo para que ONTAP le envíe eventos, incluido cualquier firewall del propio agente de seguridad de carga de trabajo (si está presente). TENGA EN CUENTA que no es necesario reservar **todos** de estos puertos, pero los puertos que reserve para esto deben estar dentro de este rango. Se recomienda comenzar reservando ~100 puertos y aumentando si es necesario.
TCP	7	Agente de Seguridad de Carga de Trabajo	Direcciones IP de LIF de datos de SVM	Eco del agente a los LIF de datos de SVM
SSH	22	Agente de Seguridad de Carga de Trabajo	Gestión de clústeres	Necesario para el bloqueo de usuarios CIFS/SMB.

Ajuste de tamaño del sistema

Consulte "Comprobador de frecuencia de eventos" la documentación para obtener información sobre la configuración de tamaño.

Instalación de Workload Security Agent

Workload Security (anteriormente Cloud Secure) recopila datos de actividad de usuario mediante uno o más agentes. Los agentes se conectan a los dispositivos de su inquilino y recopilan los datos que se envían a la capa de SaaS Workload Security para su análisis. Consulte "Requisitos del agente" para configurar una VM de agente.

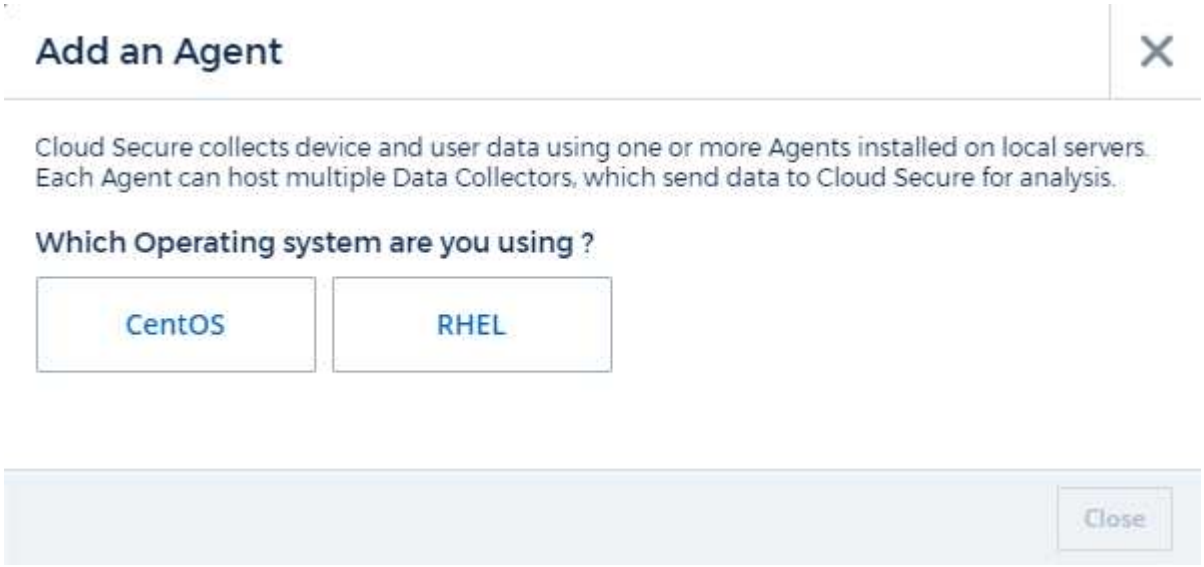
Antes de empezar

- Se requiere el privilegio sudo para la instalación, la ejecución de scripts y la desinstalación.
- Al instalar el agente, se crean en el equipo un usuario local *cssys* y un grupo local *cssys*. Si la configuración de permisos no permite la creación de un usuario local y, en su lugar, requiere Active Directory, se debe crear un usuario con el nombre de usuario *cssys* en el servidor de Active Directory.
- Puede leer sobre la seguridad de Data Infrastructure Insights "aquí".

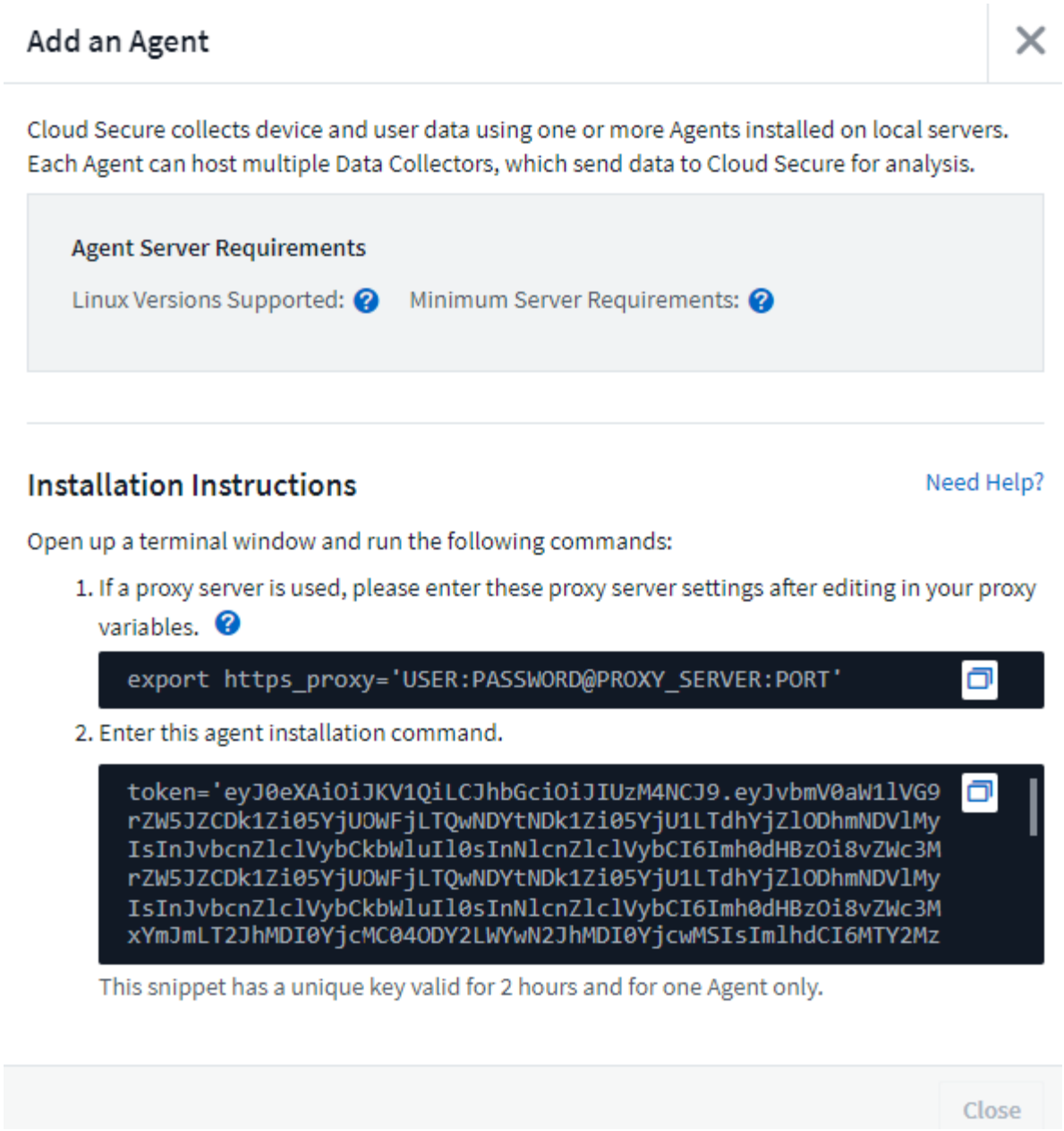
Pasos para instalar el agente

1. Inicie sesión como administrador o propietario de cuenta en su entorno de seguridad de carga de trabajo.
2. Selecciona **Colectores > Agentes > +Agente**

   El sistema muestra la página Agregar un agente:



3. Compruebe que el servidor de agentes cumple los requisitos mínimos del sistema.
4. Para comprobar que el servidor de agentes está ejecutando una versión compatible de Linux, haga clic en *version soportadas (i)*.
5. Si la red utiliza un servidor proxy, defina los detalles del servidor proxy siguiendo las instrucciones de la sección Proxy .



6. Haga clic en el icono Copiar al Portapapeles para copiar el comando de instalación.
7. Ejecute el comando de instalación en una ventana de terminal.
8. El sistema muestra el siguiente mensaje cuando la instalación se completa correctamente:

Después de terminar

1. Debe configurar un "Recopilador de directorios de usuarios".
2. Debe configurar uno o más colectores de datos.

Configuración de red

Ejecute los siguientes comandos en el sistema local para abrir puertos que utilizará Workload Security. Si existe un problema de seguridad con respecto al intervalo de puertos, puede utilizar un intervalo de puertos menor, por ejemplo *35000:35100*. Cada SVM utiliza dos puertos.

Pasos

1. `sudo firewall-cmd --permanent --zone=public --add-port=35000-55000/tcp`
2. `sudo firewall-cmd --reload`

Siga los pasos que se indican a continuación en función de su plataforma:

CentOS 7.x / RHEL 7.x:

1. `sudo iptables-save | grep 35000`

Salida de muestra:

```
 -A IN_public_allow -p tcp -m tcp --dport 35000:55000 -m conntrack
-ctstate NEW,UNTRACKED -j ACCEPT
*CentOS 8.x / RHEL 8.x*:
```

1. `sudo firewall-cmd --zone=public --list-ports | grep 35000` (Para CentOS 8)

Salida de muestra:

```
35000-55000/tcp
```

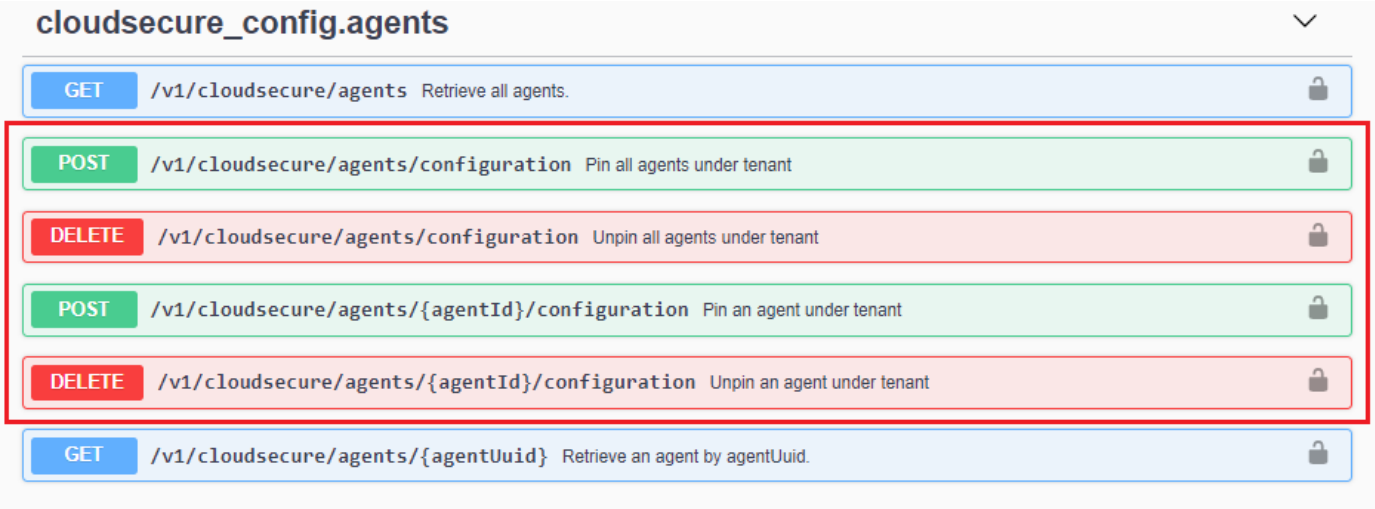
'Anclar' a un agente en la versión actual

De forma predeterminada, Data Infrastructure Insights Workload Security actualiza los agentes automáticamente. Es posible que algunos clientes deseen pausar la actualización automática, lo que deja a un agente en su versión actual hasta que ocurra una de las siguientes acciones:

- El cliente reanuda las actualizaciones automáticas del agente.
- han pasado 30 días. Tenga en cuenta que los 30 días comienzan el día de la actualización más reciente del agente, no el día en que se pone en pausa el agente.

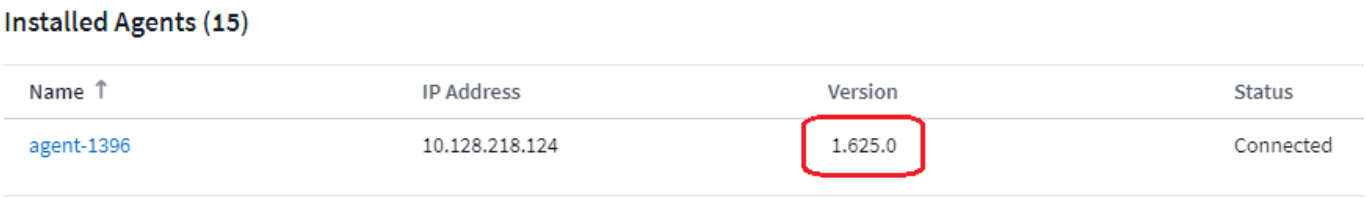
En cada uno de estos casos, el agente se actualizará en la siguiente actualización de seguridad de carga de trabajo.

Para pausar o reanudar las actualizaciones automáticas del agente, utilice las API *cloudsecure_config.agents*:



Tenga en cuenta que la acción de pausa o reanudación puede tardar hasta cinco minutos en aplicarse.

Puede ver las versiones actuales de su agente en la página **Seguridad de carga de trabajo > Colectores**, en la pestaña **Agentes**.



Solución de problemas de errores del agente

Los problemas conocidos y sus resoluciones se describen en la siguiente tabla.

Problema:	Resolución:
La instalación del agente no puede crear la carpeta /opt/netapp/cloudsecure/agent/logs/agent.log y el archivo install.log no proporciona información relevante.	Este error se produce durante el arranque del agente. El error no se registra en los archivos de registro porque se produce antes de inicializar el registrador. El error se redirige a la salida estándar y es visible en el registro de servicio mediante `journalctl -u cloudsecure-agent.service` el comando. Este comando se puede utilizar para solucionar el problema con más detalle. est
Se produce un error en la instalación del agente con ‘esta distribución de linux no es compatible. Salir de la instalación».	Este error aparece cuando intenta instalar el agente en un sistema no compatible. Consulte "Requisitos del agente".
Error en la instalación del agente: "-bash: Unzip: Command not found"	Instale unzip y ejecute de nuevo el comando de instalación. Si se instala Yum en la máquina, intente “yum install unzip” para instalar el software de descompresión. Después, vuelva a copiar el comando desde la interfaz de usuario de instalación del agente y péguelo en la CLI para volver a ejecutar la instalación.

Problema:	Resolución:
El agente se ha instalado y se estaba ejecutando. Sin embargo, el agente se ha detenido repentinamente.	SSH a la máquina del agente. Compruebe el estado del servicio del agente a través de `sudo systemctl status cloudsecure-agent.service`. 1. Compruebe si los logs muestran un mensaje “Error al iniciar el servicio de daemon de seguridad de carga de trabajo” . 2. Compruebe si el usuario cssys existe en la máquina del agente o no. Ejecute uno por uno los siguientes comandos con permiso root y compruebe si el usuario y grupo cssys existe. `sudo id cssys` `sudo groups cssys` 3. Si no existe ninguna, una política de supervisión centralizada puede haber suprimido el usuario cssys. 4. Cree el usuario y el grupo cssys manualmente ejecutando los siguientes comandos. `sudo useradd cssys` `sudo groupadd cssys` 5. Reinicie el servicio del agente después de eso ejecutando el siguiente comando `sudo systemctl restart cloudsecure-agent.service`: 6. Si aún no se está ejecutando, compruebe las otras opciones de solución de problemas.
No se pueden agregar más de 50 recopiladores de datos a un agente.	Sólo se pueden agregar 50 recopiladores de datos a un agente. Puede ser una combinación de todos los tipos de recopilador, por ejemplo, Active Directory, SVM y otros recopiladores.
La interfaz de usuario muestra que el agente está en estado NOT_CONNECTED.	Pasos para reiniciar el agente. 1. SSH a la máquina del agente. 2. Reinicie el servicio del agente después de eso ejecutando el siguiente comando `sudo systemctl restart cloudsecure-agent.service`: 3. Compruebe el estado del servicio del agente a través de `sudo systemctl status cloudsecure-agent.service`. 4. El agente debe pasar al estado CONECTADO.
El agente VM se encuentra detrás del proxy Zscaler y la instalación del agente falla. Debido a la inspección SSL del proxy de Zscaler, los certificados de seguridad de carga de trabajo se presentan como firmados por la CA de Zscaler, por lo que el agente no confía en la comunicación.	Desactive la inspección SSL en el proxy Zscaler para la URL *.cloudinsights.netapp.com. Si Zscaler realiza una inspección SSL y reemplaza los certificados, Workload Security no funcionará.

Problema:	Resolución:
Durante la instalación del agente, la instalación se bloquea después de descomprimir.	El comando “chmod 755 -RF” está fallando. Se produce un error en el comando de instalación del agente cuando un usuario sudo no raíz que tiene archivos en el directorio de trabajo, que pertenecen a otro usuario y los permisos de esos archivos no se pueden cambiar. Debido al comando chmod que falla, el resto de la instalación no se ejecuta. 1. Crea un nuevo directorio llamado “cloudsecure”. 2. Vaya a ese directorio. 3. Copia y pega el comando de instalación completo “token=…… … ./cloudsecure-agent-install.sh” y presiona ENTER. 4. La instalación debe poder continuar.
Si aún no se puede conectar el agente a Saas, abra un caso con el soporte de NetApp. Proporcione el número de serie de Data Infrastructure Insights para abrir un caso y adjunte registros al caso según lo indicado.	Para adjuntar registros al caso: 1. Ejecute el siguiente script con permiso root y comparta el archivo de salida (cloudsecure-agent-symptoms.zip). a. /opt/NetApp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh 2. Ejecute los siguientes comandos uno a uno con permiso root y comparta la salida. a. id cssys b. groups cssys c. cat /etc/os-release
La secuencia de comandos cloudsecure-agent-symptom-collector.sh falla con el siguiente error. [Root@machine tmp]# /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh recopilar registros de servicio recopilar registros de aplicación recopilar configuraciones de agente tomar instantánea de estado de servicio tomar instantánea de estructura de directorio del agente …… . …… . /Opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh: Línea 52: Zip: Comando no encontrado ERROR: No se pudo crear /tmp/cloudsecure-agent-symptoms.zip	La herramienta zip no está instalada. Instale la herramienta zip ejecutando el comando “yum install zip”. A continuación, vuelva a ejecutar el cloudsecure-agent-symptom-collector.sh.
La instalación del agente falla con useradd: No se puede crear el directorio /home/cssys	Este error puede ocurrir si el directorio de inicio de sesión del usuario no se puede crear en /home, debido a la falta de permisos. La solución sería crear un usuario cssys y agregar su directorio de inicio de sesión manualmente utilizando el siguiente comando: *Sudo useradd user_name -m -d HOME_DIR* -m :cree el directorio principal del usuario si no existe. -D : el nuevo usuario se crea utilizando HOME_DIR como valor para el directorio de inicio de sesión del usuario. Por ejemplo, *sudo useradd cssys -m -d /cssys*, agrega un usuario *cssys* y crea su directorio de inicio de sesión bajo root.

Problema:	Resolución:
El agente no se ejecuta después de la instalación. *Systemctl status cloudsecure-agent.service* muestra lo siguiente: [Root@demo ~]# systemctl status cloudsecure-agent.service agent.service – Workload Security Agent Daemon Service loaded: Loaded (/usr/lib/systemd/system/cloudsecure-agent.service; enabled; Vendor PRESET: Disabled) Active: Activate (auto-restart) (result: Exit-code) desde Tue 2021-08-03 21:12:26 PDT; ago Process: 25889 /bash/opt-Agent/Secure/bin=126/your_status= 25889 (code=salir, status=126), Aug 03 21:12:26 demo systemd[1]: cloudsecure-agent.service: proceso principal salida, code=salido, status=126/n/a Aug 03 21:12:26 demo systemd[1]: Unidad cloudsecure-agent.service entró en estado fallido. Aug 03 21:12:26 demo systemd[1]: cloudsecure-agent.service falló.	Esto puede estar fallando porque el usuario *cssys* puede no tener permiso para instalar. Si /opt/netapp es un montaje NFS y el usuario *cssys* no tiene acceso a esta carpeta, se producirá un error en la instalación. *Cssys* es un usuario local creado por el instalador de Workload Security que puede no tener permiso para acceder al recurso compartido montado. Puede comprobar esto intentando acceder a /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent usando *cssys* user. Si devuelve “permiso denegado”, el permiso de instalación no está presente. En lugar de una carpeta montada, instale en un directorio local de la máquina.
El agente se conectó inicialmente a través de un servidor proxy y el proxy se estableció durante la instalación del agente. Ahora el servidor proxy ha cambiado. ¿Cómo se puede cambiar la configuración del proxy del agente?	Puede editar el archivo agent.properties para agregar los detalles del proxy. Siga estos pasos: 1. Cambie a la carpeta que contiene el archivo de propiedades: cd /opt/netapp/cloudsecure/conf 2. Con su editor de texto favorito, abra el archivo *agent.properties* para editarlo. 3. Agregue o modifique las siguientes líneas: AGENT_PROXY_HOST=scspa1950329001.vm.NetApp.com AGENT_PROXY_PORT=80 AGENT_PROXY_USER=PXUSER AGENT_PROXY_PASSWORD=pass1234 4. Guarde el archivo. 5. Reinicie el agente: Sudo systemctl restart cloudsecure-agent.service

Eliminar un agente de seguridad de carga de trabajo

Al eliminar un agente de seguridad de carga de trabajo, primero deben eliminarse todos los recopiladores de datos asociados con el agente.

Eliminar un agente

Al eliminar un agente se eliminan todos los recopiladores de datos asociados al agente. Si planea configurar los recopiladores de datos con un agente diferente, debe crear una copia de seguridad de las configuraciones de recopilador de datos antes de eliminar el agente.

Antes de empezar

1. Asegúrese de que todos los recopiladores de datos asociados con el agente se eliminan del portal Workload Security.

   Nota: Ignore este paso si todos los recopiladores asociados están EN estado DETENIDO.

Pasos para eliminar un agente:

1. SSH en la VM del agente y ejecute el siguiente comando. Cuando se le solicite, introduzca "y" para continuar.

```
sudo /opt/netapp/cloudsecure/agent/install/cloudsecure-agent-
uninstall.sh
Uninstall CloudSecure Agent? [y|N]:
```

2. Haga clic en **Workload Security > Collectors > Agents**

   El sistema muestra la lista de agentes configurados.

3. Haga clic en el menú de opciones del agente que va a eliminar.
4. Haga clic en **Eliminar**.

   El sistema muestra la página **Eliminar agente**.

5. Haga clic en **Eliminar** para confirmar la eliminación.

Configurar un recopilador de directorios de usuarios de Active Directory (AD)

Workload Security se puede configurar para recopilar atributos de usuario desde los servidores de Active Directory.

Antes de empezar

- Debe ser un administrador de Data Infrastructure Insights o un propietario de la cuenta para realizar esta tarea.
- Debe tener la dirección IP del servidor donde se aloja el servidor de Active Directory.
- Debe configurar un agente antes de configurar un conector de directorio de usuario.

Pasos para configurar un recopilador de directorios de usuarios

1. En el menú Seguridad de la carga de trabajo, haga clic en: **Colectores > Colectores de directorios de usuarios > + Recopilador de directorios de usuarios** y seleccione **Active Directory**

   El sistema muestra la pantalla Agregar directorio de usuario.

Configure el colector de directorios de usuarios introduciendo los datos necesarios en las tablas siguientes:

Nombre	Descripción
Nombre	Nombre único del directorio de usuarios. Por ejemplo, *GlobalADCollector*
Agente	Seleccione un agente configurado de la lista
Nombre de dominio/IP del servidor	Dirección IP o nombre de dominio completo (FQDN) del servidor que aloja el directorio activo

Nombre del bosque	Nivel de bosque de la estructura de directorios. El nombre del bosque permite los dos formatos siguientes: *X. y.y.z* ⇒ nombre de dominio directo como lo tiene en su SVM. [Ejemplo: hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ nombres distintivos relativos [ejemplo: DC=hq,DC=companyname,DC=com] o puede especificar como lo siguiente: *OU=engineering,DC=hq,DC=companyname,DC=com* [para filtrar por ingeniería de OU específica] *CN=nombre de usuario,OU=engineering,DC=companyname, DC=netapp, DC=com* [para obtener sólo un usuario específico de <username> de OU <engineering>] _CN=usuarios de Acrobat,CN=usuarios,DC=nombre de confianza de la organización de Acrobat = c,DC de la organización de Active Directory.
Enlazar DN	Se permite que el usuario busque en el directorio. Por ejemplo: *username@companyname.com* o *username@domainname.com* Además, se requiere el permiso de solo lectura de dominio. El usuario debe ser miembro del grupo de seguridad *Controladores de dominio de solo lectura*.
ENLAZAR contraseña	Contraseña del servidor de directorio (es decir, contraseña para el nombre de usuario utilizado en DN de enlace)
Protocolo	ldap, ldaps, ldap-start-tls
Puertos	Seleccione el puerto

Introduzca los siguientes atributos requeridos de Directory Server si se han modificado los nombres de atributo predeterminados en Active Directory. En la mayoría de los casos, estos nombres de atributos se modifican en Active Directory, en cuyo caso simplemente puede continuar con el nombre de atributo predeterminado.

Atributos	Nombre del atributo en el servidor de directorio
Nombre para mostrar	nombre
SID	objectsid
Nombre de usuario	Nombre de cuenta SAM

Haga clic en incluir atributos opcionales para agregar cualquiera de los siguientes atributos:

Atributos	Nombre del atributo en el servidor de directorio
Dirección de correo electrónico	correo
Número de teléfono	número de teléfono
Función	título
País	co
Estado	estado

Departamento	departamento
Foto	thumbnailphoto
DN de administrador	gerente
Grupos	Miembro de

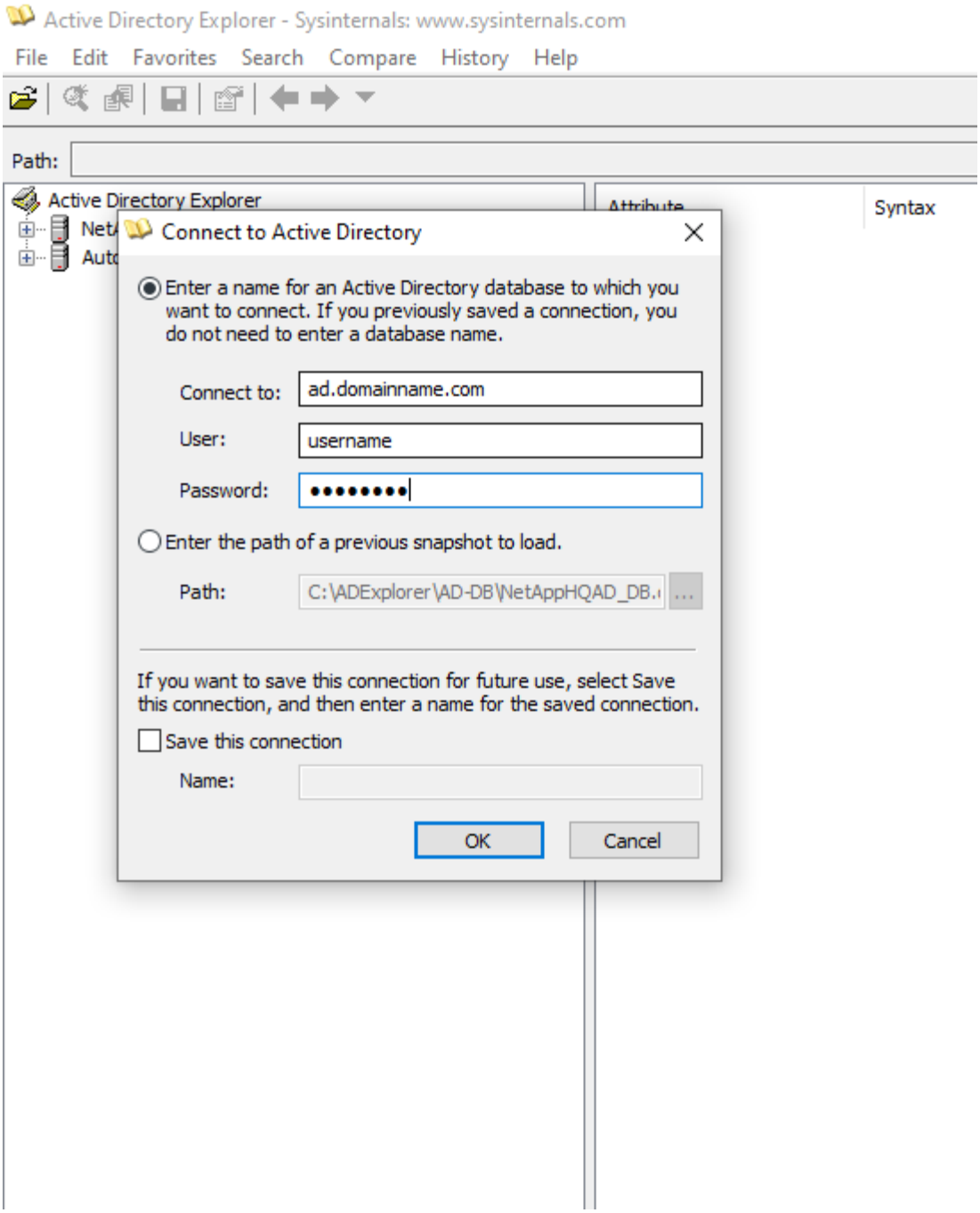
Prueba de la configuración del recopilador del directorio de usuarios

Puede validar los permisos de usuario LDAP y las definiciones de atributos mediante los procedimientos siguientes:

- Utilice el siguiente comando para validar los permisos de usuario de LDAP de seguridad de carga de trabajo:

  ```
  ldapsearch -o ldif-wrap=no -LLL -x -b "dc=netapp,dc=com" -h 10.235.40.29 -p
  389 -D Administrator@netapp.com -W
  ```

- Utilice el Explorador de AD para desplazarse por una base de datos AD, ver propiedades y atributos de objeto, ver permisos, ver el esquema de un objeto, ejecutar sofisticadas búsquedas que puede guardar y volver a ejecutar.
  - Instale "Explorador DE ANUNCIOS" en cualquier máquina de Windows que pueda conectarse al servidor AD.
  - Conéctese al servidor AD con el nombre de usuario/contraseña del servidor de directorio AD.



Solución de problemas de errores de configuración del recopilador de directorios de usuarios

En la siguiente tabla se describen los problemas conocidos y las resoluciones que pueden producirse durante la configuración del recopilador:

Problema:	Resolución:
La adición de un conector de directorio de usuarios da como resultado el estado "error". El error indica que “se han proporcionado credenciales no válidas para el servidor LDAP”.	Se ha proporcionado un nombre de usuario o contraseña incorrectos. Edite y proporcione el nombre de usuario y la contraseña correctos.

Problema:	Resolución:
La adición de un conector de directorio de usuarios da como resultado el estado "error". El error indica que “no se ha podido obtener el objeto correspondiente a DN=DC=hq,DC=domainname,DC=com proporcionado como nombre de bosque”.	Se ha proporcionado un nombre de bosque incorrecto. Edite y proporcione el nombre de bosque correcto.
Los atributos opcionales del usuario de dominio no aparecen en la página Workload Security User Profile (Perfil de usuario de seguridad de carga de trabajo).	Esto probablemente se deba a una discrepancia entre los nombres de los atributos opcionales agregados en CloudSecure y los nombres de atributos reales en Active Directory. Edite y proporcione los nombres de atributos opcionales correctos.
Recopilador de datos en estado de error "Failed to retrieve users LDAP". Motivo del error: No se puede conectar al servidor, la conexión es nula"	Reinicie el recopilador haciendo clic en el botón *restart*.
La adición de un conector de directorio de usuarios da como resultado el estado "error".	Asegúrese de haber proporcionado valores válidos para los campos requeridos (servidor, nombre de bosque, bind-DN, bind-Password). Asegúrese de que la entrada BIND-DN se proporciona siempre como ‘Administrador@<domain_forest_name>’ o como cuenta de usuario con privilegios de administrador de dominio.
La adición de un conector de Directorio de usuarios da como resultado EL estado DE "REPRUEBA". Muestra el error “no se puede definir el estado del recopilador,REASON TCP command [Connect(localhost:35012,None,List(),some(,segundos),true)] failed debido a que se rechazó java.net.ConnectionException:Connection.”	Se proporciona una IP o un FQDN incorrectos para el servidor AD. Edite y proporcione la dirección IP o el FQDN correctos.
La adición de un conector de directorio de usuarios da como resultado el estado "error". El error dice: “Error al establecer la conexión LDAP”.	Se proporciona una IP o un FQDN incorrectos para el servidor AD. Edite y proporcione la dirección IP o el FQDN correctos.
La adición de un conector de directorio de usuarios da como resultado el estado "error". El error dice: “No se han podido cargar los ajustes. Motivo: La configuración de DataSource tiene un error. Razón específica: /Connector/conf/Application.conf: 70: ldap.ldap-Port tiene TIPO CADENA en lugar DE NÚMERO”	Valor incorrecto para el puerto proporcionado. Pruebe a usar los valores de puerto predeterminados o el número de puerto correcto para el servidor AD.
Empecé con los atributos obligatorios, y funcionó. Después de agregar los opcionales, los datos de atributos opcionales no se obtienen de AD.	Esto probablemente se deba a una discrepancia entre los atributos opcionales agregados en CloudSecure y los nombres de atributos reales en Active Directory. Edite y proporcione el nombre de atributo obligatorio o opcional correcto.

Problema:	Resolución:
Después de reiniciar el recopilador, ¿cuándo se producirá la sincronización de AD?	La sincronización DE ANUNCIOS se producirá inmediatamente después de que se reinicie el recopilador. Tardará aproximadamente 15 minutos en recuperar datos de usuario de aproximadamente 300 000 usuarios y se actualiza cada 12 horas automáticamente.
Los datos de usuario se sincronizan de AD con CloudSecure. ¿Cuándo se eliminarán los datos?	Los datos de usuario se conservan durante 13 meses en caso de no actualización. Si se elimina el arrendatario, los datos se eliminarán.
El conector del directorio de usuarios tiene como resultado el estado "error". "El conector está en estado de error. Nombre del servicio: UsersLDAP. Motivo del fallo: No se pudieron recuperar los usuarios LDAP. Motivo del fallo: 80090308: LdapErr: DSID-0C090453, comentario: Error de AcceptSecurityContext, data 52e, v3839"	Se ha proporcionado un nombre de bosque incorrecto. Consulte más arriba cómo proporcionar el nombre correcto del bosque.
El número de teléfono no se rellena en la página del perfil de usuario.	Lo más probable es que esto se deba a un problema de asignación de atributos con Active Directory. 1. Edite el recopilador de Active Directory en particular que está recuperando la información del usuario de Active Directory. 2. Nota Bajo atributos opcionales, hay un nombre de campo “Número de teléfono” asignado al atributo de Active Directory “número de teléfono”. 4. Ahora, utilice la herramienta Explorador de Active Directory como se describe anteriormente para examinar Active Directory y ver el nombre de atributo correcto. 3. Asegúrese de que en Active Directory hay un atributo llamado “número de teléfono” que tiene efectivamente el número de teléfono del usuario. 5. Digamos que en Active Directory se ha modificado a “phonenumber”. 6. A continuación, edite el recopilador del directorio de usuarios de CloudSecure. En la sección atributo opcional, sustituya ‘telefonenumber’ por ‘fonenumber’. 7. Guarde el recopilador de Active Directory, el recopilador se reiniciará y obtendrá el número de teléfono del usuario y mostrará el mismo en la página de perfil de usuario.
Si el certificado de cifrado (SSL) está habilitado en el servidor de Active Directory (AD), el recopilador de directorios de usuarios de seguridad de carga de trabajo no se puede conectar al servidor AD.	Desactive el cifrado de AD Server antes de configurar un recopilador de directorios de usuarios. Una vez que se haya recuperado el detalle del usuario, estará allí por 13 meses. Si el servidor AD se desconecta después de obtener los detalles del usuario, los usuarios recién agregados en AD no se obtendrán. Para recuperar de nuevo, el recopilador de directorios de usuarios debe estar conectado a AD.

Problema:	Resolución:
Los datos de Active Directory están presentes en CloudInsights Security. Desea eliminar toda la información de usuario de CloudInsights.	No SÓLO es posible eliminar la información de usuario de Active Directory de CloudInsights Security. Para eliminar el usuario, el arrendatario completo debe ser eliminado.

Configurar un recopilador de servidor de directorio LDAP

La función Seguridad de carga de trabajo se configura para recopilar atributos de usuario desde los servidores de directorio LDAP.

Antes de empezar

- Debe ser un administrador de Data Infrastructure Insights o un propietario de la cuenta para realizar esta tarea.
- Debe tener la dirección IP del servidor donde se aloja el servidor de directorio LDAP.
- Debe configurar un agente antes de configurar un conector de directorio LDAP.

Pasos para configurar un recopilador de directorios de usuarios

1. En el menú Seguridad de la carga de trabajo, haga clic en: **Colectores > Colectores de directorios de usuarios > + Recopilador de directorios de usuarios** y seleccione **Servidor de directorios LDAP**

   El sistema muestra la pantalla Agregar directorio de usuario.

Configure el colector de directorios de usuarios introduciendo los datos necesarios en las tablas siguientes:

Nombre	Descripción
Nombre	Nombre único del directorio de usuarios. Por ejemplo, *GlobalLDAPCollector*
Agente	Seleccione un agente configurado de la lista
Nombre de dominio/IP del servidor	Dirección IP o nombre de dominio completo (FQDN) del servidor que aloja el servidor de directorio LDAP
Base de búsqueda	La base de búsqueda de la base de búsqueda de servidores LDAP permite los dos formatos siguientes: *X. y.z* ⇒ nombre de dominio directo como lo tiene en su SVM. [Ejemplo: hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ nombres distintivos relativos [ejemplo: DC=hq,DC= companyname,DC=com] o puede especificar como lo siguiente: *OU=engineering,DC=hq,DC= companyname,DC=com* [filtrar por ingeniería de OU específica] *CN=nombre,OU=ingeniería,DC=companyname, DC=netapp, DC=com* [para obtener solo un usuario específico con <username> de OU <engineering>] _CN=usuarios de Acrobat,CN=usuarios,DC=hq,DC=nombre de usuario de la organización [c,DC=companyu],s=nombre de la organización de Acrobat.

Enlazar DN	Se permite que el usuario busque en el directorio. Por ejemplo: uid=ldapuser,cn=users,cn=cuentas,dc=dominio,dc=nombre de empresa,dc=com uid=john,cn=usuarios,cn=cuentas,dc=dorp,dc=empresa,dc=com para un usuario john@dorp.company.com. dorp.company.com
--cuentas	--usuarios
--juan	--anna
ENLAZAR contraseña	Contraseña del servidor de directorio (es decir, contraseña para el nombre de usuario utilizado en DN de enlace)
Protocolo	ldap, ldaps, ldap-start-tls
Puertos	Seleccione el puerto

Introduzca los siguientes atributos requeridos de servidor de directorio si se han modificado los nombres de atributos predeterminados en servidor de directorio LDAP. En la mayoría de los casos, estos nombres de atributos se modifican *not* en el servidor de directorio LDAP, en cuyo caso simplemente puede continuar con el nombre de atributo predeterminado.

Atributos	Nombre del atributo en el servidor de directorio
Nombre para mostrar	nombre
UNIXID	uidnumber
Nombre de usuario	uid

Haga clic en incluir atributos opcionales para agregar cualquiera de los siguientes atributos:

Atributos	Nombre del atributo en el servidor de directorio
Dirección de correo electrónico	correo
Número de teléfono	número de teléfono
Función	título
País	co
Estado	estado
Departamento	número de departamento
Foto	foto
DN de administrador	gerente
Grupos	Miembro de

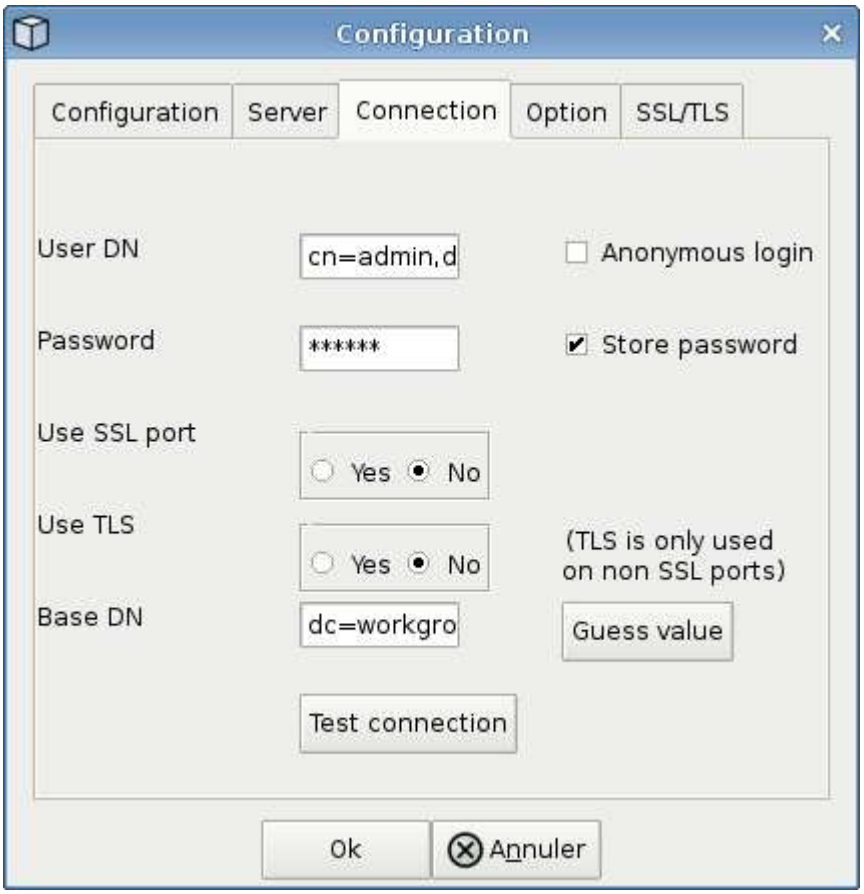
Prueba de la configuración del recopilador del directorio de usuarios

Puede validar los permisos de usuario LDAP y las definiciones de atributos mediante los procedimientos siguientes:

- Utilice el siguiente comando para validar los permisos de usuario de LDAP de seguridad de carga de trabajo:

```
 ldapsearch -D "uid=john
,cn=users,cn=accounts,dc=dorp,dc=company,dc=com" -W -x -LLL -o ldif-
wrap=no -b "cn=accounts,dc=dorp,dc=company,dc=com" -H
ldap://vmwipaapp08.dorp.company.com
* Utilice el Explorador de LDAP para desplazarse por una base de datos
LDAP, ver propiedades y atributos de objeto, ver permisos, ver el
esquema de un objeto, ejecutar sofisticadas búsquedas que puede guardar
y volver a ejecutar.
```

  - Instale LDAP Explorer (http://ldaptool.sourceforge.net/) o Java LDAP Explorer (http://jxplorer.org/) en cualquier máquina de Windows que pueda conectarse al servidor LDAP.
  - Conéctese al servidor LDAP con el nombre de usuario/contraseña del servidor de directorio LDAP.



Solución de problemas de errores de configuración de recopiladores de directorios LDAP

En la siguiente tabla se describen los problemas conocidos y las resoluciones que pueden producirse durante la configuración del recopilador:

Problema:	Resolución:
La adición de un conector de directorio LDAP da como resultado el estado ‘error’. El error indica que “se han proporcionado credenciales no válidas para el servidor LDAP”.	Se ha proporcionado una contraseña de enlace o DN de enlace incorrecta o una base de búsqueda. Edite y proporcione la información correcta.
La adición de un conector de directorio LDAP da como resultado el estado ‘error’. El error indica que “no se ha podido obtener el objeto correspondiente a DN=DC=hq,DC=domainname,DC=com proporcionado como nombre de bosque”.	Se ha proporcionado una base de búsqueda incorrecta. Edite y proporcione el nombre de bosque correcto.
Los atributos opcionales del usuario de dominio no aparecen en la página Workload Security User Profile (Perfil de usuario de seguridad de carga de trabajo).	Esto probablemente se deba a una discrepancia entre los nombres de los atributos opcionales agregados en CloudSecure y los nombres de atributos reales en Active Directory. Los campos distinguen mayúsculas de minúsculas. Edite y proporcione los nombres de atributos opcionales correctos.
Recopilador de datos en estado de error "Failed to retrieve users LDAP". Motivo del error: No se puede conectar al servidor, la conexión es nula"	Reinicie el recopilador haciendo clic en el botón *restart*.
La adición de un conector de directorio LDAP da como resultado el estado ‘error’.	Asegúrese de haber proporcionado valores válidos para los campos requeridos (servidor, nombre de bosque, bind-DN, bind-Password). Asegúrese de que la entrada BIND-DN se proporciona siempre como uid=ldapuser,cn=Users,cn=cuentas,dc=dominio,dc=companyname,dc=com.
La adición de un conector de directorio LDAP da como resultado EL estado DE "REPRUEBA". Muestra el error "no se pudo determinar el estado del colector, por lo tanto, volver a intentar"	Asegúrese de que se proporciona la IP del servidor y la base de búsqueda correctas ///
Mientras se añade el directorio LDAP se muestra el siguiente error: “Error al determinar el estado del recopilador en 2 reintentos, intente reiniciar el recopilador de nuevo(Código de error: AGENT008)”.	Asegúrese de que se proporciona la dirección IP correcta del servidor y la base de búsqueda
La adición de un conector de directorio LDAP da como resultado EL estado DE "REPRUEBA". Muestra el error “no se puede definir el estado del recopilador,REASON TCP command [Connect(localhost:35012,None,List(),some(,segundos),true)] failed debido a que se rechazó java.net.ConnectionException:Connection.”	Se proporciona una IP o un FQDN incorrectos para el servidor AD. Edite y proporcione la dirección IP o el FQDN correctos. ///
La adición de un conector de directorio LDAP da como resultado el estado ‘error’. El error dice: “Error al establecer la conexión LDAP”.	Se proporciona una IP o un FQDN incorrectos para el servidor LDAP. Edite y proporcione la dirección IP o el FQDN correctos. O valor incorrecto para el puerto proporcionado. Pruebe a usar los valores de puerto predeterminados o el número de puerto correcto para el servidor LDAP.

Problema:	Resolución:
La adición de un conector de directorio LDAP da como resultado el estado ‘error’. El error dice: “No se han podido cargar los ajustes. Motivo: La configuración de DataSource tiene un error. Razón específica: /Connector/conf/Application.conf: 70: ldap.ldap-Port tiene TIPO CADENA en lugar DE NÚMERO”	Valor incorrecto para el puerto proporcionado. Pruebe a usar los valores de puerto predeterminados o el número de puerto correcto para el servidor AD.
Empecé con los atributos obligatorios, y funcionó. Después de agregar los opcionales, los datos de atributos opcionales no se obtienen de AD.	Esto probablemente se deba a una discrepancia entre los atributos opcionales agregados en CloudSecure y los nombres de atributos reales en Active Directory. Edite y proporcione el nombre de atributo obligatorio o opcional correcto.
Después de reiniciar el recopilador, ¿cuándo se producirá la sincronización de LDAP?	La sincronización LDAP se producirá inmediatamente después de que se reinicie el recopilador. Tardará aproximadamente 15 minutos en recuperar datos de usuario de aproximadamente 300 000 usuarios y se actualiza cada 12 horas automáticamente.
Los datos de usuario se sincronizan de LDAP con CloudSecure. ¿Cuándo se eliminarán los datos?	Los datos de usuario se conservan durante 13 meses en caso de no actualización. Si se elimina el arrendatario, los datos se eliminarán.
El conector de directorio LDAP da como resultado el estado 'error'. "El conector está en estado de error. Nombre del servicio: UsersLDAP. Motivo del fallo: No se pudieron recuperar los usuarios LDAP. Motivo del fallo: 80090308: LdapErr: DSID-0C090453, comentario: Error de AcceptSecurityContext, data 52e, v3839"	Se ha proporcionado un nombre de bosque incorrecto. Consulte más arriba cómo proporcionar el nombre correcto del bosque.
El número de teléfono no se rellena en la página del perfil de usuario.	Lo más probable es que esto se deba a un problema de asignación de atributos con Active Directory. 1. Edite el recopilador de Active Directory en particular que está recuperando la información del usuario de Active Directory. 2. Nota Bajo atributos opcionales, hay un nombre de campo “Número de teléfono” asignado al atributo de Active Directory “número de teléfono”. 4. Ahora, utilice la herramienta Explorador de Active Directory como se describe anteriormente para examinar el servidor de LDAP Directory y ver el nombre de atributo correcto. 3. Asegúrese de que en el directorio LDAP hay un atributo llamado “número de teléfono” que tiene el número de teléfono del usuario. 5. Digamos que en LDAP Directory se ha modificado a “phonenumber”. 6. A continuación, edite el recopilador del directorio de usuarios de CloudSecure. En la sección atributo opcional, sustituya ‘telefonenumber’ por ‘fonenumber’. 7. Guarde el recopilador de Active Directory, el recopilador se reiniciará y obtendrá el número de teléfono del usuario y mostrará el mismo en la página de perfil de usuario.

Problema:	Resolución:
Si el certificado de cifrado (SSL) está habilitado en el servidor de Active Directory (AD), el recopilador de directorios de usuarios de seguridad de carga de trabajo no se puede conectar al servidor AD.	Desactive el cifrado de AD Server antes de configurar un recopilador de directorios de usuarios. Una vez que se haya recuperado el detalle del usuario, estará allí por 13 meses. Si el servidor AD se desconecta después de obtener los detalles del usuario, los usuarios recién agregados en AD no se obtendrán. Para recuperar de nuevo el recopilador de directorios de usuarios debe estar conectado a AD.

Configurar el recopilador de datos de SVM de ONTAP

Workload Security utiliza recopiladores de datos para recopilar datos de acceso de archivos y usuarios desde dispositivos.

Antes de empezar

- Este recopilador de datos es compatible con lo siguiente:
  - Data ONTAP 9.2 y versiones posteriores. Para obtener el mejor rendimiento, utilice una versión de Data ONTAP superior a 9.13.1.
  - Protocolo SMB, versión 3.1 y versiones anteriores.
  - Versiones de NFS hasta e incluido NFS 4,1 con ONTAP 9.15.1 o posteriores.
  - ONTAP 9.4 y versiones posteriores admiten FlexGroup
  - ONTAP Select es compatible
- Solo se admiten SVM de tipo de datos. No se admiten las SVM con Infinite Volume.
- SVM tiene varios subtipos. De estos, sólo se admiten *default*, *SYNC_Source* y *SYNC_Destination*.
- Un agente "debe configurarse" antes de configurar recopiladores de datos.
- Asegúrese de que tiene un conector de directorio de usuario configurado correctamente; de lo contrario, los eventos mostrarán nombres de usuario codificados y no el nombre real del usuario (tal como se almacena en Active Directory) en la página “Activity Forensics”.
- • El almacén persistente de ONTAP es compatible con 9.14.1.
- Para obtener un rendimiento óptimo, debe configurar el servidor FPolicy para que esté en la misma subred que el sistema de almacenamiento.
- Debe añadir una SVM mediante uno de los siguientes dos métodos:
  - Mediante Cluster IP, SVM name y Cluster Management Username and Password. ***este es el método recomendado.***
    - El nombre de la SVM debe ser exactamente el que se muestra en ONTAP y distingue entre mayúsculas y minúsculas.
  - Mediante la administración de Vserver IP, nombre de usuario y contraseña de SVM
  - Si no puede o no desea utilizar el nombre de usuario y la contraseña completos de administración de clúster/SVM, puede crear un usuario personalizado con menos Privileges, como se menciona en la “Una nota sobre los permisos” sección siguiente. Este usuario personalizado se puede crear tanto para SVM como para el acceso a clústeres.
    - o también puede usar un usuario de AD con una función que tenga al menos los permisos de csrole como se menciona en la sección “una nota sobre los permisos” que aparece a continuación.

Consulte también la "Documentación de ONTAP".

- Asegúrese de que se establecen las aplicaciones correctas para la SVM ejecutando el comando siguiente:

```
clustershell::> security login show -vserver <vservername> -user-or
-group-name <username>
```

Resultado de ejemplo:

```
Vserver: svmname
                                                                  Second
User/Group                  Authentication                 Acct   Authentication
Name           Application  Method        Role Name        Locked Method
-------------- -----------  ------------- ---------------- ------ --------------
vsadmin        http         password      vsadmin          no     none
vsadmin        ontapi       password      vsadmin          no     none
vsadmin        ssh          password      vsadmin          no     none
3 entries were displayed.
```

- Asegúrese de que la SVM tenga configurado un servidor CIFS: Clustershell::> `vserver cifs show`

  El sistema devuelve el nombre de Vserver, el nombre del servidor CIFS y los campos adicionales.

- Establezca una contraseña para el usuario de SVM vsadmin. Si utiliza el usuario personalizado o el usuario administrador del clúster, omita este paso. Clustershell::> `security login password -username vsadmin -vserver svmname`
- Desbloquee el usuario de SVM vsadmin para tener acceso externo. Si utiliza el usuario personalizado o el usuario administrador del clúster, omita este paso. Clustershell::> `security login unlock -username vsadmin -vserver svmname`
- Asegúrese de que la política de firewall de la LIF de datos esté configurada en 'mgmt' (no 'data'). Omita este paso si utiliza un LIF de gestión dedicado para añadir la SVM. Clustershell::> `network interface modify -lif <SVM_data_LIF_name> -firewall-policy mgmt`
- Cuando se habilita un firewall, debe tener una excepción definida para permitir el tráfico TCP para el puerto mediante el recopilador de datos de Data ONTAP.

  Consulte "Requisitos del agente" para obtener información sobre la configuración. Esto se aplica a los agentes y agentes de las instalaciones instalados en la nube.

- Cuando se instala un agente en una instancia de AWS EC2 para supervisar una SVM de Cloud ONTAP, el agente y el almacenamiento deben estar en el mismo VPC. Si están en VPC independientes, debe haber una ruta válida entre el VPC.

Requisitos previos para bloqueo de acceso del usuario

Tenga en cuenta lo siguiente para"Bloqueo de acceso de usuario":

Se necesitan credenciales para que esta función funcione.

Si utiliza credenciales de administración del clúster, no es necesario contar con permisos nuevos.

Si utiliza un usuario personalizado (por ejemplo, *csuser*) con permisos proporcionados al usuario, siga los pasos que se indican a continuación para otorgar permisos a Workload Security para bloquear al usuario.

Para csuser con credenciales de clúster, haga lo siguiente desde la línea de comandos ONTAP:

```
security login role create -role csrole -cmddirname "vserver export-policy
rule" -access all
security login role create -role csrole -cmddirname set -access all
security login role create -role csrole -cmddirname "vserver cifs session"
-access all
security login role create -role csrole -cmddirname "vserver services
access-check authentication translate" -access all
security login role create -role csrole -cmddirname "vserver name-mapping"
-access all
```

Una nota sobre los permisos

Permisos al agregar mediante IP de administración de clúster:

Si no puede utilizar el usuario administrador de administración de clústeres para permitir que Workload Security acceda al recopilador de datos de SVM de ONTAP, puede crear un nuevo usuario llamado “csuser” con los roles como se muestra en los comandos siguientes. Utilice el nombre de usuario “csuser” y la contraseña para “csuser” cuando configure el recopilador de datos Workload Security para utilizar Cluster Management IP.

Para crear un nuevo usuario, inicie sesión en ONTAP con el nombre de usuario/contraseña del administrador de administración del clúster y ejecute los siguientes comandos en el servidor ONTAP:

```
security login role create -role csrole -cmddirname DEFAULT -access
readonly
```

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "volume snapshot"
-access all -query "-snapshot cloudsecure_*"
security login role create -role csrole -cmddirname "event catalog"
-access all
security login role create -role csrole -cmddirname "event filter" -access
all
security login role create -role csrole -cmddirname "event notification
destination" -access all
security login role create -role csrole -cmddirname "event notification"
-access all
security login role create -role csrole -cmddirname "security certificate"
-access all
```

```
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole
security login create -user-or-group-name csuser -application ssh
-authmethod password -role csrole
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole
```

Permisos al agregar mediante IP de administración de Vserver:

Si no puede utilizar el usuario administrador de administración de clústeres para permitir que Workload Security acceda al recopilador de datos de SVM de ONTAP, puede crear un nuevo usuario llamado “csuser” con los roles como se muestra en los comandos siguientes. Utilice el nombre de usuario “csuser” y la contraseña para “csuser” cuando configure el recopilador de datos Workload Security para utilizar Vserver Management IP.

Para crear el nuevo usuario, inicie sesión en ONTAP con el nombre de usuario/contraseña del administrador de administración del clúster y ejecute los siguientes comandos en el servidor ONTAP. Para facilitar la operación, copie estos comandos en un editor de texto y sustituya la <vservername> por su nombre Vserver antes y ejecute estos comandos en ONTAP:

```
security login role create -vserver <vservername> -role csrole -cmddirname
DEFAULT -access none
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"network interface" -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
version -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
volume -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
vserver -access readonly
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"volume snapshot" -access all
```

```
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole -vserver <vservername>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole -vserver <vservername>
```

Modo Protobuf

Workload Security configurará el motor FPolicy en modo protobuf cuando esta opción esté habilitada en la configuración *Advanced Configuration* del recopilador. El modo Protobuf es compatible con ONTAP versión 9,15 y posteriores.

Puede encontrar más detalles sobre esta función en el "Documentación de ONTAP".

Se requieren permisos específicos para protobuf (puede que algunos o todos estos ya existan):

Modo de clúster:

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole
```

Modo Vserver:

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <svm_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole -vserver <svm_name>
```

Permisos para la protección autónoma frente a ransomware de ONTAP y el acceso a ONTAP denegado

Si utiliza credenciales de administración del clúster, no es necesario contar con permisos nuevos.

Si utiliza un usuario personalizado (por ejemplo, *csuser*) con permisos proporcionados al usuario, siga los pasos que se indican a continuación para otorgar permisos a Seguridad de carga de trabajo para recopilar información relacionada con ARP desde ONTAP.

Para obtener más información, lea acerca de "Integración con acceso ONTAP denegado"

1. "Integración con la protección autónoma de ransomware de ONTAP"

Configure el recopilador de datos

Pasos para la configuración

1. Inicie sesión como administrador o propietario de la cuenta en su entorno de Data Infrastructure Insights.
2. Haga clic en **Workload Security > Collectors > +Data Collectors**

   El sistema muestra los colectores de datos disponibles.

3. Pase el ratón por el icono **NetApp SVM y haga clic en *+Monitor**.

   El sistema muestra la página de configuración de la SVM de ONTAP. Introduzca los datos necesarios para cada campo.

Campo	Descripción
Nombre	Nombre único para el recopilador de datos
Agente	Seleccione un agente configurado de la lista.
Conéctese a través de la IP de administración para:	Seleccione Cluster IP o SVM Management IP
Dirección IP de administración del clúster/SVM	La dirección IP del clúster o la SVM, según lo seleccionado anteriormente.
Nombre de la SVM	Nombre de la SVM (este campo es obligatorio cuando se realiza la conexión mediante la IP del clúster)
Nombre de usuario	Nombre de usuario para acceder a la SVM/Cluster cuando se añade mediante la IP del clúster las opciones son: 1. Administrador de clúster 2. 'csuser' 3. USUARIO AD que tiene un papel similar a csuser. Cuando se agrega mediante IP de SVM, las opciones son: 4. Vsadmin 5. 'csuser' 6. NOMBRE DE USUARIO DE AD que tiene un papel similar a csuser.
Contraseña	Contraseña para el nombre de usuario anterior
Filtre los recursos compartidos/volúmenes	Elija si desea incluir o excluir recursos compartidos/volúmenes de la colección de eventos
Introduzca los nombres completos de recursos compartidos para excluir o incluir	Lista de recursos compartidos separados por comas para excluir o incluir (según corresponda) de la colección de eventos
Introduzca los nombres completos de los volúmenes para excluirlos o incluirlos	Lista de volúmenes separados por comas para excluir o incluir (según corresponda) de la colección de eventos
Supervisar el acceso a carpetas	Cuando esta opción está activada, activa los eventos para la supervisión del acceso a carpetas. Tenga en cuenta que la creación, el cambio de nombre y la eliminación de carpetas se supervisarán incluso sin seleccionar esta opción. Al activar esta opción, aumentará el número de eventos supervisados.
Establezca el tamaño del búfer de envío de ONTAP	Establece el tamaño del búfer de envío de la directiva de ONTAP. Si se utiliza una versión de ONTAP anterior a 9.8p7 y se observa un problema de rendimiento, el tamaño del búfer de envío de ONTAP se puede modificar para mejorar el rendimiento de ONTAP. Póngase en contacto con el soporte de NetApp si no ve esta opción y desea explorarla.

Después de terminar

- En la página Recolectores de datos instalados, utilice el menú de opciones situado a la derecha de cada recopilador para editar el recopilador de datos. Puede reiniciar el recopilador de datos o editar los atributos de configuración del recopilador de datos.

Configuración recomendada para MetroCluster

Se recomienda lo siguiente para MetroCluster:

1. Conecte dos recopiladores de datos, uno a la SVM de origen y otro a la SVM de destino.
2. Los recopiladores de datos deben estar conectados por *Cluster IP*.
3. En cualquier momento, un recopilador de datos debe estar en ejecución, otro será un error.

   El recopilador de datos actual de la SVM en 'ejecución' se mostrará como *running*. El colector de datos actual de la SVM 'con capacidad superpuesta' se mostrará como *error*.

4. Siempre que haya un cambio, el estado del recopilador de datos cambiará de 'en ejecución' a 'error' y viceversa.
5. El recopilador de datos tardará hasta dos minutos en pasar del estado error al estado en ejecución.

Política de servicio

Si se utiliza la política de servicio con ONTAP **versión 9.9.1 o posterior**, para conectarse al recopilador de fuentes de datos, se requiere el servicio *data-fpolicy-client* junto con el servicio de datos *data-nfs* y/o *data-cifs*.

Ejemplo:

```
Testcluster-1::*> net int service-policy create -policy only_data_fpolicy
-allowed-addresses 0.0.0.0/0 -vserver aniket_svm
-services data-cifs,data-nfs,data,-core,data-fpolicy-client
(network interface service-policy create)
```

En las versiones de ONTAP anteriores a 9.9.1, no es necesario definir *data-fpolicy-client*.

Reproducir-Pausa del recopilador de datos

Ahora se muestran 2 nuevas operaciones en el menú kebab del colector (PAUSA y REANUDACIÓN).

Si el recopilador de datos se encuentra en estado *Running*, puede pausar la recopilación. Abra el menú de tres puntos para el recopilador y seleccione PAUSE. Mientras el recopilador está en pausa, no se recopilan datos desde ONTAP y no se envía ningún dato del recopilador a ONTAP. Esto significa que no habrá eventos de Fpolicy que fluyan de ONTAP al recopilador de datos y de allí a Información de la infraestructura de datos.

Tenga en cuenta que si se crean volúmenes nuevos, etc. en ONTAP mientras el recopilador está en pausa, la seguridad de la carga de trabajo no recopilará los datos y esos volúmenes, etc., no se reflejará en las consolas ni las tablas.

Tenga en cuenta lo siguiente:

- La purga de snapshots no se producirá de acuerdo con la configuración configurada en un recopilador en pausa.
- Los eventos de EMS (como ARP de ONTAP) no se procesarán en un recopilador en pausa. Esto significa que si ONTAP identifica un ataque de ransomware, la seguridad de carga de trabajo de información sobre la infraestructura de datos no podrá adquirir ese evento.
- NO se enviarán correos electrónicos de notificaciones de estado para un recopilador en pausa.
- Las acciones manuales o automáticas (como Instantánea o Bloqueo de usuarios) no se admitirán en un recopilador en pausa.
- En las actualizaciones de agente o recopilador, la VM del agente se reinicia o reinicia el servicio del

agente, un recopilador en pausa permanecerá en estado *Paused*.

- Si el recopilador de datos está en estado *Error*, el recopilador no se puede cambiar al estado *Paused*. El botón Pausa solo se activará si el estado del recopilador es *Running*.
- Si el agente está desconectado, el recopilador no se puede cambiar al estado *Paused*. El recopilador pasará al estado *STOP* y el botón Pause se desactivará.

Almacén persistente

ONTAP 9.14.1 y versiones posteriores es compatible con el almacén persistente. Tenga en cuenta que las instrucciones de nombre del volumen varían de ONTAP 9,14 a 9,15.

El almacén persistente se puede activar seleccionando la casilla de verificación en la página de edición/adición del recopilador. Después de seleccionar la casilla de verificación, se muestra un campo de texto para aceptar el nombre del volumen. El nombre del volumen es un campo obligatorio para activar el almacén persistente.

- Para ONTAP 9.14.1, debe crear el volumen antes de habilitar la función e introducir el mismo nombre en el campo *Volume Name*. El tamaño de volumen recomendado es de 16GB TB.
- Para ONTAP 9.15.1, el recopilador creará el volumen automáticamente con un tamaño de 16GB, utilizando el nombre proporcionado en el campo *Nombre del Volumen*.

Se necesitan permisos específicos para el almacén persistente (es posible que algunos o todos estos ya existan):

Modo de clúster:

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster-name>
security login rest-role create -role csrestrole -api /api/cluster/jobs/
-access readonly -vserver <cluster-name>
```

Modo Vserver:

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <vserver-name>
security login rest-role create -role csrestrole -api /api/cluster/jobs/
-access readonly -vserver <vserver-name>
```

Resolución de problemas

Consulte "Solucionar problemas del recopilador de SVM"la página para obtener consejos sobre la solución de problemas.

Configurar el recopilador Cloud Volumes ONTAP y Amazon FSX para ONTAP de NetApp

Workload Security utiliza recopiladores de datos para recopilar datos de acceso de archivos y usuarios desde dispositivos.

Configuración del almacenamiento de Cloud Volumes ONTAP

Consulte la documentación de OnCommand Cloud Volumes ONTAP para configurar una instancia de AWS de un solo nodo/de alta disponibilidad para alojar el agente de seguridad de carga de trabajo: https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html

Una vez finalizada la configuración, siga los pasos para configurar la SVM: https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html

Plataformas compatibles

- Cloud Volumes ONTAP, compatible con todos los proveedores de servicios cloud disponibles allá donde esté disponible. Por ejemplo: Amazon, Azure y Google Cloud.
- Amazon FSX de ONTAP

Configuración de máquina de agente

La máquina del agente debe estar configurada en las subredes respectivas de los proveedores de servicios en la nube. Obtenga más información sobre el acceso a la red en [requisitos del agente].

A continuación se muestran los pasos para la instalación del agente en AWS. Los pasos equivalentes, según proceda y según el proveedor de servicios cloud, se pueden seguir en Azure o Google Cloud para la instalación.

En AWS, siga estos pasos para configurar el equipo que se utilizará como agente de seguridad de carga de trabajo:

Siga estos pasos para configurar el equipo que se utilizará como agente de seguridad de carga de trabajo:

Pasos

1. Inicie sesión en la consola de AWS y desplácese a la página EC2-instance y seleccione *Launch instance*.
2. Seleccione una AMI de RHEL o CentOS con la versión adecuada, tal y como se menciona en esta página: https://docs.netapp.com/us-en/cloudinsights/concept_cs_agent_requirements.html
3. Seleccione el VPC y la subred en que reside la instancia de Cloud ONTAP.
4. Seleccione *t2.xlarge* (4 vcpu y 16 GB de RAM) como recursos asignados.
    a. Cree la instancia de EC2.
5. Instale los paquetes de Linux necesarios con el gestor de paquetes YUM:
    a. Instale los paquetes nativos de Linux *wget* y *unzip*.

Instale el agente de seguridad de carga de trabajo

1. Inicie sesión como administrador o propietario de la cuenta en su entorno de Data Infrastructure Insights.
2. Navegue a Workload Security **Collectors** y haga clic en la pestaña **Agentes**.
3. Haga clic en **+Agent** y especifique RHEL como plataforma de destino.
4. Copie el comando instalación del agente.
5. Pegue el comando Agent Installation en la instancia de RHEL EC2 en la que ha iniciado sesión. Se instala el agente de seguridad de carga de trabajo, siempre que se cumplan todos los"Requisitos previos del agente".

Para conocer los pasos detallados, consulte este enlace: https://docs.NetApp.com/us-es/cloudinsights/

task_cs_add_agent.html#steps-to-install-agent

Resolución de problemas

Los problemas conocidos y sus resoluciones se describen en la siguiente tabla.

Problema	Resolución
El recopilador de datos muestra el error “Workload Security: Failed to determine ONTAP type for Amazon FxSN data collector” (Seguridad de carga de trabajo: Error al determinar el tipo de para el recopilador de datos de Amazon FxSN). El cliente no puede agregar un nuevo recopilador de datos de Amazon FSxN a Workload Security. La conexión al clúster FSxN en el puerto 443 del agente se agota el tiempo de espera. Los grupos de seguridad de firewall y AWS tienen habilitadas las reglas necesarias para permitir la comunicación. Un agente ya está implementado y se encuentra también en la misma cuenta de AWS. Este mismo agente se utiliza para conectar y supervisar los demás dispositivos de NetApp (y todos funcionan).	Resuelva este problema añadiendo el segmento de red LIF fsxadmin a la regla de seguridad del agente. Se permiten todos los puertos si no está seguro de los puertos.

Gestión de usuarios

Las cuentas de usuario de seguridad de carga de trabajo se gestionan a través de Información de infraestructura de datos.

Data Infrastructure Insights proporciona cuatro niveles de cuenta de usuario: Propietario de la cuenta, administrador, usuario e invitado. A cada cuenta se le asignan niveles de permisos específicos. Una cuenta de usuario con privilegios de administrador puede crear o modificar usuarios y asignar a cada usuario uno de los siguientes roles de seguridad de carga de trabajo:

Función	Acceso de seguridad de cargas de trabajo
Administrador	Puede realizar todas las funciones de seguridad de carga de trabajo, incluidas las de Alertas, Forensics, recopiladores de datos, directivas de respuesta automatizadas y API para Workload Security. Un administrador también puede invitar a otros usuarios, pero sólo puede asignar funciones de seguridad de carga de trabajo.
Usuario	Puede ver y gestionar alertas y visualizar información forense. El rol de usuario puede cambiar el estado de alerta, añadir una nota, tomar instantáneas manualmente y restringir el acceso de usuario.
Invitado	Puede ver Alertas y Forensics. El rol de invitado no puede cambiar el estado de alerta, agregar una nota, tomar instantáneas manualmente o restringir el acceso de usuario.

Pasos

1. Inicie sesión en Workload Security
2. En el menú, haga clic en **Administración > Administración de usuarios**

   Se le reenviará a la página Gestión de usuarios de Data Infrastructure Insights.

3. Seleccione el rol que desee para cada usuario.

Al agregar un nuevo usuario, solo tiene que seleccionar el rol que desee (normalmente Usuario o invitado).

Puede encontrar más información sobre las cuentas de usuario y las funciones en la documentación de Data Infrastructure Insights"Rol de usuario".

Comprobador de tasa de eventos de SVM (guía de ajuste de tamaño del agente)

El comprobador de tasa de eventos se utiliza para comprobar la tasa de eventos combinada de NFS/SMB en la SVM antes de instalar un recopilador de datos de SVM de ONTAP, a fin de ver cuántas SVM podrá supervisar un equipo de agente. Utilice el Comprobador de tasa de eventos como guía de tamaño para ayudar a planificar su entorno de seguridad.

Un agente puede admitir hasta un máximo de 50 recopiladores de datos.

Exigencias legales:

- IP del clúster
- Nombre de usuario y contraseña de administrador del clúster

> Cuando se ejecuta este script, no se debe ejecutar ningún recopilador de datos de SVM de ONTAP para la SVM para la cual se está determinando la tasa de evento.

Pasos:

1. Instale el agente siguiendo las instrucciones de CloudSecure.
2. Una vez instalado el agente, ejecute el script *Server_data_rate_checker.sh* como usuario sudo:

```
 /opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
. Esta secuencia de comandos requiere que se instale _sshpass_ en la
máquina linux. Hay dos formas de instalarlo:
```

   a. Ejecute el siguiente comando:

```
 linux_prompt> yum install sshpass
.. Si esto no funciona, descargue _sshpass_ en el equipo linux desde
la web y ejecute el siguiente comando:
```

```
linux_prompt> rpm -i sshpass
```

3. Introduzca los valores correctos cuando se le solicite. Consulte a continuación un ejemplo.
4. La secuencia de comandos tardará aproximadamente 5 minutos en ejecutarse.
5. Una vez finalizada la ejecución, el script imprimirá la tasa de evento desde la SVM. Puede comprobar la tasa de eventos por SVM en la salida de la consola:

```
“Svm svm_rate is generating 100 events/sec”.
```

Cada recopilador de datos de SVM de ONTAP se puede asociar a una única SVM, lo que significa que cada recopilador de datos podrá recibir el número de eventos que genera una única SVM.

Tenga en cuenta lo siguiente:

A) Utilice esta tabla como guía de tamaño general. Puede aumentar el número de núcleos y/o memoria para aumentar el número de recopiladores de datos admitidos, hasta un máximo de 50 recopiladores de datos:

Configuración de máquina de agente	Número de recolectores de datos de SVM	Velocidad máxima de eventos que el equipo del agente puede manejar
4 núcleos, 16 GB	10 recopiladores de datos	20.000 eventos/s
4 núcleos, 32 GB	20 recopiladores de datos	20.000 eventos/s

B) para calcular el total de eventos, añada los eventos generados para todas las SVM de ese agente.

C) Si la secuencia de comandos no se ejecuta durante las horas pico o si el tráfico pico es difícil de predecir, entonces mantenga un búfer de tasa de eventos del 30%.

B + C debe ser menor que A, de lo contrario, la máquina del agente no podrá supervisar.

En otras palabras, el número de recopiladores de datos que se pueden agregar a un solo agente debe cumplir la fórmula siguiente:

```
 Sum of all Event rate of all Data Source Collectors + Buffer Event rate
of 30% < 20000 events/second
Consulte
xref:{relative_path}concept_cs_agent_requirements.html["Requisitos del
agente"]la página para obtener más requisitos y requisitos previos.
```

Ejemplo

Digamos que tenemos tres SVM que generan tasas de eventos de 100, 200 y 300 eventos por segundo, respectivamente.

Aplicamos la fórmula:

```
 (100+200+300) + [(100+200+300)*30%] = 600+180 = 780events/sec
780 events/second is < 20000 events/second, so the 3 SVMs can be monitored
via one agent box.
```

La salida de la consola está disponible en el equipo del agente en el nombre de archivo *fpolicy_stat_<SVM Name>.log* en el directorio de trabajo actual.

La secuencia de comandos puede dar resultados erróneos en los siguientes casos:

- Se proporcionan credenciales, IP o nombre de SVM incorrectos.
- Una fpolicy ya existente con el mismo nombre, número de secuencia, etc. dará error.
- El script se detiene abruptamente mientras se ejecuta.

A continuación se muestra un ejemplo de ejecución de script:

```
[root@ci-cs-data agent]#
/opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
```

```
Enter the cluster ip: 10.192.139.166
Enter the username to SSH: admin
Enter the password:
Getting event rate for NFS and SMB events.
Available SVMs in the Cluster
-----------------------------
QA_SVM
Stage_SVM
Qa-fas8020
Qa-fas8020-01
Qa-fas8020-02
audit_svm
svm_rate
vs_new
vs_new2
```

```
-----------------------------
Enter [1/5] SVM name to check (press enter to skip): svm_rate
Enter [2/5] SVM name to check (press enter to skip): audit_svm
Enter [3/5] SVM name to check (press enter to skip):
Enter [4/5] SVM name to check (press enter to skip):
Enter [5/5] SVM name to check (press enter to skip):
Running check for svm svm_rate...
Running check for svm audit_svm...
Waiting 5 minutes for stat collection
Stopping sample svm_rate_sample
Stopping sample audit_svm_sample
fpolicy stats of svm svm_rate is saved in fpolicy_stat_svm_rate.log
Svm svm_rate is generating 100 SMB events/sec and 100 NFS events/sec
Overall svm svm_rate is generating 200 events/sec
fpolicy stats of svm audit_svm is saved in fpolicy_stat_audit_svm.log
Svm audit_svm is generating 200 SMB events/sec and 100 NFS events/sec
Overall svm audit_svm is generating 300 events/sec
```

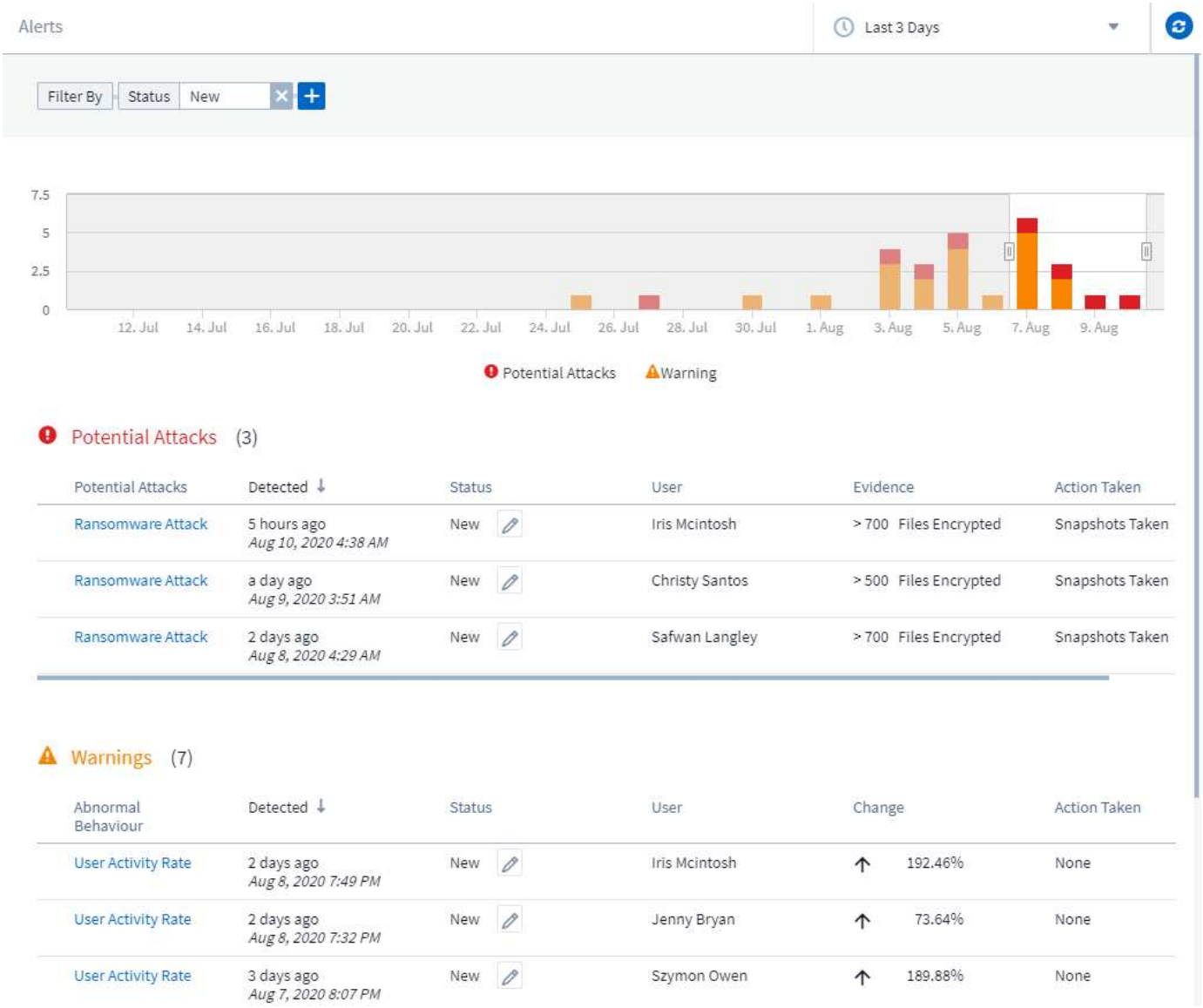
```
[root@ci-cs-data agent]#
```

Resolución de problemas

Pregunta	Responda
Si ejecuto este script en una SVM que ya está configurada para la seguridad de la carga de trabajo, ¿utiliza simplemente la configuración de fpolicy existente en la SVM o configura una temporal y ejecuta el proceso?	El comprobador de tasa de eventos puede ejecutarse correctamente incluso para una SVM ya configurada para la seguridad de la carga de trabajo. No debería haber ningún impacto.
¿Puedo aumentar el número de SVM en las que se puede ejecutar el script?	Sí. Solo tiene que editar la secuencia de comandos y cambiar el número máximo de SVM de 5 a cualquier número que desee.
Si aumenta el número de SVM, ¿aumentará el tiempo de ejecución del script?	No. El script se ejecutará durante un máximo de 5 minutos, incluso si se aumenta el número de SVM.
¿Puedo aumentar el número de SVM en las que se puede ejecutar el script?	Sí. Debe editar el script y cambiar el número máximo de SVM de 5 a cualquier número que desee.
Si aumenta el número de SVM, ¿aumentará el tiempo de ejecución del script?	No. El script se ejecutará durante un máximo de 5mins, incluso si se aumenta el número de SVM.
¿Qué ocurre si ejecuto el Comprobador de frecuencia de sucesos con un agente existente?	Si se ejecuta el comprobador de tasa de eventos con un agente ya existente, se puede aumentar la latencia en la SVM. Este aumento será de naturaleza temporal mientras se ejecuta el comprobador de tasa de eventos.

Alertas

La página Workload Security Alerts (Alertas de seguridad de carga de trabajo) muestra una línea temporal de ataques y/o advertencias recientes y permite ver detalles de cada problema.



Alerta

La lista Alerta muestra un gráfico que muestra el número total de ataques potenciales y/o advertencias que se han generado en el intervalo de tiempo seleccionado, seguido de una lista de ataques y/o advertencias que se han producido en ese intervalo de tiempo. Puede cambiar el intervalo de tiempo ajustando los controles deslizantes de hora de inicio y hora de finalización del gráfico.

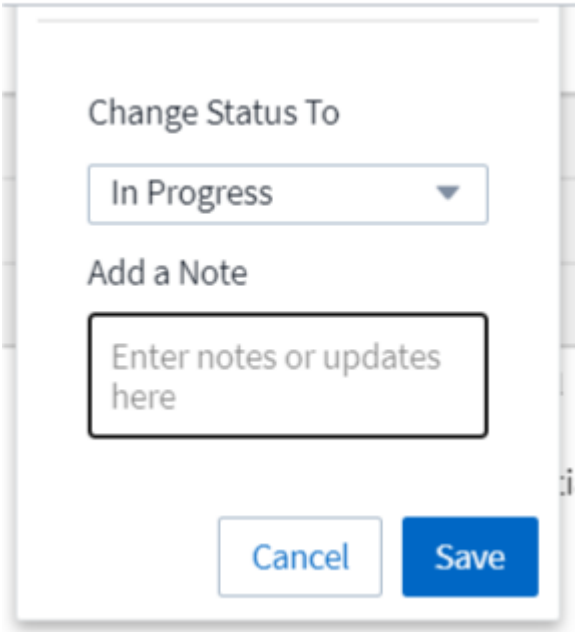
Se muestran los siguientes elementos para cada alerta:

Ataques potenciales:

- El tipo *Potential Attack* (por ejemplo, ransomware o sabotaje)

- La fecha y la hora en que se *detectó* el ataque potencial
- El *Status* de la alerta:
  - **Nuevo**: Este es el valor predeterminado para las alertas nuevas.
  - **En curso**: La alerta está bajo investigación de un miembro o miembros del equipo.
  - **Resuelto**: La alerta ha sido marcada como resuelta por un miembro del equipo.
  - **Despedido**: La alerta ha sido desestimada como comportamiento falso positivo o esperado.

    Un administrador puede cambiar el estado de la alerta y agregar una nota para ayudar con la investigación.



- El *User* cuyo comportamiento activó la alerta
- *Evidence* del ataque (por ejemplo, se ha cifrado un gran número de archivos)
- La *Action tomó* (por ejemplo, se tomó una instantánea)

Advertencias:

- El *comportamiento anormal* que activó la advertencia
- La fecha y la hora en que se detectó el comportamiento
- El *Status* de la alerta (Nuevo, en curso, etc.)
- El *User* cuyo comportamiento activó la alerta
- Una descripción del *Change* (por ejemplo, un aumento anormal del acceso a archivos)
- La *Acción tomada*

Opciones de filtro

Puede filtrar alertas según lo siguiente:

- El *Status* de la alerta

- Texto específico en el *Note*
- Tipo de *ataques/Advertencias*
- El *User* cuyas acciones activaron la alerta/advertencia

La página Alert Details

Puede hacer clic en un enlace de alerta de la página de lista Alertas para abrir una página de detalles de la alerta. Los detalles de alerta pueden variar según el tipo de ataque o alerta. Por ejemplo, una página de detalles de ataque de Ransomware puede mostrar la siguiente información:

Sección de resumen:

- Tipo de ataque (ransomware, sabotaje) e ID de alerta (asignado por seguridad de carga de trabajo)
- Fecha y hora en la que se detectó el ataque
- Acción realizada (por ejemplo, se ha realizado una instantánea automática. La hora de la copia Snapshot se muestra inmediatamente debajo de la sección de resumen)
- Estado (nuevo, en curso, etc.)

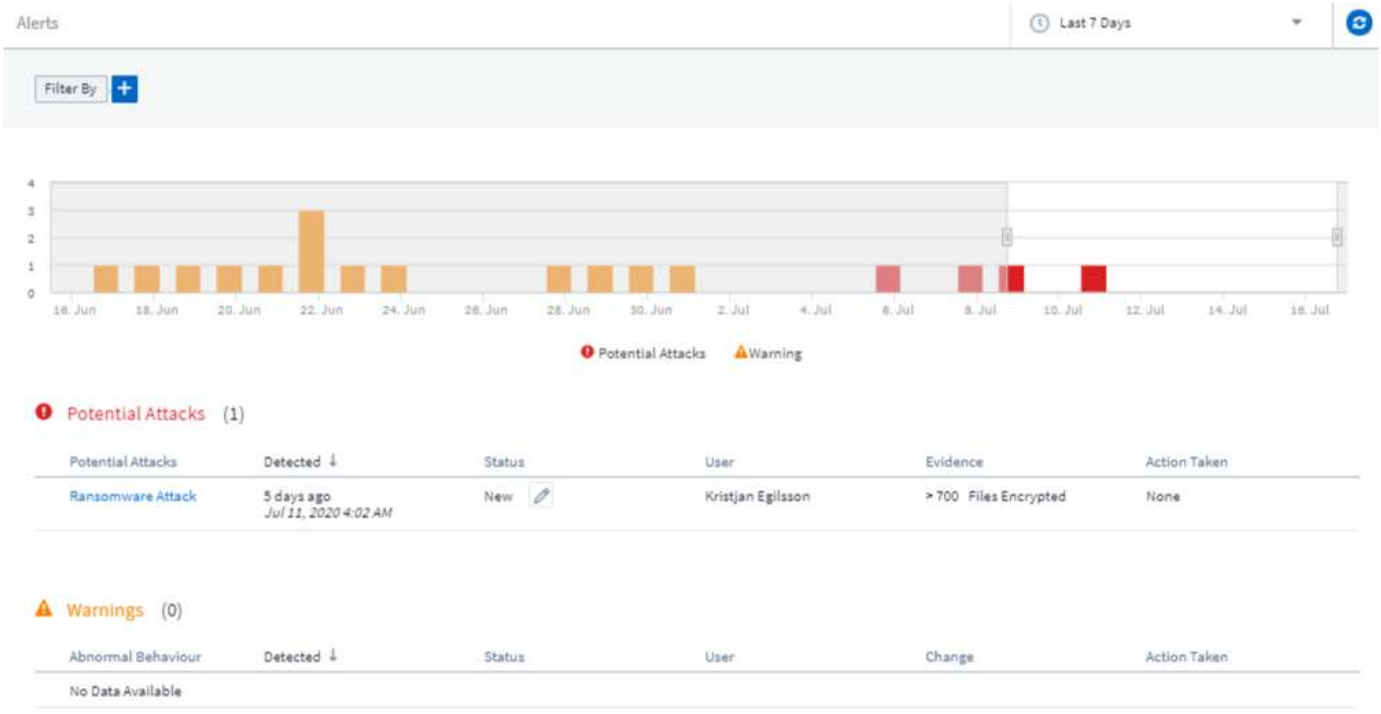
Sección de resultados del ataque:

- Número de volúmenes y archivos afectados
- Un resumen adjunto de la detección
- Gráfico que muestra la actividad de archivo durante el ataque

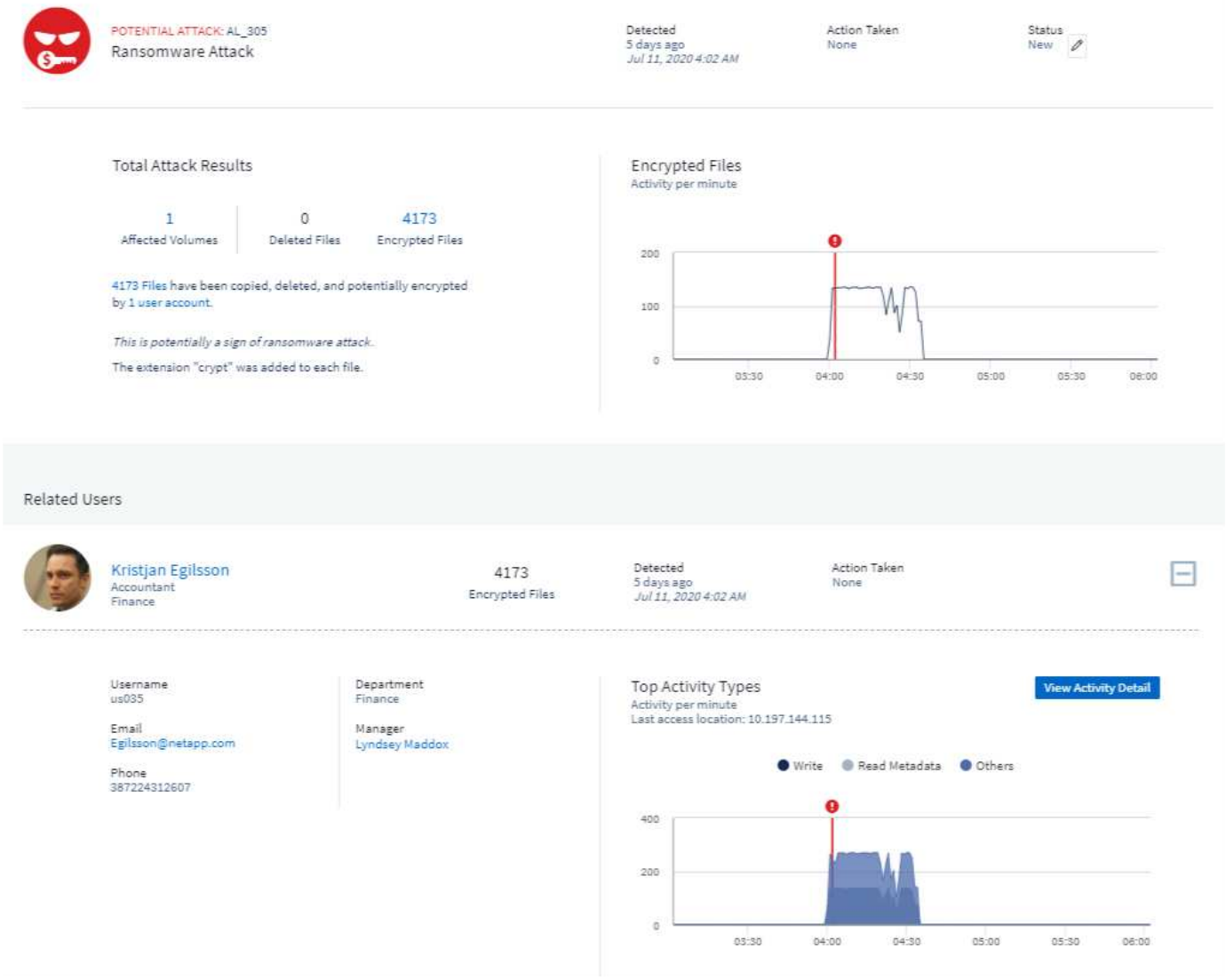
Sección usuarios relacionados:

En esta sección se muestran detalles sobre el usuario involucrado en el ataque potencial, incluido un gráfico de actividad superior para el usuario.

Página Alerts (Este ejemplo muestra un posible ataque de ransomware):



Página de detalles (este ejemplo muestra un posible ataque de ransomware):

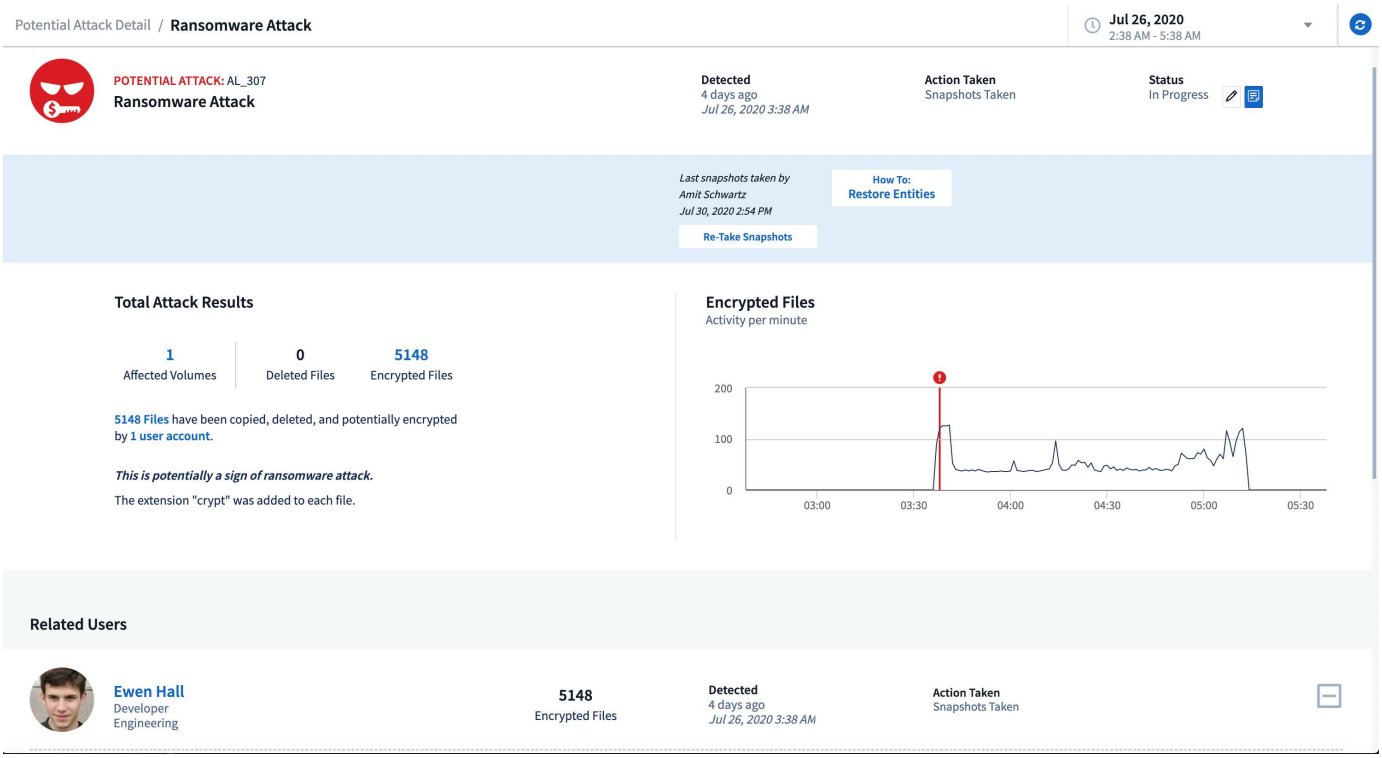


Tomar una instantánea **Acción**

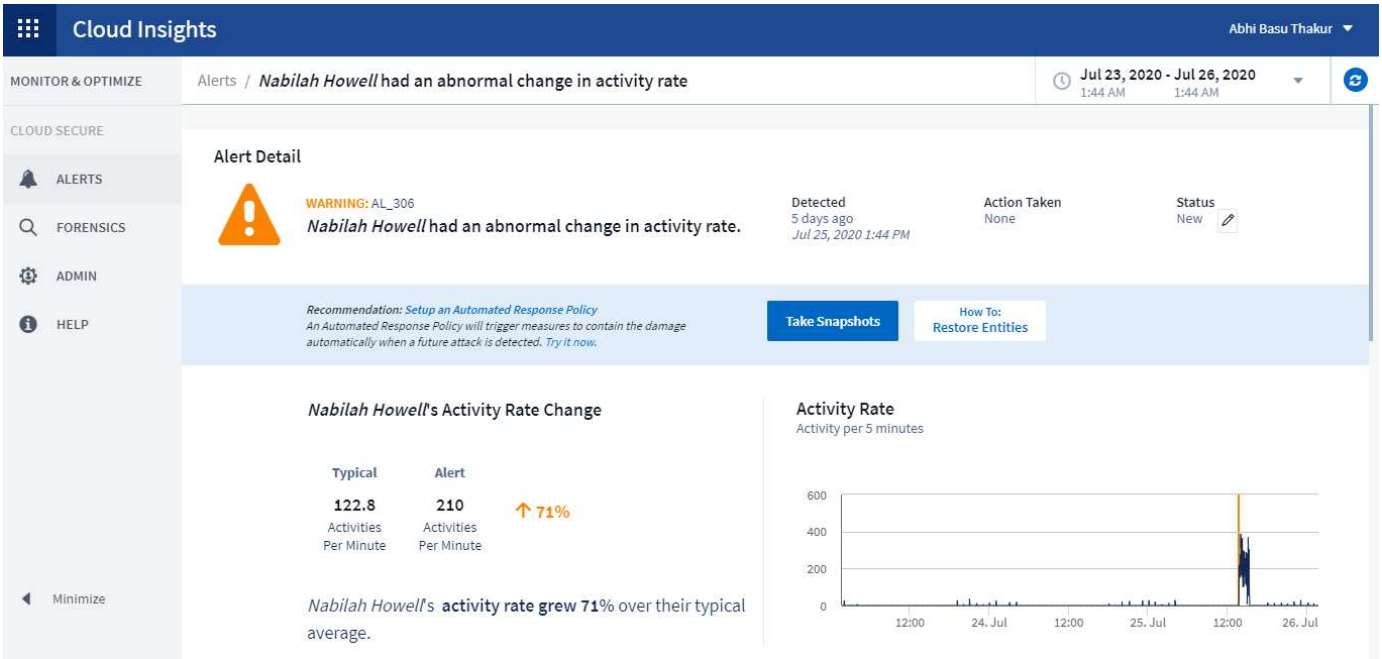
Workload Security protege los datos al tomar automáticamente una instantánea cuando se detecta una actividad maliciosa, garantizando que se realiza un backup de los datos de forma segura.

Puede definir "políticas de respuesta automatizadas" que tomar una instantánea cuando se detecte un ataque de ransomware u otra actividad anormal del usuario. También puede realizar una copia de Snapshot manualmente desde la página de alertas.

Instantánea automática realizada:



Instantánea manual:



Notificaciones de alerta

Las notificaciones por correo electrónico de alertas se envían a una lista de destinatarios de alertas para cada acción de la alerta. Para configurar destinatarios de alertas, haga clic en **Admin > Notificaciones** e introduzca una dirección de correo electrónico para cada destinatario.

Política de retención

Las alertas y advertencias se conservan durante 13 meses. Se eliminarán alertas y advertencias de más de 13 meses. Si se elimina el entorno Workload Security, también se eliminan todos los datos asociados con el

entorno.

Resolución de problemas

Problema:	Pruebe lo siguiente:
Existe una situación en la que ONTAP toma instantáneas cada hora al día. ¿Le afectarán las instantáneas de seguridad de carga de trabajo (WS)? ¿La instantánea de WS tomará el lugar de la instantánea cada hora? ¿Se detendrá la instantánea predeterminada por hora?	Las instantáneas de seguridad de carga de trabajo no afectarán a los snapshots de hora. Las instantáneas de WS no tomarán el espacio de instantáneas por hora y eso debería continuar como antes. La copia de Snapshot por hora predeterminada no se detendrá.
¿Qué sucederá si se alcanza el número máximo de snapshots en ONTAP?	Si se alcanza el número máximo de instantáneas, la toma posterior de instantáneas fallará y Workload Security mostrará un mensaje de error indicando que la instantánea está llena. El usuario tiene que definir políticas de Snapshot para eliminar las snapshots más antiguas. De lo contrario, no se harán snapshots. En ONTAP 9.3 y versiones anteriores, un volumen puede contener hasta 255 copias snapshot. A partir de la versión 9.4 de ONTAP, un volumen puede contener hasta 1023 copias snapshot. Consulte la Documentación de ONTAP para obtener información sobre "Configurando política de eliminación de Snapshot".
Workload Security no puede tomar instantáneas en absoluto.	Asegúrese de que el rol que se usa para crear instantáneas tiene un enlace: derechos apropiados asignados. Asegúrese de que *csrole* se crea con derechos de acceso adecuados para tomar instantáneas: Security login role create -vserver <vservername> -role csrole -cmddirname "volume snapshot" -access all
Las copias Snapshot fallan en alertas antiguas en las SVM que se quitaron de Workload Security y, posteriormente, se vuelven a añadir. Para las alertas nuevas que ocurren después de que se vuelve a añadir la SVM, se hacen snapshots.	Este es un escenario raro. En el caso de que experimente esto, inicie sesión en ONTAP y realice las snapshots manualmente para las alertas anteriores.
En la página *Alert Details*, el mensaje de error “Last intentando realizar error” se muestra debajo del botón *Take Snapshot*. Si se pasa el ratón por encima del error, se muestra “el comando Invoke API ha agotado el tiempo de espera para el recopilador de datos con id”.	Esto puede suceder cuando se añade un recopilador de datos al estado de carga de trabajo de seguridad mediante la IP de gestión de SVM, si la LIF de la SVM está en el estado *disabled* en ONTAP. Habilite el LIF concreto en ONTAP y active *Take Snapshot* manualmente desde Workload Security. A continuación, la acción de Snapshot tendrá éxito.

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.

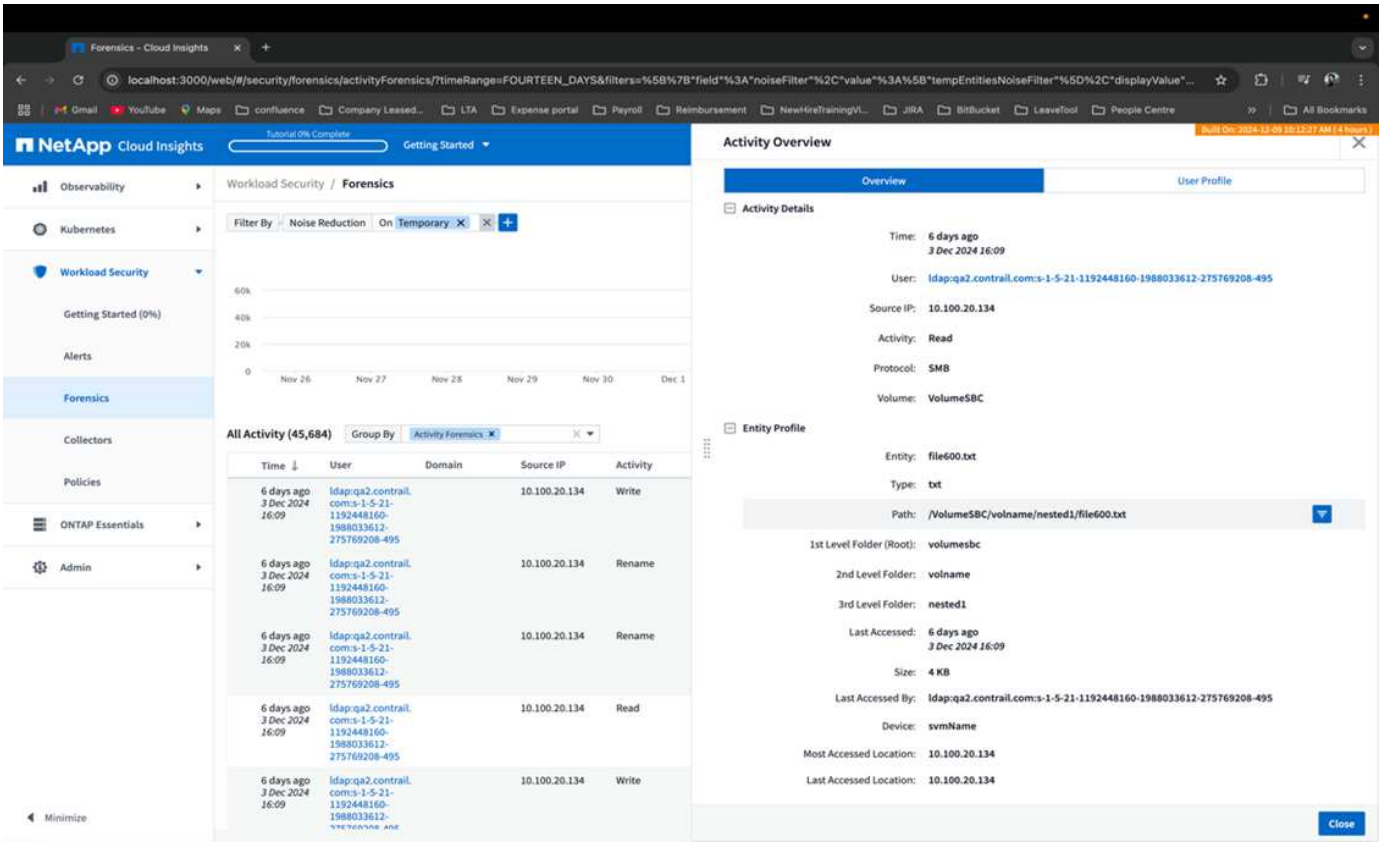
- Una lista de los datos *All Activity*.
- Una lista desplegable GROUP BY proporcionará la opción de agrupar la actividad por usuarios, ruta, tipo de entidad, etc.
- Un botón de ruta común estará disponible sobre la tabla en clic del que podemos obtener el panel deslizante con detalles de ruta de la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

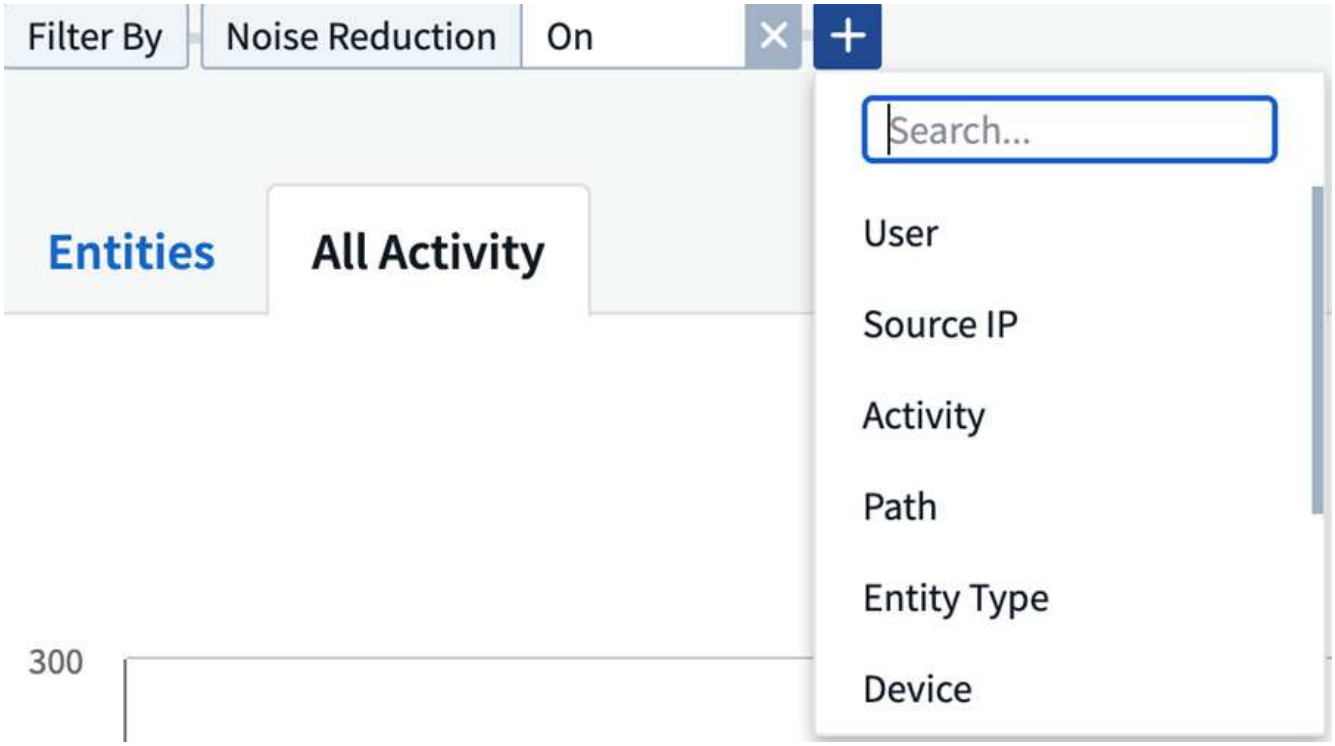
- El recuento de actividades se muestra como un hipervínculo; al seleccionarlo, se agregará la agrupación seleccionada como filtro. La tabla de actividad se actualizará en función de ese filtro.
- Tenga en cuenta que si cambia el filtro, modifica el intervalo de tiempo o actualiza la pantalla, no podrá 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.
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.

Expresión de filtro aplicada por el usuario	Resultado esperado	Evaluación del rendimiento	Comentar
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.

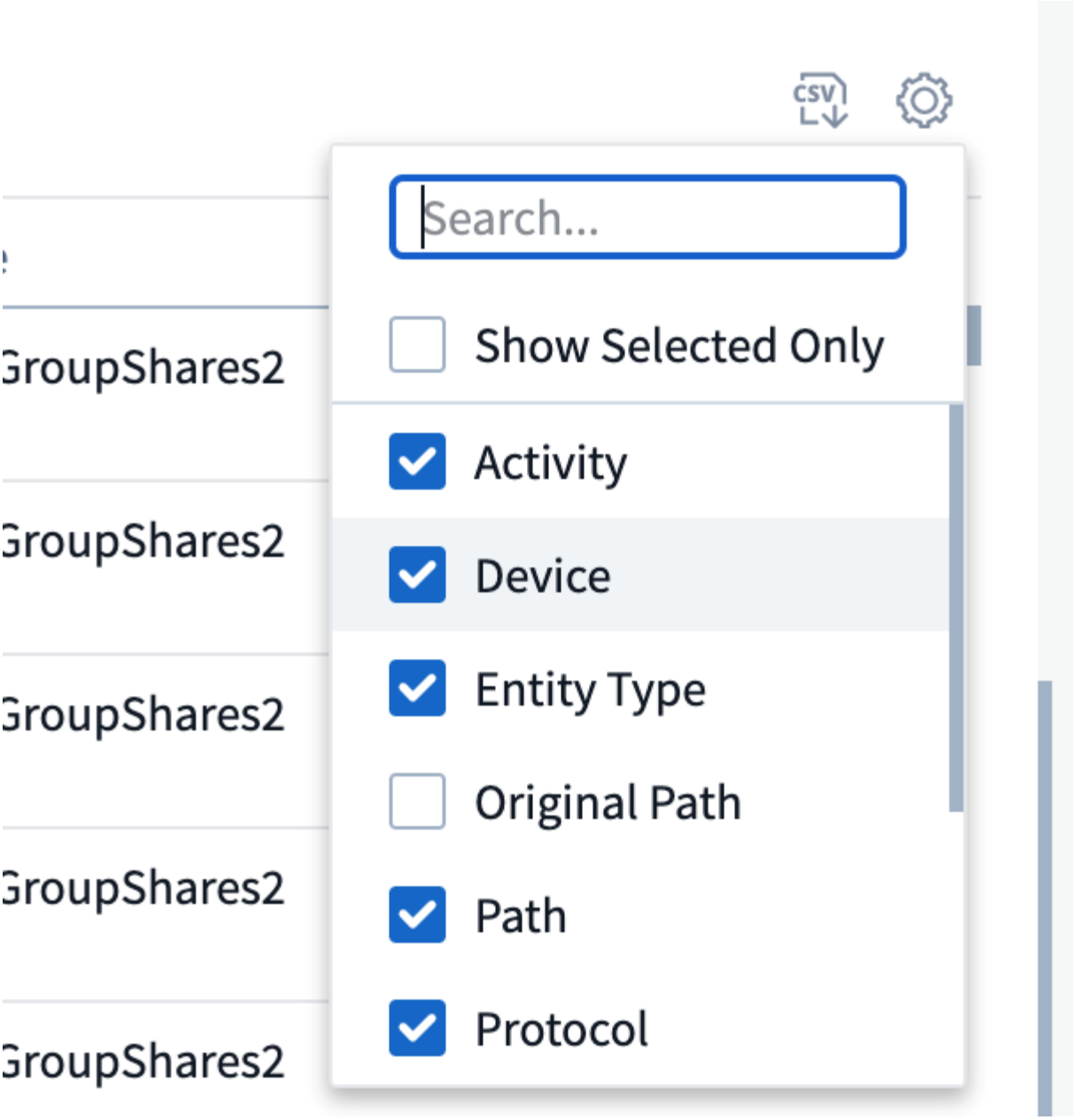
Una vez finalizado el trabajo de exportación, se activará el botón Descargar último archivo CSV de exportación.

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.

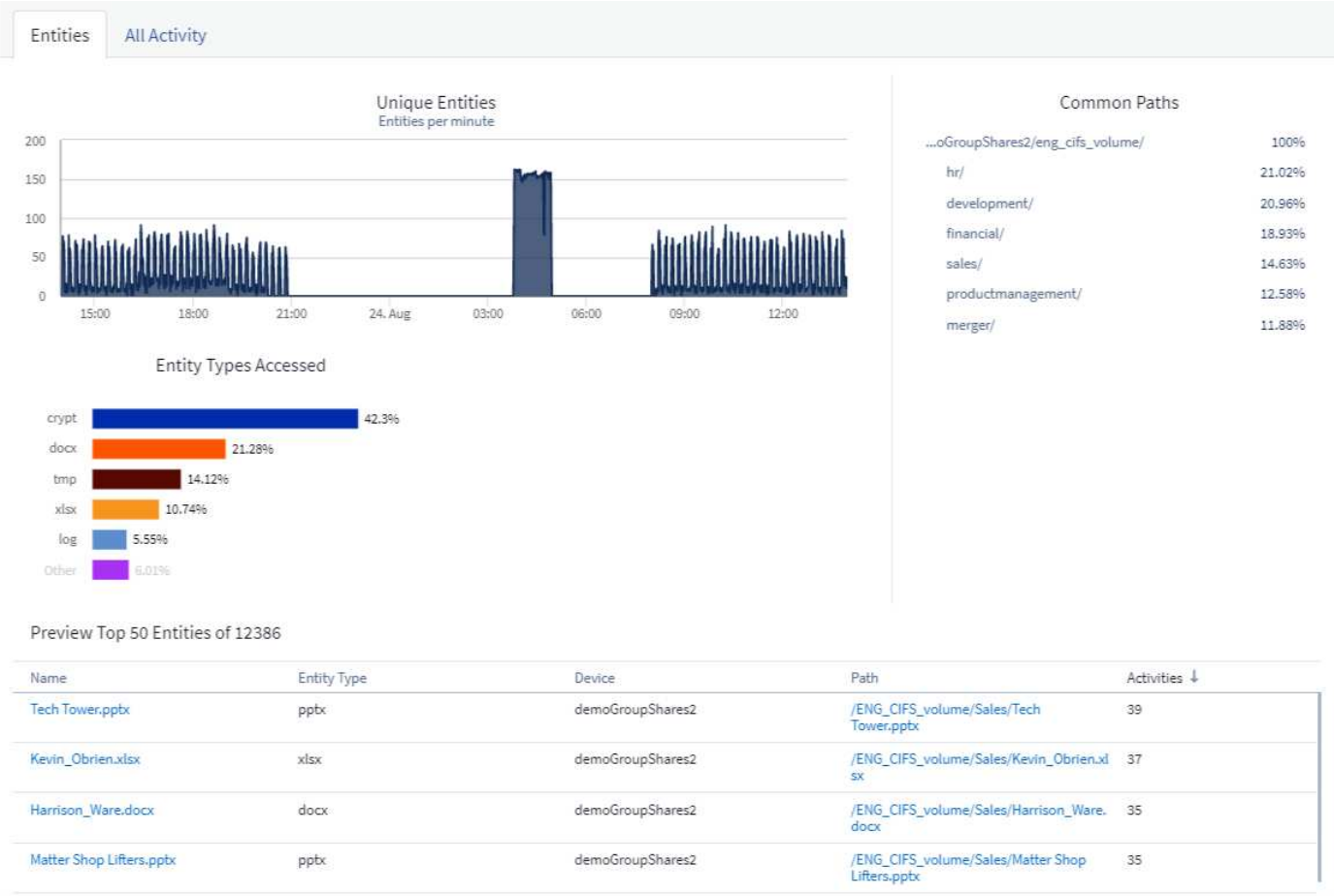
Página de entidades forenses

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

Examen de la Información de entidad

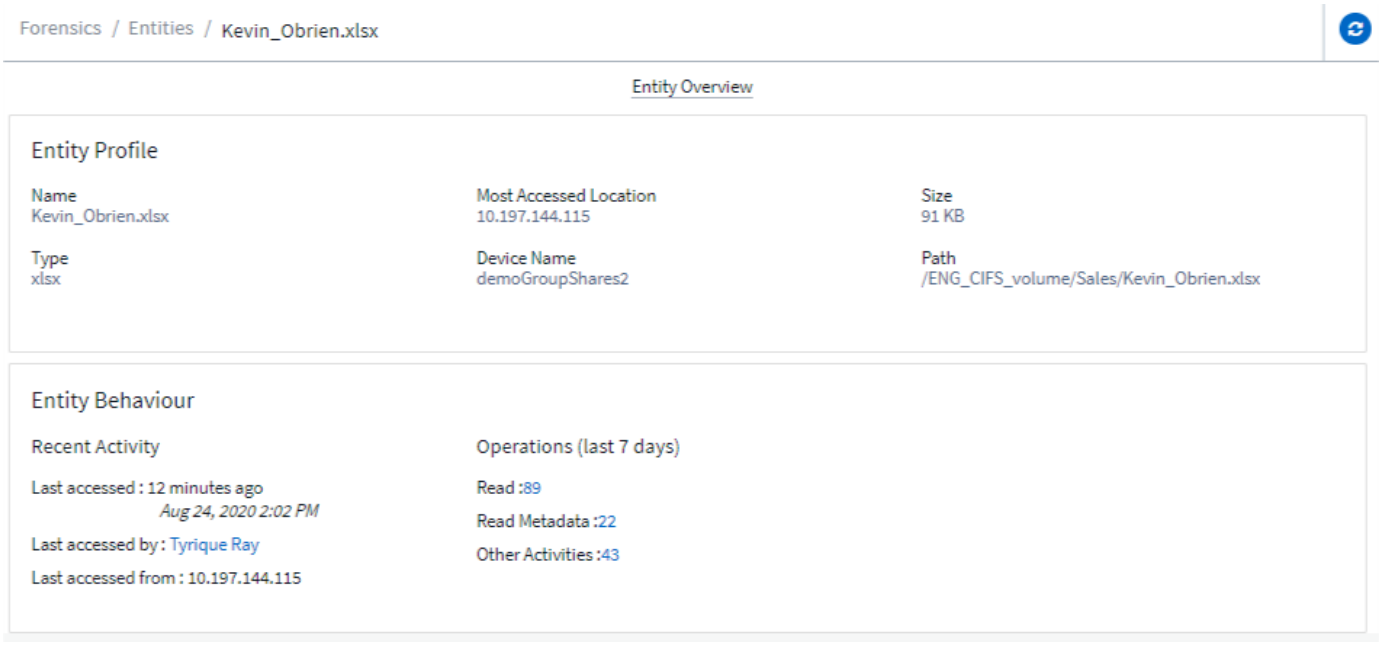
Haga clic en **Forensics > Activity Forensics** y haga clic en la ficha *Entities* para acceder a la página de entidades.

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.

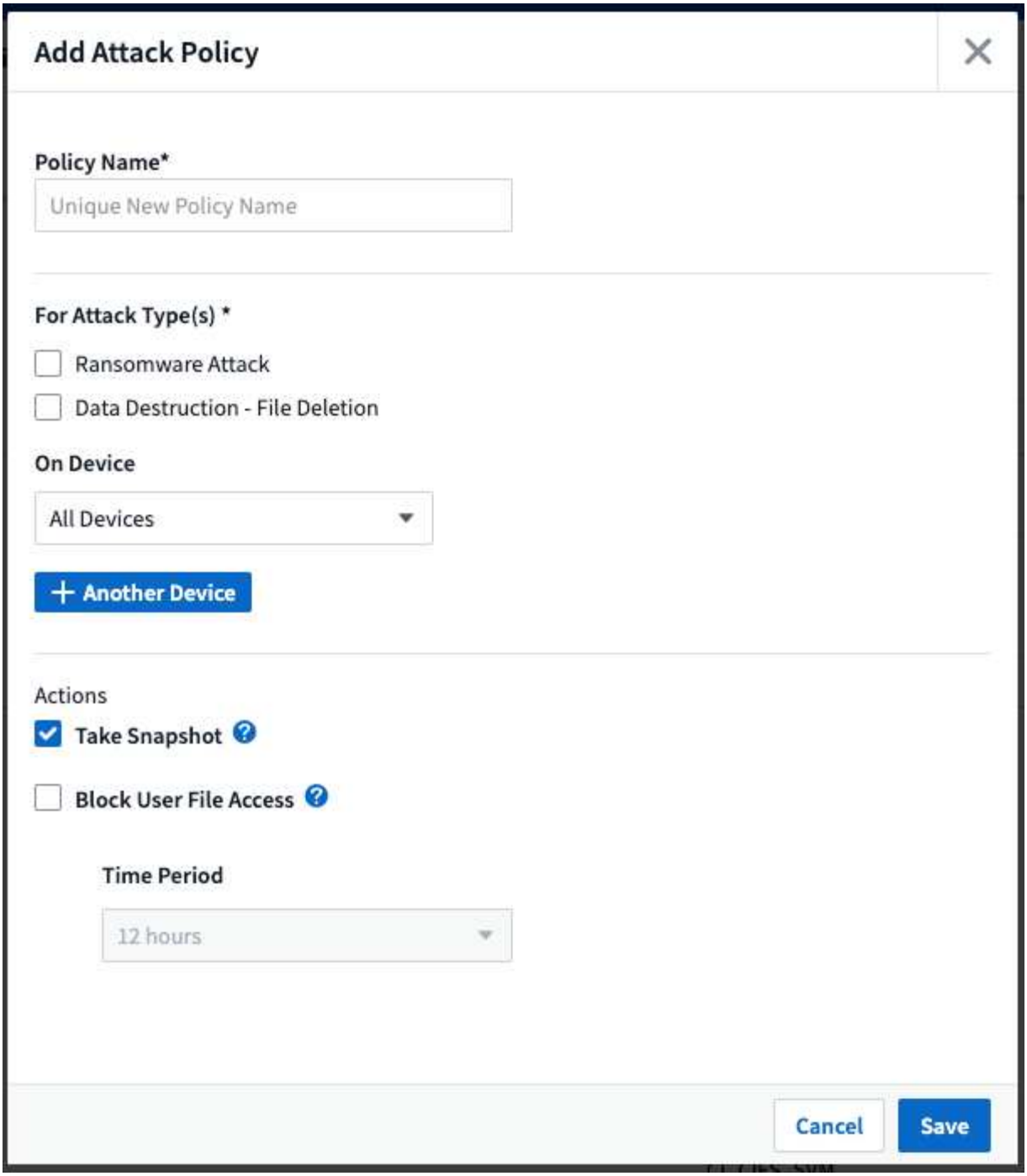
Política de retención

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.

Políticas de respuesta automatizadas

Las directivas de respuesta activan acciones como la toma de instantáneas o la restricción del acceso de los usuarios en caso de un ataque o un comportamiento anómalo del usuario.

Puede establecer políticas en dispositivos específicos o en todos los dispositivos. Para establecer una política de respuesta, seleccione **Admin > Políticas de respuesta automatizadas** y haga clic en el botón **+Policy** correspondiente. Puede crear directivas para ataques o advertencias.



Se debe guardar la política con un nombre exclusivo.

Para deshabilitar una acción de respuesta automática (por ejemplo, tomar Snapshot), solo tiene que quitar el control de la acción y guardar la política.

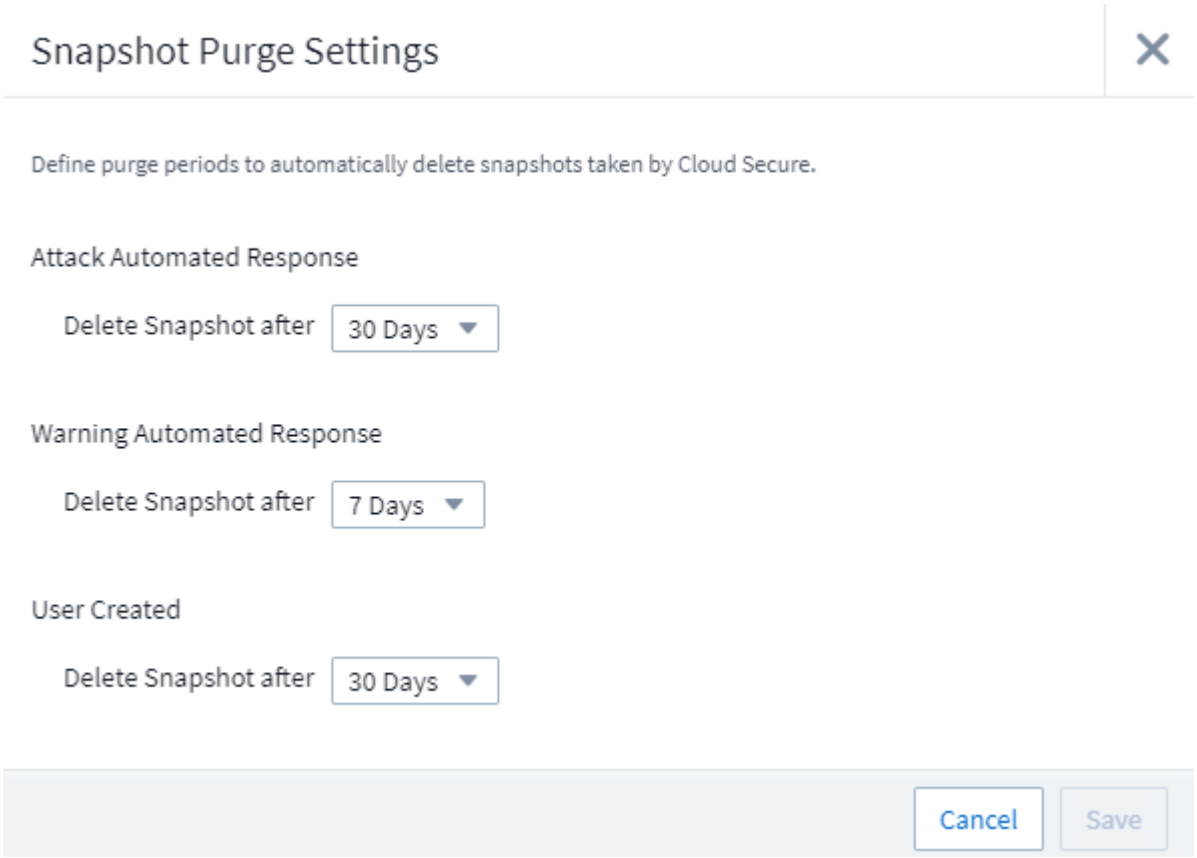
Cuando se activa una alerta en los dispositivos especificados (o en todos los dispositivos, si se ha seleccionado), la política de respuesta automática toma una instantánea de los datos. Puede ver el estado de la instantánea en la "Página de detalles Alert".

Consulte la "Restringir acceso de usuarios" página para obtener más detalles sobre la restricción del acceso de los usuarios por IP.

Puede modificar o poner en pausa una directiva de respuesta automática seleccionando la opción del menú

desplegable de la directiva.

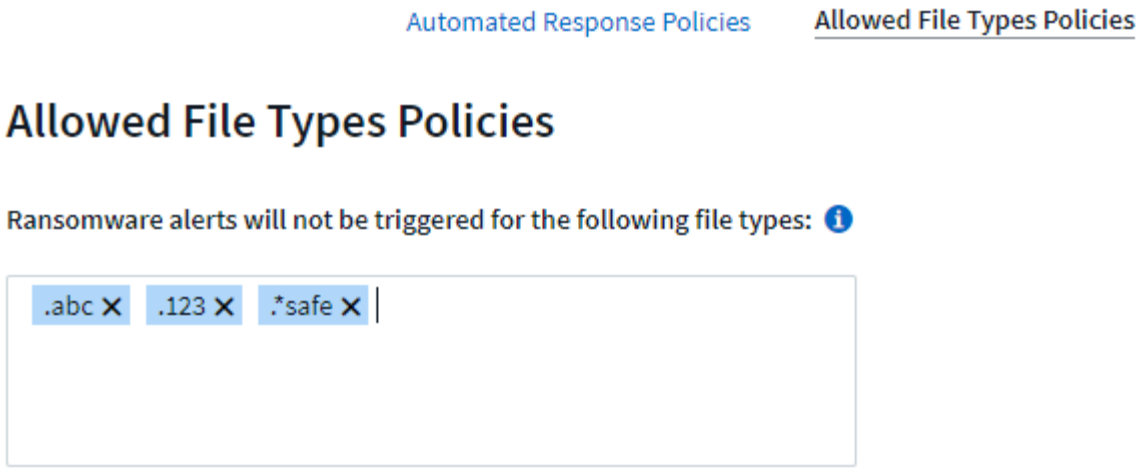
Workload Security eliminará automáticamente las snapshots una vez al día en función de la configuración de purga de snapshots.



Políticas de tipos de archivos permitidos

Si se detecta un ataque de ransomware para una extensión de archivo conocida y se generan alertas en la pantalla Alerts, esa extensión de archivo se puede agregar a una lista *allowed file types* para evitar alertas innecesarias.

Vaya a **Workload Security > Policies** y vaya a la pestaña *Allowed File Type Policies*.



Una vez agregado a la lista *allowed file types*, no se generará ninguna alerta de ataque de ransomware para ese tipo de archivo permitido. Tenga en cuenta que la política *Allowed File Types* solo se aplica para la detección de ransomware.

Por ejemplo, si se cambia el nombre de un archivo llamado *test.txt* a *test.txt.abc* y Workload Security detecta un ataque de ransomware debido a la extensión *.abc*, la extensión *.abc* se puede agregar a la lista *allowed file types*. Después de ser agregado a la lista, los ataques de ransomware ya no se generarán contra archivos con la extensión *.abc*.

Los tipos de archivo permitidos pueden ser coincidencias exactas (por ejemplo, ".abc") o expresiones (por ejemplo, "**.type", ".type**" o "**type**"). No se admiten expresiones de tipos ".a*c", ".p*f".

Integración con la protección autónoma de ransomware de ONTAP

La función de protección de ransomware autónoma de ONTAP (ARP) utiliza el análisis de cargas de trabajo en entornos NAS (NFS y SMB) para detectar de forma proactiva y advertir sobre una actividad anómala en el archivo que puede indicar un ataque de ransomware.

Se pueden encontrar detalles adicionales y requisitos de licencia sobre ARP "aquí".

Workload Security se integra con ONTAP para recibir eventos ARP y proporcionar una capa de análisis adicional y respuestas automáticas.

Workload Security recibe los eventos ARP de ONTAP y realiza las siguientes acciones:

1. Correlaciona los eventos de cifrado de volúmenes con la actividad de usuario para identificar quién está causando los daños.
2. Implementa políticas de respuesta automática (si está definido)
3. Proporciona capacidades forenses:
   - Permitir a los clientes realizar investigaciones de infracciones de datos.
   - Identificar los ficheros que se vieron afectados, lo que ayudó a recuperarse más rápidamente y llevar a cabo investigaciones de infracciones de datos.

Requisitos previos

1. Versión mínima de ONTAP: 9.11.1
2. Volúmenes con ARP habilitado. Se pueden encontrar detalles sobre la activación de ARP "aquí". ARP debe habilitarse mediante System Manager de OnCommand. La seguridad de carga de trabajo no puede habilitar ARP.
3. Se debe agregar el recopilador de seguridad de carga de trabajo a través de la IP del clúster.
4. Se necesitan credenciales para que esta función funcione. En otras palabras, se deben usar credenciales de nivel de clúster al añadir la SVM.

Se requieren permisos de usuario

Si utiliza credenciales de administración del clúster, no es necesario contar con permisos nuevos.

Si utiliza un usuario personalizado (por ejemplo, *csuser*) con permisos proporcionados al usuario, siga los pasos que se indican a continuación para otorgar permisos a Seguridad de carga de trabajo para recopilar información relacionada con ARP desde ONTAP.

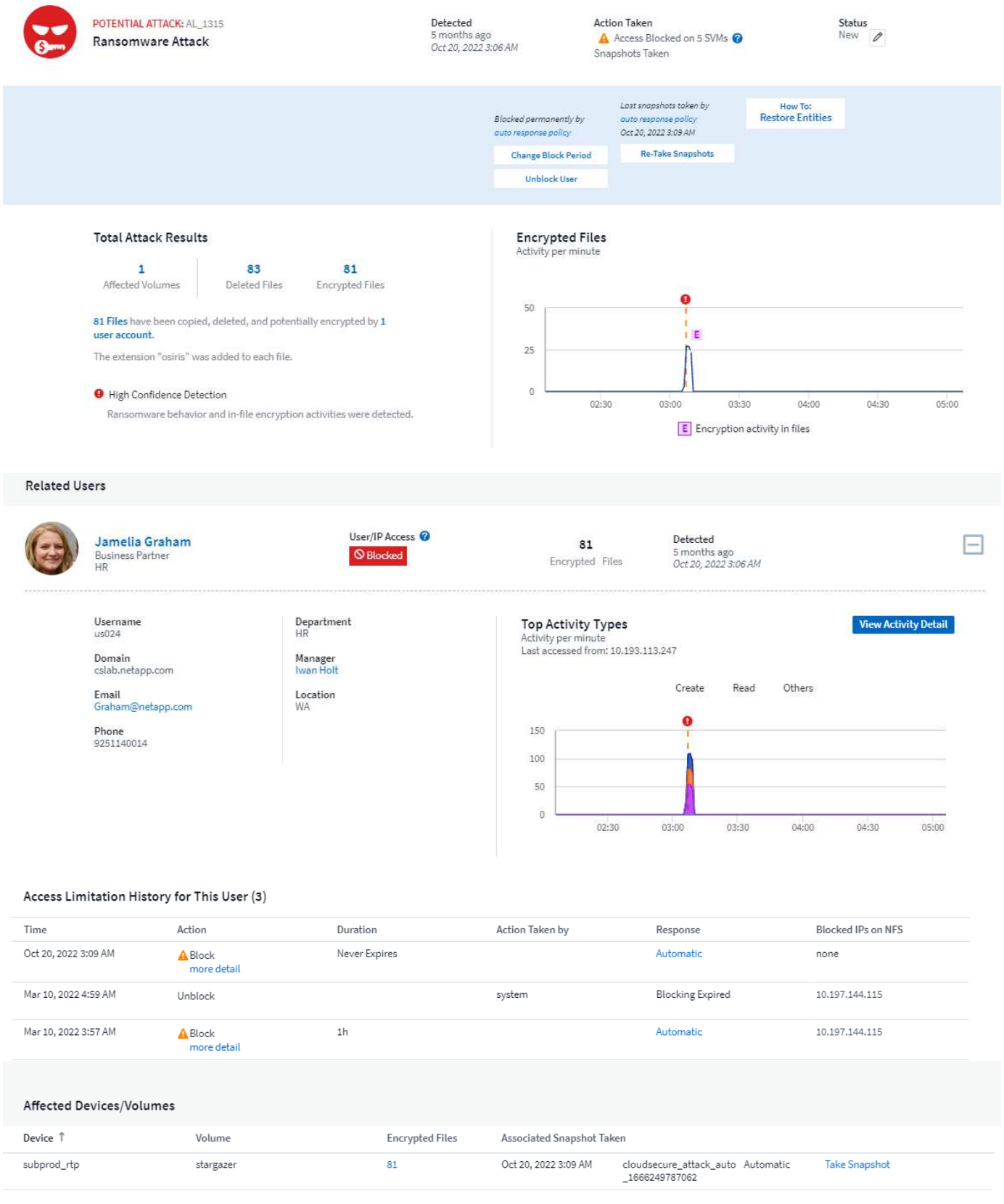
Para *csuser* con credenciales de clúster, haga lo siguiente desde la línea de comandos de ONTAP:

```
security login rest-role create -role arwrole -api /api/storage/volumes
-access readonly -vserver <cluster_name>
security login rest-role create -api /api/security/anti-ransomware -access
readonly  -role arwrole -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role arwrole
```

Leer más sobre la configuración de otros "Permisos de ONTAP".

Alerta de muestra

A continuación se muestra una alerta de muestra generada debido a un evento ARP:



Un banner de gran confianza indica que el ataque ha mostrado el comportamiento de ransomware junto con actividades de cifrado de archivos. El gráfico de archivos cifrados indica la Marca de tiempo en la que la solución ARP ha detectado la actividad de cifrado de volúmenes.

Limitaciones

En caso de que una SVM no esté supervisada por Workload Security, pero hay eventos de ARP generados por ONTAP, los eventos serán recibidos y mostrados por Workload Security. Sin embargo, la información forense relacionada con la alerta, así como la asignación de usuarios, no se capturará ni se mostrará.

Resolución de problemas

Los problemas conocidos y sus resoluciones se describen en la siguiente tabla.

Problema:	Resolución:
Las alertas por correo electrónico se reciben 24 horas después de que se detecta un ataque. En la interfaz de usuario, las alertas se muestran 24 horas antes cuando los correos electrónicos son recibidos por Data Infrastructure Insights Workload Security.	Cuando ONTAP envía el evento *Ransomware Detected* a la seguridad de las cargas de trabajo de información de la infraestructura de datos (es decir, seguridad de las cargas de trabajo), se envía el correo electrónico. El evento contiene una lista de ataques y sus marcas de tiempo. La interfaz de usuario de Workload Security muestra la Marca de tiempo de alerta del primer archivo atacado. ONTAP envía el evento *Ransomware Detected* a Información de la infraestructura de datos cuando se codifica un cierto número de archivos. Por lo tanto, es posible que haya una diferencia entre la hora en que se muestra la alerta en la interfaz de usuario y la hora en la que se envía el correo electrónico.

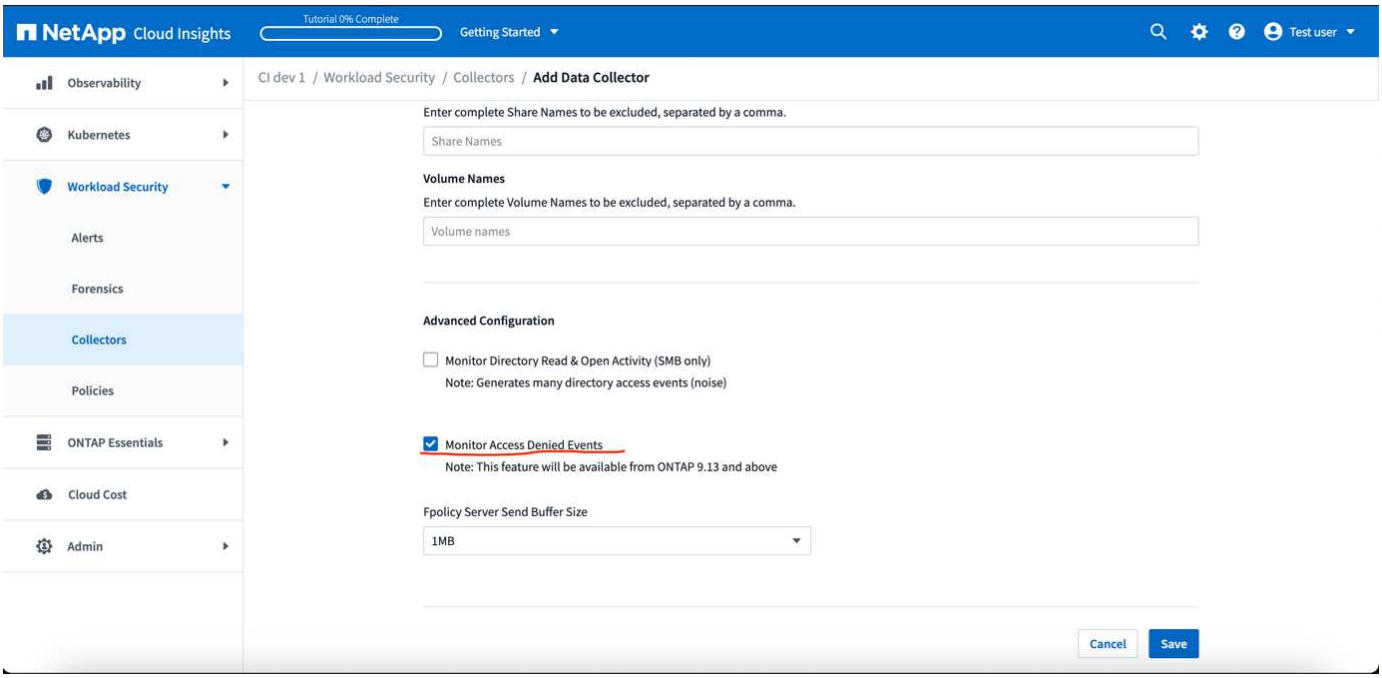
Integración con acceso ONTAP denegado

La función Acceso denegado de ONTAP utiliza análisis de carga de trabajo en entornos NAS (NFS y SMB) para detectar y advertir de forma proactiva sobre operaciones de archivos fallidas (es decir, un usuario que intenta realizar una operación para la que no tiene permiso). Estas notificaciones de operación de archivos fallidas, especialmente en casos de fallas relacionadas con la seguridad, ayudarán aún más a bloquear los ataques internos en las primeras etapas.

Información sobre la infraestructura de datos Seguridad de cargas de trabajo se integra con ONTAP para recibir acceso a eventos denegados y proporcionar una capa adicional de análisis y respuesta automática.

Requisitos previos

- Versión mínima de ONTAP: 9.13.0.
- Un administrador de seguridad de carga de trabajo debe habilitar la función Acceso denegado al agregar un nuevo recopilador o editar un recopilador existente, seleccionando la casilla de control *Monitor Access Deneged Events* en Configuración avanzada.



Se requieren permisos de usuario

Si el recopilador de datos se agrega mediante credenciales de administración de cluster, no se necesitan permisos nuevos.

Si el recopilador se agrega utilizando un usuario personalizado (por ejemplo, *csuser*) con permisos otorgados al usuario, siga los pasos que se indican a continuación para otorgar a Seguridad de carga de trabajo el permiso necesario para registrarse en eventos de acceso denegado con ONTAP.

Para csuser con credenciales *cluster*, ejecute los siguientes comandos desde la línea de comandos de ONTAP. Tenga en cuenta que *csrestrole* es un rol personalizado y *csuser* es un usuario personalizado de ONTAP.

```
 security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster_name>
 security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole
```

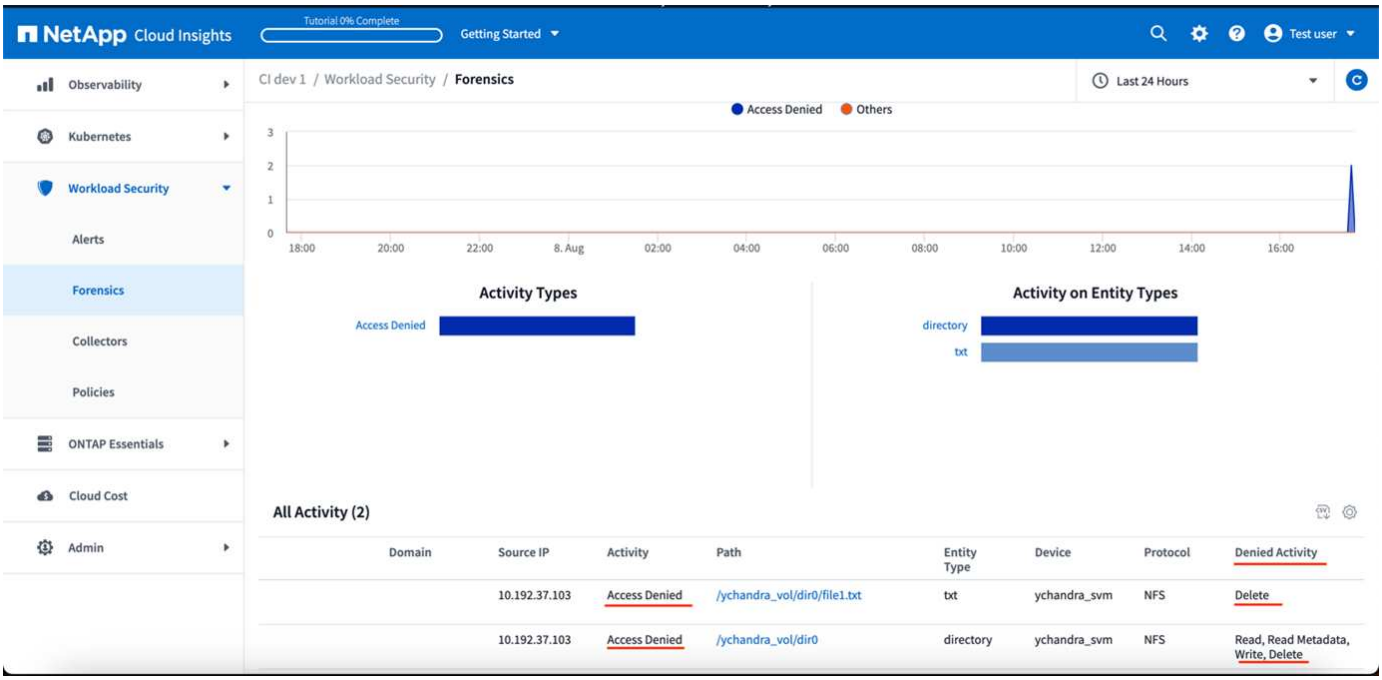
Para csuser con credenciales *SVM*, ejecute los siguientes comandos desde la línea de comandos de ONTAP:

```
 security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <svm_name>
 security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole -vserver <svm_name>
```

Leer más sobre la configuración de otros "Permisos de ONTAP".

Acceso denegado a eventos

Una vez adquiridos los eventos del sistema ONTAP, la página Forenses de Seguridad de Carga de Trabajo mostrará los eventos Acceso Denegado. Además de la información mostrada, puede ver los permisos de usuario que faltan para una operación en particular agregando la columna *Desired Activity* a la tabla desde el icono de engranaje.



Bloquear el acceso del usuario

Una vez detectado un ataque, Workload Security puede detener el ataque bloqueando el acceso del usuario al sistema de archivos. El acceso se puede bloquear automáticamente, mediante Directivas de respuesta automática o manualmente desde las páginas de alerta o de detalles del usuario.

Al bloquear el acceso de los usuarios, debe definir un período de tiempo de bloqueo. Una vez finalizado el período de tiempo seleccionado, el acceso del usuario se restaura automáticamente. El bloqueo de acceso es compatible tanto con los protocolos SMB como NFS.

El usuario está bloqueado directamente para las direcciones SMB e IP de los equipos host que provocan el ataque se bloqueará para NFS. Esas direcciones IP de la máquina no podrán acceder a ninguna de las máquinas virtuales de almacenamiento (SVM) supervisadas por Workload Security.

Por ejemplo, pongamos por caso que Workload Security gestiona 10 SVM y que la política de respuesta automática está configurada para cuatro de esos SVM. Si el ataque se origina en una de las cuatro SVM, el acceso del usuario se bloqueará en las 10 SVM. Se sigue utilizando una snapshot en la SVM de origen.

Si hay cuatro SVM con una SVM configurada para SMB, una configurada para NFS y los dos restantes configurados para NFS y SMB, todas las SVM se bloquearán si el ataque se origina en cualquiera de las cuatro SVM.

Requisitos previos para bloqueo de acceso del usuario

Se necesitan credenciales para que esta función funcione.

Si utiliza credenciales de administración del clúster, no es necesario contar con permisos nuevos.

Si utiliza un usuario personalizado (por ejemplo, *csuser*) con permisos proporcionados al usuario, siga los pasos que se indican a continuación para otorgar permisos a Workload Security para bloquear al usuario.

Para csuser con credenciales de clúster, haga lo siguiente desde la línea de comandos ONTAP:

```
security login role create -role csrole -cmddirname "vserver export-policy
rule" -access all
security login role create -role csrole -cmddirname set -access all
security login role create -role csrole -cmddirname "vserver cifs session"
-access all
security login role create -role csrole -cmddirname "vserver services
access-check authentication translate" -access all
security login role create -role csrole -cmddirname "vserver name-mapping"
-access all
```

Asegúrese de revisar la sección Permisos de la "Configurar el recopilador de datos de SVM de ONTAP" página también.

¿Cómo se habilita la función?

- En Seguridad de carga de trabajo, vaya a **Seguridad de carga de trabajo > Políticas > Políticas de respuesta automatizada**. Seleccione **+Política de ataque**.
- Seleccione (marque) *Block User File Access*.

¿Cómo configurar el bloqueo automático de acceso de usuario?

- Cree una nueva directiva de ataque o edite una directiva de ataque existente.
- Seleccione las SVM en las que debe supervisarse la política de ataque.
- Haga clic en la casilla de verificación “Bloquear acceso a archivo de usuario”. La función se activará cuando se seleccione esta opción.
- En “Time Period” (período de tiempo), seleccione la hora hasta la que se debe aplicar el bloqueo.
- Para probar el bloqueo automático de usuarios, puede simular un ataque a través de una "guión simulado".

¿Cómo saber si hay usuarios bloqueados en el sistema?

- En la página de listas de alertas, se mostrará un banner en la parte superior de la pantalla en caso de que se bloquee cualquier usuario.
- Al hacer clic en el banner, se abre la página “usuarios”, donde se puede ver la lista de usuarios bloqueados.
- En la página “Users” (usuarios), hay una columna llamada “User/IP Access” (acceso de usuario/IP). En esa columna, se mostrará el estado actual del bloqueo de usuario.

Restringir y administrar el acceso de los usuarios manualmente

- Puede ir a la pantalla de detalles de alerta o de usuario y, a continuación, bloquear o restaurar manualmente a un usuario desde dichas pantallas.

Historial de limitación de acceso del usuario

En la página de detalles de alerta y detalles de usuario, en el panel de usuario, puede ver una auditoría del historial de limitación de acceso del usuario: Tiempo, Acción (bloqueo, desbloqueo), duración, acción realizada por, IP manuales/automáticas y afectadas para NFS.

¿Cómo deshabilitar la función?

Es posible deshabilitar la función en cualquier momento. Si hay usuarios restringidos en el sistema, primero debe restaurar su acceso.

- En Seguridad de carga de trabajo, vaya a **Seguridad de carga de trabajo > Políticas > Políticas de respuesta automatizada**. Seleccione **+Política de ataque**.
- Desactive (desactive) *Bloquear acceso a archivos de usuario*.

La operación se ocultará de todas las páginas.

Restaurar manualmente las IP para NFS

Siga estos pasos para restaurar manualmente cualquier IP desde ONTAP si finaliza la prueba de seguridad de la carga de trabajo o si el agente/recopilador está inactivo.

1. Enumere todas las políticas de exportación de una SVM.

```
contrail-qa-fas8020::> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- ---------------------
---------
svm0         default         1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm1         default         4       cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm3         test            3       cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
4 entries were displayed.
```

2. Elimine las reglas en todas las directivas de la SVM que tengan “cloudsecure_rule” como Client Match especificando su respectivo RuleIndex. La regla de seguridad de la carga de trabajo suele estar en 1.

```
 contrail-qa-fas8020::*> export-policy rule delete -vserver <svm name>
-policyname * -ruleindex 1
. Asegúrese de que se elimine la regla de seguridad de la carga de
trabajo (paso opcional para confirmar).
```

```
contrail-qa-fas8020::*> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- ---------------------
---------
svm0         default         4       cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            3       cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
2 entries were displayed.
```

Restaurar manualmente usuarios para SMB

Siga estos pasos para restaurar manualmente cualquier usuario de ONTAP si finaliza la prueba de seguridad de la carga de trabajo o si el agente/recopilador está inactivo.

Puede obtener la lista de usuarios bloqueados en Workload Security desde la página de lista de usuarios.

1. Inicie sesión en el clúster de ONTAP (donde desea desbloquear los usuarios) con las credenciales del clúster *admin*. (Para Amazon FSX, inicie sesión con las credenciales de FSX).
2. Ejecute el siguiente comando para enumerar todos los usuarios bloqueados por Workload Security for SMB en todas las SVM:

```
vserver name-mapping show -direction win-unix -replacement " "
```

```
Vserver:   <vservername>
Direction: win-unix
Position Hostname         IP Address/Mask
-------- ---------------- ----------------
1       -                -                    Pattern: CSLAB\\US040
                                          Replacement:
2       -                -                    Pattern: CSLAB\\US030
                                          Replacement:
2 entries were displayed.
```

En la salida anterior, se bloquearon 2 usuarios (US030, US040) con el dominio CSLAB.

1. Una vez que identificamos la posición de la salida anterior, ejecute el siguiente comando para desbloquear al usuario:

```
 vserver name-mapping delete -direction win-unix -position <position>
. Confirme que los usuarios no están bloqueados mediante la ejecución
del comando:
```

```
vserver name-mapping show -direction win-unix -replacement " "
```

No se deben mostrar entradas para los usuarios bloqueados anteriormente.

Resolución de problemas

Problema	Pruebe esto
Algunos de los usuarios no se están restringiendo, aunque hay un ataque.	1. Asegúrese de que el recopilador de datos y el agente de las SVM están en estado *Running*. Workload Security no podrá enviar comandos si se detienen el recopilador de datos y el agente. 2. Esto se debe a que el usuario puede haber accedido al almacenamiento desde una máquina con una nueva IP que no se ha utilizado antes. La restricción ocurre mediante la dirección IP del host a través del cual el usuario accede al almacenamiento. Compruebe en la interfaz de usuario (Detalles de alerta > Historial de limitación de acceso para este usuario > IP afectadas) la lista de direcciones IP restringidas. Si el usuario accede al almacenamiento desde un host con una IP diferente a las IP restringidas, el usuario podrá seguir accediendo al almacenamiento a través de la IP sin restricciones. Si el usuario intenta acceder desde los hosts cuyas IP están restringidas, no se podrá acceder al almacenamiento.
Al hacer clic manualmente en restringir acceso se proporciona “las direcciones IP de este usuario ya han sido restringidas”.	La dirección IP que se va a restringir ya está restringida a otro usuario.
No se ha podido modificar la política. Motivo: No está autorizado para ese comando.	Compruebe si está utilizando csuser, los permisos se conceden al usuario como se ha mencionado anteriormente.

Problema	Pruebe esto
El bloqueo del usuario (dirección IP) para NFS funciona, pero para SMB / CIFS, aparece un mensaje de error: “Error de la transformación de SID a DomainName. Motivo de tiempo de espera: No se ha establecido el socket”	Esto puede suceder es *csuser* no tiene permiso para realizar ssh. (Asegúrese de conexión a nivel de clúster y, a continuación, asegúrese de que el usuario pueda realizar ssh). el rol *csuser* requiere estos permisos. https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blocking Para *csuser* con credenciales de cluster, realice lo siguiente desde la línea de comandos de ONTAP: Security login role create -role csrole -CMdirname «vserver export-policy rule» -access all security login role create -role csrole -CMdirname set -access all security login role create -role csrole ONTAP
Estoy recibiendo el mensaje de error *SID translate failed. REASON:255:Error: Comando fallido: No autorizado para ese comando Error: “Access-check” no es un comando reconocido*, cuando un usuario debería haber sido bloqueado.	Esto puede suceder cuando *csuser* no tiene los permisos correctos. Consulte "Requisitos previos para bloqueo de acceso del usuario" para obtener más información. Después de aplicar los permisos, se recomienda reiniciar el recopilador de datos de ONTAP y el recopilador de datos del directorio de usuarios. A continuación se muestran los comandos de permiso necesarios. ---- security login role create -role csrole -cmddirname «vserver export-policy rule» -access all security login role create -role csrole -cmddirname set -access all security login role create -role csrole -cmddirname «vserver cifs session» -access all security login role create -role csrole -cmddirname «vserver services access-check authentication translate» -access all security login role create -role csrole -cmdirname «vserver name-mapping» -access all ----

Seguridad de la carga de trabajo: Simulación de un ataque

Puede utilizar las instrucciones de esta página para simular un ataque con el fin de probar o demostrar la seguridad de la carga de trabajo mediante el script de simulación de Ransomware incluido.

Cosas que tomar en cuenta antes de empezar

- El script de simulación de ransomware sólo funciona en Linux.
- La secuencia de comandos se proporciona con los archivos de instalación del agente de seguridad de carga de trabajo. Está disponible en cualquier equipo que tenga instalado un agente de seguridad de carga de trabajo.
- Puede ejecutar la secuencia de comandos en la propia máquina del agente de seguridad de carga de trabajo; no es necesario preparar otra máquina Linux. Sin embargo, si prefiere ejecutar la secuencia de comandos en otro sistema, simplemente copie la secuencia de comandos y ejecútela donde desee.

Tener al menos 1,000 archivos de ejemplo

Este script debe ejecutarse en una SVM con una carpeta que tenga archivos para cifrar. Recomendamos tener al menos 1,000 archivos dentro de esa carpeta y cualquier subcarpeta. Los archivos no deben estar vacíos. No cree los archivos ni los cifre utilizando el mismo usuario. La seguridad de la carga de trabajo considera que se trata de una actividad de bajo riesgo y, por lo tanto, no generará una alerta (es decir, el mismo usuario modifica los archivos que acaba de crear).

Consulte a continuación las instrucciones para "cree archivos no vacíos mediante programación".

Directrices antes de ejecutar el simulador:

1. Asegúrese de que los archivos cifrados no están vacíos.
2. Asegúrese de cifrar > 50 archivos. Se ignorará un pequeño número de archivos.
3. No ejecute un ataque varias veces con el mismo usuario. Después de algunas veces, Workload Security aprenderá el comportamiento de este usuario y asumirá que es el comportamiento normal del usuario.
4. No cifre los archivos que acaba de crear el mismo usuario. El cambio de un archivo que acaba de crear un usuario no se considera una actividad arriesgada. En su lugar, utilice los archivos creados por otro usuario O espere unas horas entre crear los archivos y cifrarlos.

Prepare el sistema

En primer lugar, monte el volumen objetivo en la máquina. Puede montar un montaje NFS o una exportación CIFS.

Para montar la exportación NFS en Linux:

```
mount -t nfs -o vers=4.0 10.193.177.158:/svmvol1 /mntpt
mount -t nfs -o vers=4.0 Vserver data IP>:/nfsvol /destinationlinuxfolder
```

No monte NFS versión 4.1; no es compatible con Fpolicy.

Para montar CIFS en Linux:

```
 mount -t cifs //10.193.77.91/sharedfolderincluster
/root/destinationfolder/ -o username=raisa
A continuación, configure un recopilador de datos:
```

1. Configure el agente de seguridad de carga de trabajo si no lo ha hecho todavía.
2. Configure el recopilador de datos de SVM si aún no ha terminado.

Ejecute el script Ransomware Simulator

1. Inicie sesión (ssh) en la máquina del agente de seguridad de carga de trabajo.
2. Desplácese hasta: */opt/netapp/cloudsecure/agent/install*
3. Llame al script del simulador sin parámetros para ver el uso:

```
# pwd
/opt/netapp/cloudsecure/agent/install
# ./ransomware_simulator.sh
Error: Invalid directory  provided.
Usage: ./ransomware_simulator.sh [-e] [-d] [-i <input_directory>]
       -e to encrypt files (default)
       -d to restore files
       -i <input_directory> - Files under the directory to be encrypted
```

```
Encrypt command example: ./ransomware_simulator.sh -e -i
/mnt/audit/reports/
Decrypt command example: ./ransomware_simulator.sh -d -i
/mnt/audit/reports/
```

Cifre sus archivos de prueba

Para cifrar los archivos, ejecute el siguiente comando:

```
# ./ransomware_simulator.sh -e -i /root/for/
Encryption key is saved in /opt/netapp/cloudsecure/cloudsecure-agent-
1.251.0/install/encryption-key,
which can be used for restoring the files.
Encrypted /root/for/File000.txt
Encrypted /root/for/File001.txt
Encrypted /root/for/File002.txt
...
```

Restaurar archivos

Para descifrar, ejecute el siguiente comando:

```
[root@scspa2527575001 install]# ./ransomware_simulator.sh -d -i /root/for/
File /root/for/File000.txt is restored.
File /root/for/File001.txt is restored.
File /root/for/File002.txt is restored.
...
```

Ejecute el script varias veces

Después de generar un ataque de ransomware para un usuario, cambie a otro usuario para generar un ataque adicional. Workload Security aprende el comportamiento del usuario y no avisa sobre los ataques repetidos de ransomware dentro de un período de tiempo breve para el mismo usuario.

Cree archivos mediante programación

Antes de crear los archivos, primero debe detener o pausar el procesamiento del recopilador de datos. Realice los pasos siguientes antes de agregar el recopilador de datos al agente. Si ya ha agregado el recopilador de datos, simplemente edite el recopilador de datos, introduzca una contraseña no válida y guárdelo. Esto pondrá temporalmente el recopilador de datos en el estado de error. NOTA: Asegúrese de anotar la contraseña original.

La opción recomendada es "pausar el recopilador"antes de crear los archivos.]

Antes de ejecutar la simulación, primero debe agregar archivos para su cifrado. Puede copiar manualmente los archivos que se van a cifrar en la carpeta de destino o utilizar una secuencia de comandos (vea el ejemplo siguiente) para crear los archivos mediante programación. Sea cual sea el método que utilice, copie al menos 1,000 archivos.

Si elige crear los archivos mediante programación, haga lo siguiente:

1. Inicie sesión en el cuadro Agente.
2. Monte una exportación NFS desde la SVM del servidor dedicado a almacenamiento al equipo del agente. CD en esa carpeta.
3. En esa carpeta, cree un archivo denominado createfiles.sh
4. Copie las siguientes líneas en ese archivo.

```
for i in {000..1000}
do
   echo hello > "File${i}.txt"
done
echo 3 > /proc/sys/vm/drop_caches ; sync
```

5. Guarde el archivo.
6. Asegúrese de que ejecuta el permiso en el archivo:

```
 chmod 777 ./createfiles.sh
. Ejecute el script:
```

```
./createfiles.sh
```

   se crearán archivos 1000 en la carpeta actual.

7. Vuelva a habilitar el recopilador de datos

   Si deshabilitó el recopilador de datos en el paso 1, edite el recopilador de datos, introduzca la contraseña correcta y guárdelo. Asegúrese de que el recopilador de datos vuelve a estar en estado de ejecución.

8. Si pausó el recopilador antes de seguir estos pasos, asegúrese de "reanude el recopilador".

Configuración de notificaciones por correo electrónico para alertas, advertencias y el estado del agente/colector de origen de datos

Para configurar los destinatarios de alertas de seguridad de carga de trabajo, haga clic en **Admin > Notificaciones** e introduzca una dirección de correo electrónico en la sección correspondiente para cada destinatario.

Alertas y advertencias de posibles ataques

Para enviar notificaciones de alerta *Potential Attack*, introduzca las direcciones de correo electrónico de los destinatarios en la sección *Send Potential Attack Alerts*. Las notificaciones por correo electrónico se envían a la lista de destinatarios de alertas para cada acción de la alerta.

Para enviar notificaciones *Warning*, introduzca las direcciones de correo electrónico de los destinatarios en la sección *Send Warning Alerts*.

Supervisión del estado de los agentes y los recopiladores de datos

Puede supervisar el estado de los agentes y los orígenes de datos mediante notificaciones.

Para recibir notificaciones en caso de que un agente o un recopilador de origen de datos no funcione, introduzca las direcciones de correo electrónico de los destinatarios en la sección *Data Collection Health Alerts*.

Tenga en cuenta lo siguiente:

- Las alertas de estado se enviarán solo después de que el agente/cobrador deje de informar durante al menos una hora.
- Sólo se envía una notificación de correo electrónico a los destinatarios previstos en un período de 24 horas, incluso si el agente o el recopilador de datos se desconecta durante más tiempo.
- En caso de fallo del agente, se enviará una alerta (no una por cobrador). El correo electrónico incluirá una lista de todas las SVM afectadas.
- Se informa de un error de recopilación de Active Directory como una advertencia; no afecta a la detección de Ransomware.
- La lista de instalación primeros pasos ahora incluye una nueva fase *Configure email Notificaciones*.

Recepción de Notificaciones de Actualización de Agente y Recopilador de Datos

- Ingrese el ID(s) de correo electrónico en “Alertas de salud de recopilación de datos”.
- Se habilita la casilla de comprobación «Enable upgrade notifications».
- Las notificaciones por correo electrónico de actualización de agente y recopilador de datos se envían a los ID de correo electrónico un día antes de la actualización planificada.

Resolución de problemas

Problema:	Pruebe esto:
Los ID de correo electrónico están presentes en las “Alertas de salud del recopilador de datos”, sin embargo, no estoy recibiendo notificaciones.	Los mensajes de correo electrónico de notificación se envían desde el dominio Información sobre infraestructuras de datos de NetApp, es decir, *accounts@service.cloudinsights.NetApp.com*. Algunas empresas bloquean los correos electrónicos entrantes si son de un dominio externo. Asegúrese de que las notificaciones externas de los dominios de NetApp Data Infrastructure Insights estén en la lista blanca.

API de seguridad de cargas de trabajo

La API de seguridad de carga de trabajo permite a los clientes y proveedores independientes de software (ISV) de NetApp integrar la seguridad de la carga de trabajo con otras aplicaciones, como CMDB u otros sistemas de emisión de boletos.

Requisitos para el acceso a API:

- Se utiliza un modelo de token de acceso de API para conceder acceso.
- La gestión de token de API la realizan los usuarios de Workload Security con la función de administrador.

Documentación de API (Swagger)

La información más reciente de la API se encuentra iniciando sesión en Workload Security y navegando a **Admin > API Access**. Haga clic en el enlace **Documentación de API**. La documentación de la API se basa en Swagger, lo que proporciona una breve descripción e información de uso para la API y le permite probarla en su inquilino.

Si llama a la API de actividad de Forensics, use la API cloudsecure_forensics.activities.**v2**. Si realiza varias llamadas a esta API, asegúrese de que las llamadas se realicen secuencialmente, no en paralelo. Varias llamadas paralelas pueden hacer que la API se agote.

Tokens de acceso API

Antes de utilizar la API de seguridad de carga de trabajo, debe crear uno o más * tokens de acceso de API*. Los tokens de acceso conceden permisos de lectura. También puede establecer la caducidad de cada token de acceso.

Para crear un token de acceso:

- Haga clic en **Admin > API Access**
- Haga clic en **+símbolo de acceso de API**
- Introduzca **Nombre de símbolo**
- Especifique **caducidad de token**

El token sólo estará disponible para copiar en el portapapeles y guardar durante el proceso de creación. Los tokens no se pueden recuperar una vez creados, por lo que se recomienda encarecidamente copiar el token y guardarlo en una ubicación segura. Se le pedirá que haga clic en el botón Copiar clave de acceso de API antes de cerrar la pantalla de creación de token.

Puede desactivar, activar y revocar tokens. Se pueden activar los tokens desactivados.

Los tokens conceden acceso a las API de propósito general desde la perspectiva del cliente, gestionando el acceso a las API en el ámbito de su propio inquilino.

La aplicación recibe un token de acceso después de que un usuario autentica correctamente y autoriza el acceso, a continuación, pasa el token de acceso como credencial cuando llama a la API de destino. El token pasado informa a la API de que el portador del token ha sido autorizado para acceder a la API y realizar acciones específicas en función del ámbito que se haya concedido durante la autorización.

El encabezado HTTP donde se pasa el token de acceso es **X-CloudInsights-ApiKey:**

Por ejemplo, utilice lo siguiente para recuperar activos de almacenamientos:

```
 curl https://<tenant_host_name>/rest/v1/cloudsecure/activities -H 'X-
CloudInsights-ApiKey: <API_Access_Token>'
Donde _<API_Access_Token>_ es el token que ha guardado durante la creación
de la clave de acceso de API.
```

Puede encontrar información detallada en el enlace *API Documentation* en **Admin > API Access**.

Script para extraer datos a través de la API

Los agentes de seguridad de carga de trabajo incluyen un script de exportación para facilitar las llamadas paralelas a la API de v2 dividiendo el rango de tiempo solicitado en lotes más pequeños.

El script está ubicado en */opt/NetApp/cloudsecure/agent/export-script*. Un archivo README en el mismo directorio proporciona instrucciones de uso.

A continuación se muestra un comando de ejemplo para invocar el script:

```
python3 data-export.py --tenant_url <tenant
id>.cs01.cloudinsights.netapp.com --access_key %ACCESS_KEY% --path_filter
"<dir path>" --user_name "<user>" --from_time "01-08-2024 00:00:00"
--to_time "31-08-2024 23:59:59" --iteration_interval 12 --num_workers 3
```

Parámetros Clave: - `--iteration_interval 12`: Divide el rango de tiempo solicitado en intervalos de 12 horas. `--num_workers 3`- : Fetches estos intervalos en paralelo usando 3 hilos.