Empezando

Data Infrastructure Insights

NetApp
February 10, 2026

Tabla de contenidos

Empezando

Introducción a la seguridad de la carga de trabajo

Workload Security le ayuda a supervisar la actividad del usuario y a detectar posibles amenazas de seguridad en su entorno de almacenamiento. Antes de poder comenzar la monitorización, es necesario configurar los agentes, los recopiladores de datos y los servicios de directorio para establecer las bases de una monitorización de seguridad integral.

El sistema de seguridad de carga de trabajo utiliza un agente para recopilar datos de acceso de los sistemas de almacenamiento e información de usuario de los servidores de servicios de directorio.

Debe configurar lo siguiente antes de poder comenzar a recopilar datos:

Tarea	Información relacionada
Configurar un agente	"Requisitos del agente" "Agregar agente"
Configurar un conector de directorio de usuarios	"Agregar conector de directorio de usuarios"
Configurar recopiladores de datos	Haga clic en **Seguridad de carga de trabajo > Recopiladores** Haga clic en el recopilador de datos que desea configurar. Consulte la sección de referencia del proveedor del recopilador de datos de la documentación para obtener información sobre el recopilador.
Crear cuentas de usuario	"Administrar cuentas de usuario"

Workload Security también puede integrarse con otras herramientas. Por ejemplo,"ver esta guía" sobre la integración con Splunk.

Requisitos del agente de seguridad de carga de trabajo

Despliega Workload Security Agents en servidores dedicados que cumplan los requisitos mínimos de sistema operativo, CPU, memoria y espacio en disco para asegurar un monitoreo y una detección de amenazas óptimos. Esta guía especifica los requisitos de hardware y red necesarios antes de "instalando tu Workload Security Agent", incluyendo las distribuciones de Linux compatibles, las reglas de conectividad de red y la guía para el dimensionamiento del sistema.

Componente	Requisitos de Linux
Sistema operativo	Un equipo que ejecuta una versión con licencia de uno de los siguientes: * AlmaLinux 9.4 (64 bits) a 9.5 (64 bits), 10 (64 bits), incluido SELinux * CentOS Stream 9 (64 bits) * Debian 11 (64 bits), 12 (64 bits), incluido SELinux * OpenSUSE Leap 15.3 (64 bits) a 15.6 (64 bits) * Oracle Linux 8.10 (64 bits), 9.1 (64 bits) a 9.6 (64 bits), incluido SELinux * Red Hat Enterprise Linux 8.10 (64 bits), 9.1 (64 bits) a 9.6 (64 bits), 10 (64 bits), incluido SELinux * Rocky 9.4 (64 bits) a 9.6 (64 bits), incluido SELinux * SUSE Linux Enterprise Server 15 SP4 (64 bits) a 15 SP6 (64 bits), incluido SELinux * Ubuntu 20.04 LTS (64 bits), 22.04 LTS (64 bits), 24.04 LTS (64 bits) Esta computadora no debe ejecutar ningún otro software de nivel de aplicación. Se recomienda un servidor dedicado.
Comandos	Se requiere 'unzip' para la instalación. Además, se requiere el comando 'sudo su –' para la instalación, la ejecución de scripts y la desinstalación.
UPC	4 núcleos de CPU
Memoria	16 GB de RAM
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 en disco adicional para permitir la creación del sistema de archivos. Asegúrese de que haya al menos 35 GB de espacio libre en el sistema de archivos. Si /opt es una carpeta montada desde 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 acceder a esta carpeta. Consulte la"solución de problemas" Sección para más detalles.
Red	Conexión Ethernet de 100 Mbps a 1 Gbps, dirección IP estática, conectividad IP a todos los dispositivos y un puerto requerido para la instancia de Workload Security (80 o 443).

Tenga en cuenta: El agente de seguridad de carga de trabajo se puede instalar en la misma máquina que una unidad y/o agente de adquisición de Data Infrastructure Insights . Sin embargo, se recomienda instalarlos en máquinas separadas. En el caso de que estén instalados en la misma máquina, 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 la hora tanto en el sistema ONTAP como en la máquina del Agente mediante el Protocolo de tiempo de red (NTP) o el Protocolo simple de tiempo de red (SNTP).

Reglas de acceso a la red en la nube

Para entornos de seguridad de carga de trabajo con sede en EE. UU.:

Protocolo	Puerto	Fuente	Destino	Descripción
TCP	443	Agente de seguridad de carga de trabajo	<nombre_del_sitio>.cs01.cloudinsights.netapp.com <nombre_del_sitio>.c01.cloudinsights.netapp.com <nombre_del_sitio>.c02.cloudinsights.netapp.com	Acceso a Data Infrastructure Insights
TCP	443	Agente de seguridad de carga de trabajo	agentlogin.cs01.cloudinsights.netapp.com	Acceso a servicios de autenticación

Para entornos de seguridad de carga de trabajo con sede en Europa:

Protocolo	Puerto	Fuente	Destino	Descripción
TCP	443	Agente de seguridad de carga de trabajo	<nombre_del_sitio>.cs01-eu-1.cloudinsights.netapp.com <nombre_del_sitio>.c01-eu-1.cloudinsights.netapp.com <nombre_del_sitio>.c02-eu-1.cloudinsights.netapp.com	Acceso a Data Infrastructure Insights
TCP	443	Agente de seguridad de carga de trabajo	agentlogin.cs01-eu-1.cloudinsights.netapp.com	Acceso a servicios de autenticación

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

Protocolo	Puerto	Fuente	Destino	Descripción
TCP	443	Agente de seguridad de carga de trabajo	<nombre_del_sitio>.cs01-ap-1.cloudinsights.netapp.com <nombre_del_sitio>.c01-ap-1.cloudinsights.netapp.com <nombre_del_sitio>.c02-ap-1.cloudinsights.netapp.com	Acceso a Data Infrastructure Insights
TCP	443	Agente de seguridad de carga de trabajo	agentlogin.cs01-ap-1.cloudinsights.netapp.com	Acceso a servicios de autenticación

Reglas dentro de la red

Protocolo	Puerto	Fuente	Destino	Descripción
TCP	389(LDAP) 636 (LDAP/start-tls)	Agente de seguridad de carga de trabajo	URL del servidor LDAP	Conectarse a LDAP
TCP	443	Agente de seguridad de carga de trabajo	Dirección IP de administración de clúster o SVM (según la configuración del recopilador SVM)	Comunicación API con ONTAP

Protocolo	Puerto	Fuente	Destino	Descripción
TCP	35000 - 55000	Direcciones IP de LIF de datos SVM	Agente de seguridad de carga de trabajo	Comunicación de ONTAP al agente de seguridad de carga de trabajo para eventos Fpolicy. Estos puertos deben estar abiertos hacia el Agente de Seguridad de Carga de Trabajo para que ONTAP pueda enviarle eventos, incluido cualquier firewall en el mismo Agente de Seguridad de Carga de Trabajo (si está presente). TENGA EN CUENTA que no es necesario reservar **todos** estos puertos, pero los puertos que reserve para esto deben estar dentro de este rango. Se recomienda comenzar reservando ~100 puertos y aumentar si es necesario.

Protocolo	Puerto	Fuente	Destino	Descripción
TCP	35000-55000	IP de gestión de clúster	Agente de seguridad de carga de trabajo	Comunicación de la IP de administración de clúster de ONTAP al agente de seguridad de carga de trabajo para **eventos EMS**. Estos puertos deben estar abiertos hacia el Agente de Seguridad de Carga de Trabajo para que ONTAP pueda enviarle **eventos EMS**, incluido cualquier firewall en el propio Agente de Seguridad de Carga de Trabajo (si está presente). TENGA EN CUENTA que no es necesario reservar **todos** estos puertos, pero los puertos que reserve para esto deben estar dentro de este rango. Se recomienda comenzar reservando ~100 puertos y aumentar si es necesario.
SSH	22	Agente de seguridad de carga de trabajo	Gestión de clústeres	Necesario para el bloqueo de usuarios CIFS/SMB.

Dimensionamiento del sistema

Ver el"Comprobador de tasa de eventos" Documentación para obtener información sobre el tamaño.

Implementar agentes de seguridad de carga de trabajo

Los agentes de seguridad de carga de trabajo son esenciales para monitorear la actividad del usuario y detectar posibles amenazas a la seguridad en su infraestructura de almacenamiento. Esta guía proporciona instrucciones de instalación paso a paso, mejores prácticas para la gestión de agentes (incluidas capacidades de pausa/reanudación y fijación/desfijación) y requisitos de configuración posteriores a la implementación. Antes de comenzar, asegúrese de que su servidor de agente cumpla

con los "Requisitos del sistema".

Antes de empezar

- El privilegio sudo es necesario para la instalación, la ejecución de scripts y la desinstalación.
- Durante la instalación del agente, se crean un usuario local *cssys* y un grupo local *cssys* en la máquina. 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" .

Mejores prácticas

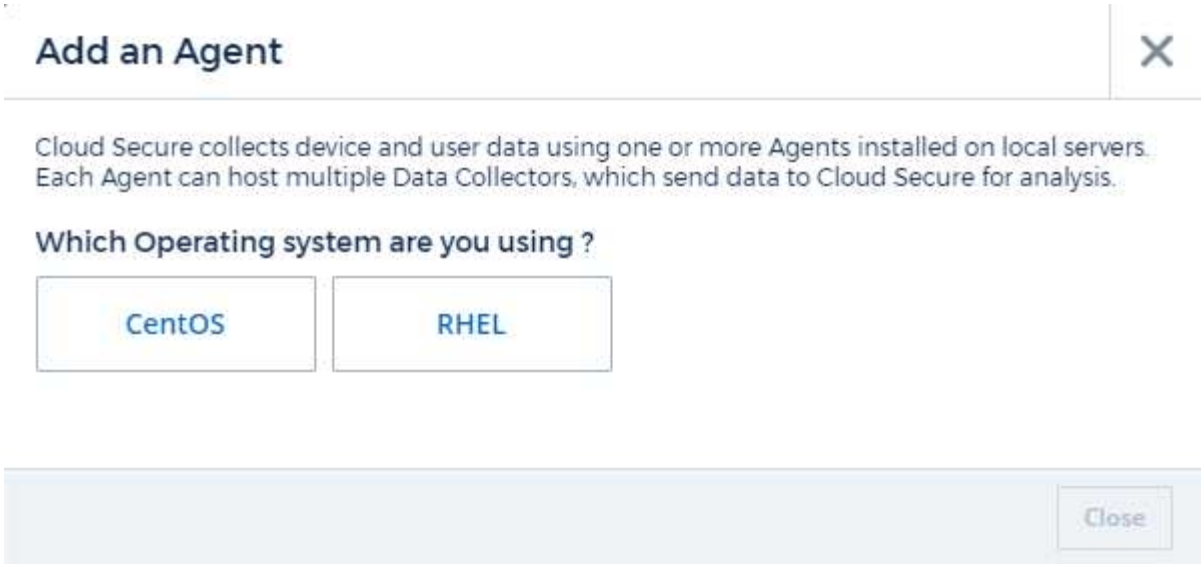
Tenga en cuenta lo siguiente antes de configurar su agente de seguridad de carga de trabajo.

Pausa y reanudar	Pausa: Elimina fpolicies de ONTAP. Se suele utilizar cuando los clientes realizan actividades de mantenimiento prolongadas que pueden llevar mucho tiempo, como reinicios de máquinas virtuales de agentes o reemplazos de almacenamiento. Resumen: Se vuelven a agregar las políticas fpolicies a ONTAP.
Anclar y desanclar	Unpin descarga inmediatamente la última versión (si está disponible) y actualiza el agente y el recopilador. Durante esta actualización, fpolicies se desconectará y volverá a conectarse. Esta función está diseñada para clientes que desean controlar el momento de las actualizaciones automáticas. Véase más abajo paraInstrucciones para fijar/desfijar .
Enfoque recomendado	Para configuraciones grandes, es recomendable usar Pin y Unpin en lugar de pausar los colectores. No es necesario pausar ni reanudar la actividad al usar las funciones de fijar y desfijar. Los clientes pueden mantener sus agentes y recopiladores vinculados y, al recibir una notificación por correo electrónico sobre una nueva versión, disponen de un plazo de 30 días para actualizar selectivamente los agentes uno por uno. Este enfoque minimiza el impacto de la latencia en las políticas de fpolicies y proporciona un mayor control sobre el proceso de actualización.

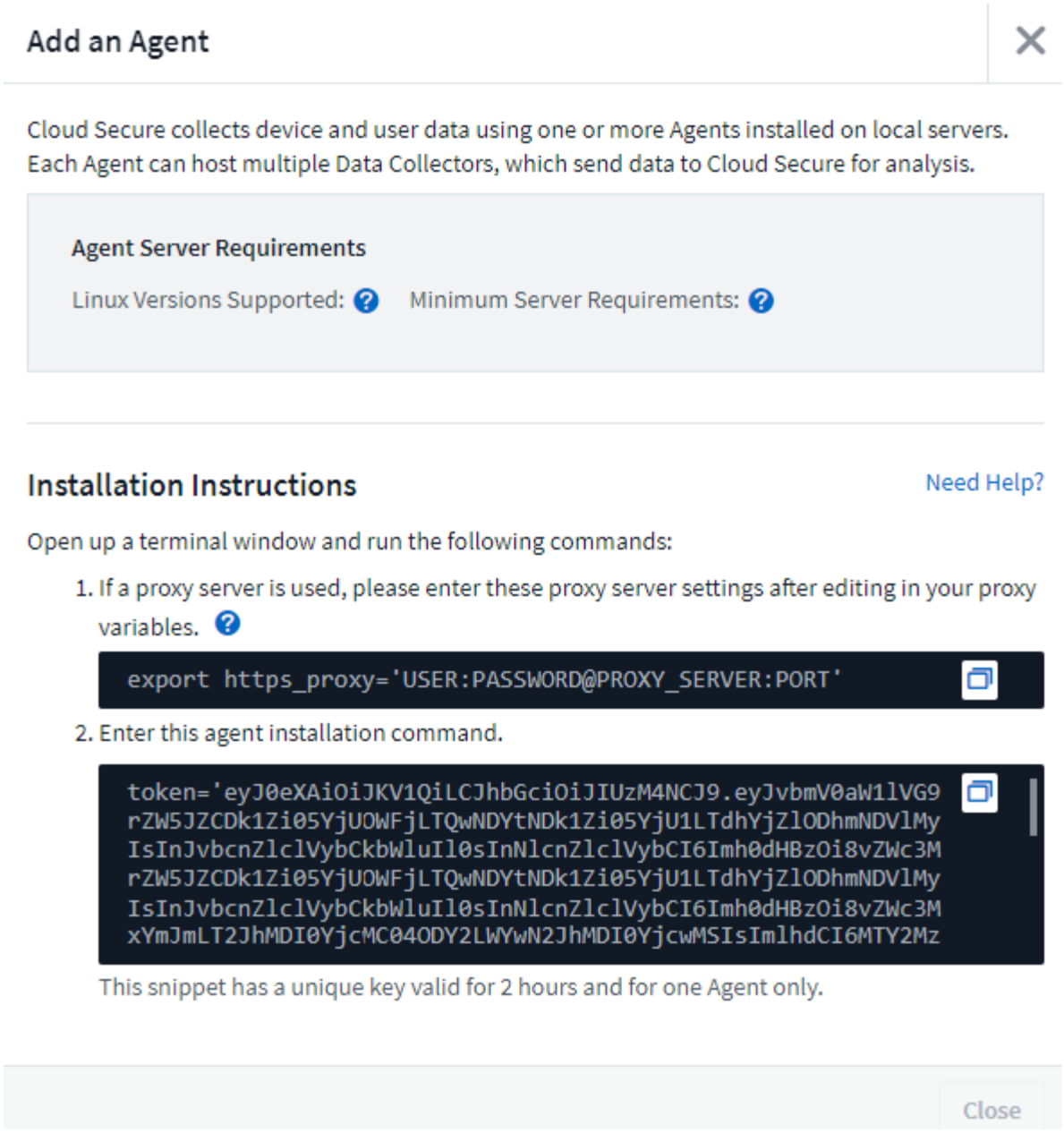
Pasos para instalar el agente

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

   El sistema muestra la página Agregar un agente:



3. Verifique que el servidor del agente cumpla con los requisitos mínimos del sistema.
4. Para verificar que el servidor del agente esté ejecutando una versión compatible de Linux, haga clic en *Versiones compatibles (i)*.
5. Si su red utiliza un servidor proxy, configure los detalles del servidor proxy siguiendo las instrucciones en 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. Necesitas configurar un"Recopilador de directorios de usuarios" .
2. Necesita configurar uno o más recopiladores de datos.

Configuración de red

Ejecute los siguientes comandos en el sistema local para abrir los puertos que utilizará Workload Security. Si existe un problema de seguridad con respecto al rango de puertos, puede utilizar un rango 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`

Sigue los siguientes pasos según tu 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
```

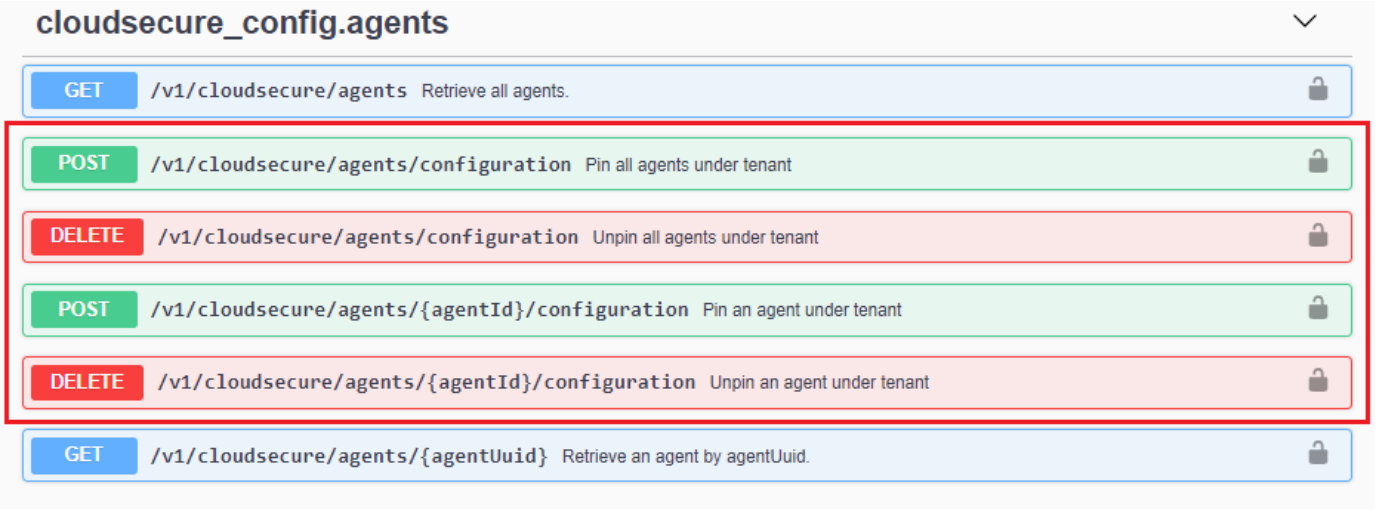
"Fijar" un agente en la versión actual

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 al Agente en su versión actual hasta que ocurra una de las siguientes situaciones:

- 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 pausa el Agente.

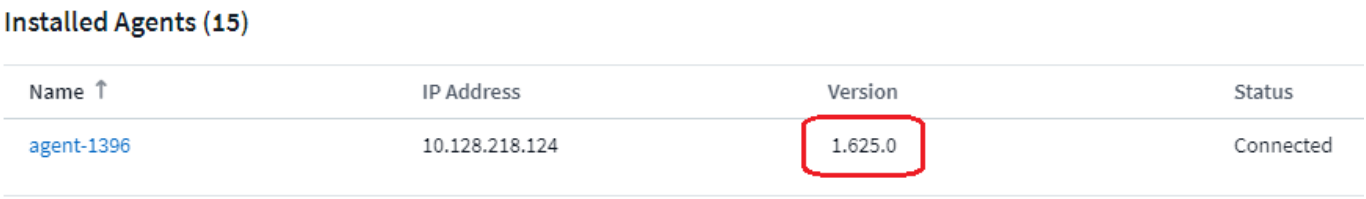
En cada uno de estos casos, el agente se actualizará en la próxima actualización de Seguridad de carga de trabajo.

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



Tenga en cuenta que la acción de pausar o reanudar puede tardar hasta cinco minutos en surtir efecto.

Puede ver las versiones actuales de su Agente en la página **Seguridad de carga de trabajo > Recopiladores**, 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 logra 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 ocurre antes de que se inicialice el registrador. El error se redirige a la salida estándar y es visible en el registro de servicio mediante el `journalctl -u cloudsecure-agent.service` dominio. Este comando se puede utilizar para solucionar el problema con más detalle.
La instalación del agente falla con el mensaje 'Esta distribución de Linux no es compatible'. Saliendo de la instalación'.	Este error aparece cuando intenta instalar el Agente en un sistema no compatible. Ver "Requisitos del agente" .
La instalación del agente falló con el error: "-bash: unzip: comando no encontrado"	Instale, descomprima y luego ejecute el comando de instalación nuevamente. Si Yum está instalado en la máquina, intente “yum install unzip” para instalar el software de descompresión. Después de eso, vuelva a copiar el comando desde la interfaz de usuario de instalación del Agente y péguelo en la CLI para ejecutar la instalación nuevamente.

Problema:	Resolución:
El agente se instaló y estaba ejecutándose. Sin embargo, el agente se detuvo de repente.	SSH a la máquina del agente. Verifique el estado del servicio del agente a través de `sudo systemctl status cloudsecure-agent.service` . 1. Compruebe si los registros muestran el mensaje “Error al iniciar el servicio de demonio de seguridad de carga de trabajo”. 2. Verifique si el usuario cssys existe en la máquina del Agente o no. Ejecute los siguientes comandos uno por uno con permiso de root y verifique si el usuario y el grupo cssys existen. `sudo id cssys` `sudo groups cssys` 3. Si no existe ninguno, es posible que una política de monitoreo centralizada haya eliminado el usuario cssys. 4. Cree un usuario y un grupo cssys manualmente ejecutando los siguientes comandos. `sudo useradd cssys` `sudo groupadd cssys` 5. Luego reinicie el servicio del agente ejecutando el siguiente comando: `sudo systemctl restart cloudsecure-agent.service` 6. Si aún no funciona, verifique 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 recopiladores, por ejemplo, Active Directory, SVM y otros recopiladores.
La interfaz de usuario muestra que el agente está en estado NO CONECTADO.	Pasos para reiniciar el Agente. 1. SSH a la máquina del agente. 2. Luego reinicie el servicio del agente ejecutando el siguiente comando: `sudo systemctl restart cloudsecure-agent.service` 3. Verifique el estado del servicio del agente a través de `sudo systemctl status cloudsecure-agent.service` . 4. El agente debe pasar al estado CONECTADO.
La máquina virtual del agente está detrás del proxy Zscaler y la instalación del agente está fallando. Debido a la inspección SSL del proxy Zscaler, los certificados de seguridad de carga de trabajo se presentan como si estuvieran firmados por Zscaler CA, por lo que el agente no confía en la comunicación.	Deshabilite 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:
Al instalar el agente, la instalación se bloquea después de descomprimirlo.	El comando “chmod 755 -Rf” está fallando. El comando falla cuando el comando de instalación del agente lo ejecuta un usuario sudo que no es root y que tiene archivos en el directorio de trabajo que pertenecen a otro usuario y no se pueden cambiar los permisos de esos archivos. Debido a la falla del comando chmod, el resto de la instalación no se ejecuta. 1. Cree un nuevo directorio llamado “cloudsecure”. 2. Vaya a ese directorio. 3. Copie y pegue el comando de instalación completo “token=…… … ./cloudsecure-agent-install.sh" y presione Enter. 4. La instalación debería poder continuar.
Si el agente aún no puede conectarse 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 como se indica.	Para adjuntar registros al estuche: 1. Ejecute el siguiente script con permiso de 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 por uno con permiso de root y comparta la salida. a. id cssys b. groups cssys c. cat /etc/os-release
El script cloudsecure-agent-symptom-collector.sh falla con el siguiente error. [root@machine tmp]# /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh Recopilación de registro de servicio Recopilación de registros de aplicaciones Recopilación de configuraciones de agente Toma de instantánea del estado del servicio Toma de instantánea de la estructura del 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”. Luego ejecute cloudsecure-agent-symptom-collector.sh nuevamente.
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 alternativa sería crear un usuario cssys y agregar su directorio de inicio de sesión manualmente usando el siguiente comando: *sudo useradd user_name -m -d HOME_DIR* -m: Crea el directorio de inicio 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 la raíz.

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 – Servicio Daemon del agente de seguridad de carga de trabajo Cargado: cargado (/usr/lib/systemd/system/cloudsecure-agent.service; habilitado; valor predeterminado del proveedor: deshabilitado) Activo: activando (reinicio automático) (Resultado: código de salida) desde el martes 2021-08-03 21:12:26 PDT; Hace 2 s Proceso: 25889 ExecStart=/bin/bash /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent (código=salido estado=126) PID principal: 25889 (código=salido, estado=126), 03 ago 21:12:26 demo systemd[1]: cloudsecure-agent.service: proceso principal salió, código=salido, estado=126/n/a 03 ago 21:12:26 demo systemd[1]: La unidad cloudsecure-agent.service entró en estado de error. 03 de agosto 21:12:26 demo systemd[1]: cloudsecure-agent.service falló.	Esto puede fallar porque el usuario *cssys* podría no tener permiso para instalar. Si /opt/netapp es un montaje NFS y el usuario *cssys* no tiene acceso a esta carpeta, la instalación fallará. *cssys* es un usuario local creado por el instalador de Workload Security que puede no tener permiso para acceder al recurso compartido montado. Puede comprobarlo intentando acceder a /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent usando el usuario *cssys*. Si devuelve “Permiso denegado”, el permiso de instalación no está presente. En lugar de una carpeta montada, instálelo en un directorio local de la máquina.
El agente se conectó inicialmente a través de un servidor proxy y el proxy se configuró durante la instalación del agente. Ahora el servidor proxy ha cambiado. ¿Cómo se puede cambiar la configuración del proxy del Agente?	Puede editar 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. Usando 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

Cuando se elimina un agente de seguridad de carga de trabajo, primero se deben eliminar todos los recopiladores de datos asociados con el agente.

Eliminar un agente

Al eliminar un agente se eliminan todos los recopiladores de datos asociados con el agente. Si planea configurar los recopiladores de datos con un agente diferente, debe crear una copia de seguridad de las configuraciones del 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 eliminen del portal de seguridad de carga de trabajo.

   Nota: Ignore este paso si todos los recolectores asociados están en estado DETENIDO.

Pasos para eliminar un Agente:

1. Inicie sesión en la máquina virtual del agente mediante SSH y ejecute el siguiente comando. Cuando se le solicite, ingrese "y" para continuar.

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

2. Haga clic en **Seguridad de la carga de trabajo > Recopiladores > Agentes**

   El sistema muestra la lista de Agentes configurados.

3. Haga clic en el menú de opciones del Agente que está eliminando.
4. Haga clic en **Eliminar**.

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

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

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

La seguridad de la carga de trabajo se puede configurar para recopilar atributos de usuario de los servidores de Active Directory.

Antes de empezar

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

Pasos para configurar un recopilador de directorios de usuarios

1. En el menú Seguridad de la carga de trabajo, haga clic en: **Recopiladores > Recopiladores del directorio de usuarios > + Recopilador del directorio de usuarios** y seleccione **Directorio activo**

   El sistema muestra la pantalla Agregar directorio de usuarios.

Configure el recopilador de directorios de usuarios ingresando los datos requeridos en las siguientes tablas:

Nombre	Descripción
Nombre	Nombre único para el 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 del directorio. El nombre del bosque permite ambos formatos siguientes: *x.y.z* ⇒ nombre de dominio directo tal como lo tiene en su SVM. [Ejemplo: hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ Nombres distinguidos relativos [Ejemplo: DC=hq,DC=companyname,DC=com] O puede especificarlo de la siguiente manera: *OU=engineering,DC=hq,DC=companyname,DC=com* [para filtrar por OU engineering específica] *CN=username,OU=engineering,DC=companyname, DC=netapp, DC=com* [para obtener solo un usuario específico con <username> de la OU <engineering>] *CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com ,O= companyname,L=Boston,S=MA,C=US* [para obtener todos los usuarios de Acrobat dentro de los usuarios de esa organización] También se admiten dominios de Active Directory de confianza.
Vincular DN	Usuario autorizado para buscar en el directorio. Por ejemplo: *nombreusuario@nombreempresa.com* o *nombreusuario@nombredominio.com* Además, se requiere permiso de Solo lectura del dominio. El usuario debe ser miembro del grupo de seguridad *Controladores de dominio de solo lectura*.
Contraseña BIND	Contraseña del servidor de directorio (es decir, contraseña para el nombre de usuario utilizado en Bind DN)
Protocolo	ldap, ldaps, ldap-start-tls
Puertos	Seleccionar puerto

Introduzca los siguientes atributos obligatorios del servidor de directorio si se han modificado los nombres de atributos predeterminados en Active Directory. La mayoría de las veces, estos nombres de atributos *no* se modifican en Active Directory, en cuyo caso puede simplemente continuar con el nombre de atributo predeterminado.

Atributos	Nombre del atributo en el servidor de directorio
Nombre para mostrar	nombre
SID	objectid
Nombre de usuario	nombreDeCuentaSAMA

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 telefónico	número de teléfono
Role	título

País	co
Estado	estado
Departamento	departamento
Foto	foto en miniatura
AdministradorDN	gerente
Grupos	miembro de

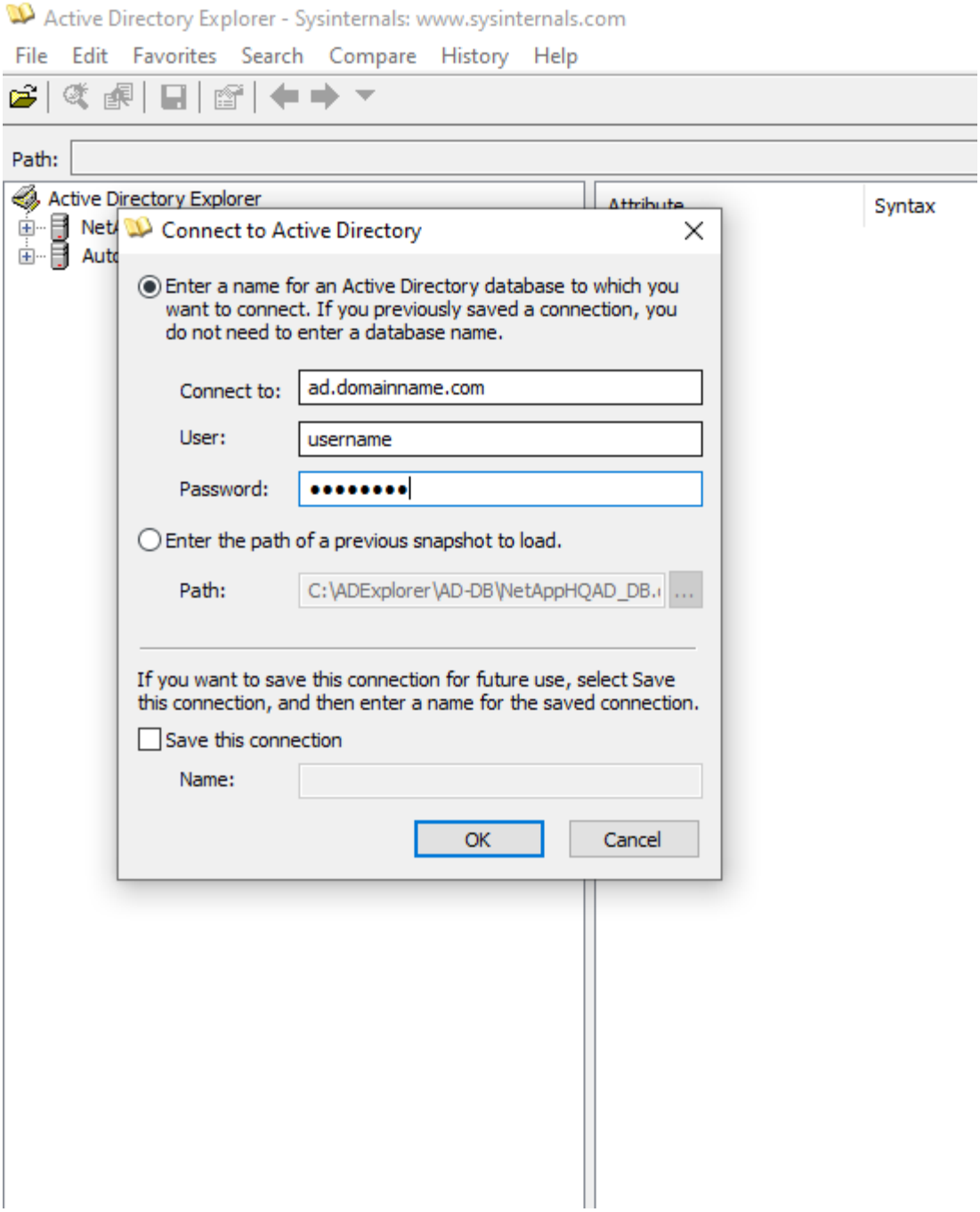
Prueba de la configuración del recopilador de directorios de usuarios

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

- Utilice el siguiente comando para validar el permiso de usuario LDAP de Workload Security:

  ```
  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 AD Explorer para navegar por una base de datos de AD, ver propiedades y atributos de objetos, ver permisos, ver el esquema de un objeto, ejecutar búsquedas sofisticadas que puede guardar y volver a ejecutar.
  - Instalar"Explorador de AD" en cualquier máquina Windows que pueda conectarse al servidor AD.
  - Conéctese al servidor AD utilizando el nombre de usuario y la contraseña del servidor de directorio AD.



Solución de problemas de configuración del recopilador de directorios de usuarios

La siguiente tabla describe problemas conocidos y resoluciones que pueden ocurrir durante la configuración del recopilador:

Problema:	Resolución:
Al agregar un conector de Directorio de usuarios se genera el estado "Error". El error dice: “Credenciales no válidas proporcionadas para el servidor LDAP”.	Nombre de usuario o contraseña proporcionados incorrectos. Edite y proporcione el nombre de usuario y la contraseña correctos.

Problema:	Resolución:
Al agregar un conector de Directorio de usuarios se genera el estado "Error". El error dice: “No se pudo obtener el objeto correspondiente a DN=DC=hq,DC=domainname,DC=com proporcionado como nombre de bosque”.	Nombre de bosque proporcionado incorrecto. Edite y proporcione el nombre del bosque correcto.
Los atributos opcionales del usuario del dominio no aparecen en la página Perfil de usuario de seguridad de carga de trabajo.	Es probable que esto se deba a una falta de coincidencia entre los nombres de los atributos opcionales agregados en CloudSecure y los nombres de los atributos reales en Active Directory. Edite y proporcione los nombres de atributos opcionales correctos.
Recopilador de datos en estado de error con "Error al recuperar usuarios LDAP". Motivo del fallo: No se puede conectar al servidor, la conexión es nula.	Reinicie el recopilador haciendo clic en el botón *Reiniciar*.
Al agregar un conector de Directorio de usuarios se genera el estado "Error".	Asegúrese de haber proporcionado valores válidos para los campos obligatorios (Servidor, nombre del bosque, DN de enlace, Contraseña de enlace). Asegúrese de que la entrada de bind-DN siempre se proporcione como 'Administrador@<nombre_del_bosque_de_dominio>' o como una cuenta de usuario con privilegios de administrador de dominio.
Al agregar un conector de Directorio de usuarios se genera el estado 'REINTENTANDO'. Muestra el error “No se puede definir el estado del recopilador, motivo por el cual el comando TCP [Connect(localhost:35012,None,List(),Some(,seconds),true)] falló debido a java.net.ConnectionException:Connection rejected”.	Se proporcionó IP o FQDN incorrectos para el servidor AD. Edite y proporcione la dirección IP o FQDN correcto.
Al agregar un conector de Directorio de usuarios se genera el estado "Error". El error dice: “Error al establecer la conexión LDAP”.	Se proporcionó IP o FQDN incorrectos para el servidor AD. Edite y proporcione la dirección IP o FQDN correcto.
Al agregar un conector de Directorio de usuarios se genera el estado "Error". El error dice: “Error al cargar la configuración. Motivo: La configuración de la fuente de datos tiene un error. Motivo específico: /connector/conf/application.conf: 70: ldap.ldap-port tiene tipo STRING en lugar de NUMBER”	Valor incorrecto para el puerto proporcionado. Intente utilizar los valores de puerto predeterminados o el número de puerto correcto para el servidor AD.
Comencé con los atributos obligatorios y funcionó. Después de agregar los opcionales, los datos de atributos opcionales no se obtienen de AD.	Es probable que esto se deba a una falta de coincidencia entre los atributos opcionales agregados en CloudSecure y los nombres de atributos reales en Active Directory. Edite y proporcione el nombre del atributo obligatorio u opcional correcto.

Problema:	Resolución:
Después de reiniciar el recopilador, ¿cuándo se producirá la sincronización de AD?	La sincronización de AD se realizará inmediatamente después de que se reinicie el recopilador. Tomará aproximadamente 15 minutos obtener los datos de usuario de aproximadamente 300 000 usuarios y se actualiza automáticamente cada 12 horas.
Los datos del usuario se sincronizan desde AD a CloudSecure. ¿Cuándo se eliminarán los datos?	Los datos del usuario se conservan durante 13 meses en caso de no actualizarse. Si se elimina el inquilino, se eliminarán los datos.
El conector del directorio de usuarios genera el estado 'Error'. "El conector está en estado de error. Nombre del servicio: usersLdap. Motivo del error: No se pudieron recuperar los usuarios LDAP. Motivo del error: 80090308: LdapErr: DSID-0C090453, comentario: Error de AcceptSecurityContext, datos 52e, v3839	Nombre de bosque proporcionado incorrecto. Vea más arriba cómo proporcionar el nombre de bosque correcto.
El número de teléfono no se completa en la página de perfil del 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 específico que obtiene la información del usuario de Active Directory. 2. Tenga en cuenta que, entre los atributos opcionales, hay un campo llamado “Número de teléfono” asignado al atributo 'número de teléfono' de Active Directory. 4. Ahora, utilice la herramienta Explorador de Active Directory como se describe anteriormente para explorar Active Directory y ver el nombre del atributo correcto. 3. Asegúrese de que en Active Directory haya un atributo llamado 'telephonenumber' que contenga el número de teléfono del usuario. 5. Digamos que en Active Directory se ha modificado a 'número de teléfono'. 6. Luego edite el recopilador del directorio de usuarios de CloudSecure. En la sección de atributos opcionales, reemplace 'número de teléfono' por 'número de teléfono'. 7. Guarde el recopilador de Active Directory, el recopilador se reiniciará y obtendrá el número de teléfono del usuario y lo mostrará en la página de perfil del usuario.
Si el certificado de cifrado (SSL) está habilitado en el servidor de Active Directory (AD), el recopilador de directorio de usuarios de Workload Security no puede conectarse al servidor de AD.	Deshabilite el cifrado del servidor AD antes de configurar un recopilador de directorio de usuarios. Una vez que se obtienen los detalles del usuario, permanecerán allí durante 13 meses. Si el servidor de AD se desconecta después de obtener los detalles del usuario, no se obtendrán los usuarios recién agregados en AD. Para recuperarlos nuevamente, el recopilador del directorio de usuarios debe estar conectado a AD.

Problema:	Resolución:
Los datos de Active Directory están presentes en CloudInsights Security. Desea eliminar toda la información del usuario de CloudInsights.	No es posible eliminar SÓLO la información de usuarios de Active Directory desde CloudInsights Security. Para eliminar el usuario es necesario eliminar el inquilino completo.

Configuración de un recopilador de servidor de directorio LDAP

Configura Workload Security para recopilar atributos de usuario de los servidores de directorio LDAP.

Antes de empezar

- Debe ser administrador de Data Infrastructure Insights o propietario de cuenta para realizar esta tarea.
- Debe tener la dirección IP del servidor que aloja el servidor de directorio LDAP.
- Se 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: **Recopiladores > Recopiladores del directorio de usuarios > + Recopilador del directorio de usuarios** y seleccione **Servidor de directorio LDAP**

   El sistema muestra la pantalla Agregar directorio de usuarios.

Configure el recopilador de directorios de usuarios ingresando los datos requeridos en las siguientes tablas:

Nombre	Descripción
Nombre	Nombre único para el 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	Base de búsqueda del servidor LDAP La base de búsqueda permite ambos formatos siguientes: *x.y.z* ⇒ nombre de dominio directo tal como lo tiene en su SVM. [Ejemplo: hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ Nombres distinguidos relativos [Ejemplo: DC=hq,DC= companyname,DC=com] O puede especificar lo siguiente: *OU=engineering,DC=hq,DC= companyname,DC=com* [para filtrar por OU engineering específica] *CN=username,OU=engineering,DC=companyname, DC=netapp, DC=com* [para obtener solo el usuario específico con <username> de la OU <engineering>] *CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com ,O= companyname,L=Boston,S=MA,C=US* [para obtener todos los usuarios de Acrobat dentro de los usuarios de esa organización]
Vincular DN	Usuario autorizado para buscar en el directorio. Por ejemplo: uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=companyname,dc=com uid=john,cn=users,cn=accounts,dc=dorp,dc=company,dc=com para un usuario john@dorp.company.com. dorp.company.com
--cuentas	--usuarios
--John	--anna
Contraseña BIND	Contraseña del servidor de directorio (es decir, contraseña para el nombre de usuario utilizado en Bind DN)
Protocolo	ldap, ldaps, ldap-start-tls
Puertos	Seleccionar puerto

Introduzca los siguientes atributos obligatorios del servidor de directorio si se han modificado los nombres de atributos predeterminados en el servidor de directorio LDAP. La mayoría de las veces, estos nombres de atributos *no* se modifican en el servidor de directorio LDAP, en cuyo caso puede simplemente continuar con el nombre de atributo predeterminado.

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

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 telefónico	número de teléfono
Role	título
País	co
Estado	estado
Departamento	número de departamento
Foto	foto
AdministradorDN	gerente
Grupos	miembro de

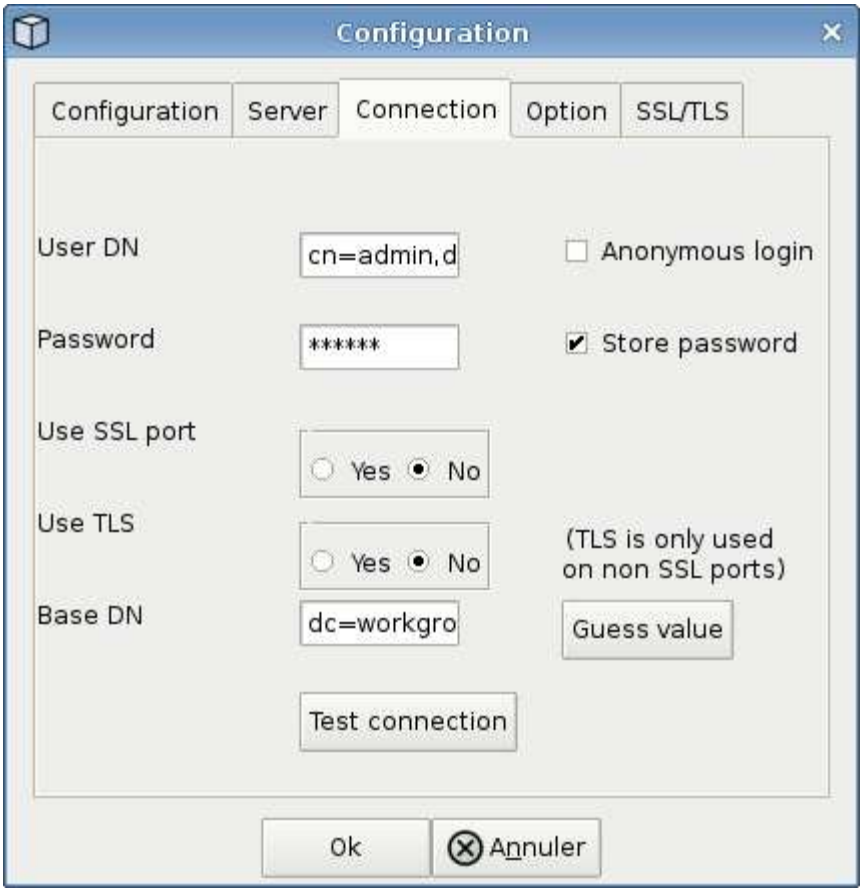
Prueba de la configuración del recopilador de directorios de usuarios

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

- Utilice el siguiente comando para validar el permiso de usuario LDAP de Workload Security:

```
 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 LDAP Explorer para navegar por una base de datos LDAP, ver
propiedades y atributos de objetos, ver permisos, ver el esquema de un
objeto, ejecutar búsquedas sofisticadas que puede guardar y volver a
ejecutar.
```

  - Instalar el explorador LDAP(http://ldaptool.sourceforge.net/) o el Explorador LDAP de Java(http://jxplorer.org/) en cualquier máquina Windows que pueda conectarse al servidor LDAP.
  - Conéctese al servidor LDAP utilizando el nombre de usuario y la contraseña del servidor de directorio LDAP.



Solución de problemas de configuración del recopilador de directorios LDAP

La siguiente tabla describe problemas conocidos y resoluciones que pueden ocurrir durante la configuración del recopilador:

Problema:	Resolución:
Al agregar un conector de directorio LDAP se genera el estado "Error". El error dice: “Credenciales no válidas proporcionadas para el servidor LDAP”.	Se proporcionó un DN de enlace, una contraseña de enlace o una base de búsqueda incorrectos. Editar y proporcionar la información correcta.
Al agregar un conector de directorio LDAP se genera el estado "Error". El error dice: “No se pudo obtener el objeto correspondiente a DN=DC=hq,DC=domainname,DC=com proporcionado como nombre de bosque”.	Base de búsqueda proporcionada incorrecta. Edite y proporcione el nombre del bosque correcto.
Los atributos opcionales del usuario del dominio no aparecen en la página Perfil de usuario de seguridad de carga de trabajo.	Es probable que esto se deba a una falta de coincidencia entre los nombres de los atributos opcionales agregados en CloudSecure y los nombres de los atributos reales en Active Directory. Los campos distinguen entre mayúsculas y minúsculas. Edite y proporcione los nombres de atributos opcionales correctos.
Recopilador de datos en estado de error con "Error al recuperar usuarios LDAP". Motivo del fallo: No se puede conectar al servidor, la conexión es nula.	Reinicie el recopilador haciendo clic en el botón *Reiniciar*.

Problema:	Resolución:
Al agregar un conector de directorio LDAP se genera el estado "Error".	Asegúrese de haber proporcionado valores válidos para los campos obligatorios (Servidor, nombre del bosque, DN de enlace, Contraseña de enlace). Asegúrese de que la entrada bind-DN siempre se proporcione como uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=companyname,dc=com.
Al agregar un conector de directorio LDAP se genera el estado 'REINTENTANDO'. Muestra el error "No se pudo determinar el estado del recopilador, por lo que se vuelve a intentar".	Asegúrese de que se proporcione la IP del servidor y la base de búsqueda correctas ////
Al agregar el directorio LDAP, se muestra el siguiente error: “No se pudo determinar el estado del recopilador en 2 reintentos, intente reiniciar el recopilador nuevamente (Código de error: AGENT008)”	Asegúrese de que se proporcione la IP del servidor y la base de búsqueda correctas
Al agregar un conector de directorio LDAP se genera el estado 'REINTENTANDO'. Muestra el error “No se puede definir el estado del recopilador, motivo por el cual el comando TCP [Connect(localhost:35012,None,List(),Some(,seconds),true)] falló debido a java.net.ConnectionException:Connection rejected”.	Se proporcionó IP o FQDN incorrectos para el servidor AD. Edite y proporcione la dirección IP o FQDN correcto. ////
Al agregar un conector de directorio LDAP se genera el estado "Error". El error dice: “Error al establecer la conexión LDAP”.	Se proporcionó IP o FQDN incorrectos para el servidor LDAP. Edite y proporcione la dirección IP o FQDN correcto. O valor incorrecto para el puerto proporcionado. Intente utilizar los valores de puerto predeterminados o el número de puerto correcto para el servidor LDAP.
Al agregar un conector de directorio LDAP se genera el estado "Error". El error dice: “Error al cargar la configuración. Motivo: La configuración de la fuente de datos tiene un error. Motivo específico: /connector/conf/application.conf: 70: ldap.ldap-port tiene tipo STRING en lugar de NUMBER”	Valor incorrecto para el puerto proporcionado. Intente utilizar los valores de puerto predeterminados o el número de puerto correcto para el servidor AD.
Comencé con los atributos obligatorios y funcionó. Después de agregar los opcionales, los datos de atributos opcionales no se obtienen de AD.	Es probable que esto se deba a una falta de coincidencia entre los atributos opcionales agregados en CloudSecure y los nombres de atributos reales en Active Directory. Edite y proporcione el nombre del atributo obligatorio u opcional correcto.
Después de reiniciar el recopilador, ¿cuándo se producirá la sincronización LDAP?	La sincronización LDAP se realizará inmediatamente después de que se reinicie el recopilador. Tomará aproximadamente 15 minutos obtener los datos de usuario de aproximadamente 300 000 usuarios y se actualiza automáticamente cada 12 horas.

Problema:	Resolución:
Los datos del usuario se sincronizan desde LDAP a CloudSecure. ¿Cuándo se eliminarán los datos?	Los datos del usuario se conservan durante 13 meses en caso de no actualizarse. Si se elimina el inquilino, se eliminarán los datos.
El conector de directorio LDAP genera el estado 'Error'. "El conector está en estado de error. Nombre del servicio: usersLdap. Motivo del error: No se pudieron recuperar los usuarios LDAP. Motivo del error: 80090308: LdapErr: DSID-0C090453, comentario: Error de AcceptSecurityContext, datos 52e, v3839	Nombre de bosque proporcionado incorrecto. Vea más arriba cómo proporcionar el nombre de bosque correcto.
El número de teléfono no se completa en la página de perfil del 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 específico que obtiene la información del usuario de Active Directory. 2. Tenga en cuenta que, entre los atributos opcionales, hay un campo llamado “Número de teléfono” asignado al atributo 'número de teléfono' de Active Directory. 4. Ahora, utilice la herramienta Active Directory Explorer como se describe anteriormente para explorar el servidor de directorio LDAP y ver el nombre del atributo correcto. 3. Asegúrese de que en el directorio LDAP haya un atributo llamado 'telephonenumber' que contenga el número de teléfono del usuario. 5. Digamos que en el directorio LDAP se ha modificado a "número de teléfono". 6. Luego edite el recopilador del directorio de usuarios de CloudSecure. En la sección de atributos opcionales, reemplace 'número de teléfono' por 'número de teléfono'. 7. Guarde el recopilador de Active Directory, el recopilador se reiniciará y obtendrá el número de teléfono del usuario y lo mostrará en la página de perfil del usuario.
Si el certificado de cifrado (SSL) está habilitado en el servidor de Active Directory (AD), el recopilador de directorio de usuarios de Workload Security no puede conectarse al servidor de AD.	Deshabilite el cifrado del servidor AD antes de configurar un recopilador de directorio de usuarios. Una vez que se obtienen los detalles del usuario, permanecerán allí durante 13 meses. Si el servidor de AD se desconecta después de obtener los detalles del usuario, no se obtendrán los usuarios recién agregados en AD. Para recuperar el directorio de usuarios, el recopilador debe estar conectado a AD.

Configuración del recopilador de datos ONTAP SVM

El recopilador de datos ONTAP SVM permite que Workload Security monitoree las actividades de acceso a archivos y usuarios en las máquinas virtuales de almacenamiento (SVM) de NetApp ONTAP . Esta guía lo guiará a través de la configuración y administración del recopilador de datos SVM para proporcionar un monitoreo de seguridad integral de su entorno ONTAP .

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 anteriores.
  - Versiones de NFS hasta NFS 4.1 inclusive (tenga en cuenta que NFS 4.1 es compatible con ONTAP 9.15 o posterior).
  - Flexgroup es compatible con ONTAP 9.4 y versiones posteriores
  - FlexCache es compatible con NFS con ONTAP 9.7 y versiones posteriores.
  - FlexCache es compatible con SMB con ONTAP 9.14.1 y versiones posteriores.
  - ONTAP Select es compatible
- Sólo se admiten SVM de tipo de datos. No se admiten SVM con volúmenes infinitos.
- SVM tiene varios subtipos. De estos, solo se admiten *default*, *sync_source* y *sync_destination*.
- Un agente"debe estar configurado" antes de poder configurar los recopiladores de datos.
- Asegúrese de tener un Conector de directorio de usuarios configurado correctamente; de lo contrario, los eventos mostrarán nombres de usuario codificados y no el nombre real del usuario (tal como está almacenado en Active Directory) en la página “Análisis forense de actividad”.
- ONTAP Persistent Store es compatible desde la versión 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.
- Para conocer las mejores prácticas y recomendaciones completas sobre la configuración de Workload Security FPolicy, consulte"Artículo de KB sobre las mejores prácticas de FPolicy" .
- Debe agregar un SVM utilizando uno de los dos métodos siguientes:
  - Mediante el uso de la IP del clúster, el nombre de SVM y el nombre de usuario y la contraseña de administración del clúster. ***Este es el método recomendado.***
    - El nombre de SVM debe ser exactamente como se muestra en ONTAP y distingue entre mayúsculas y minúsculas.
  - Mediante la administración de SVM Vserver IP, nombre de usuario y contraseña
  - Si no puede o no desea utilizar el nombre de usuario y la contraseña de administración del clúster de administrador/SVM completos, puede crear un usuario personalizado con privilegios menores, como se menciona en“Una nota sobre los permisos” sección a continuación. Este usuario personalizado se puede crear para acceso a SVM o a clúster.
    - También puede utilizar un usuario de AD con un rol que tenga al menos los permisos de csrole como se menciona en la sección “Una nota sobre permisos” a continuación. Consulte también la"Documentación de ONTAP" .
- Asegúrese de que las aplicaciones correctas estén configuradas para la SVM ejecutando el siguiente comando:

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

Ejemplo de salida:

```
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 un servidor CIFS configurado: clustershell:> `vserver cifs show`

  El sistema devuelve el nombre del servidor V, el nombre del servidor CIFS y campos adicionales.

- Establezca una contraseña para el usuario vsadmin de SVM. Si utiliza un usuario personalizado o un usuario administrador del clúster, omita este paso. clustershell:> `security login password -username vsadmin -vserver svmname`
- Desbloquee el usuario vsadmin de SVM para acceso externo. Si utiliza un usuario personalizado o un usuario administrador del clúster, omita este paso. clustershell:> `security login unlock -username vsadmin -vserver svmname`
- Asegúrese de que la política de firewall del LIF de datos esté configurada en 'mgmt' (no en 'data'). Omita este paso si utiliza un lif de administración dedicado para agregar el 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 que utiliza el recopilador de datos de Data ONTAP .

  Ver"Requisitos del agente" para obtener información de configuración. Esto se aplica a los agentes locales y a los agentes instalados en la nube.

- Cuando se instala un agente en una instancia de AWS EC2 para monitorear una SVM de Cloud ONTAP , el agente y el almacenamiento deben estar en la misma VPC. Si están en VPC separadas, debe haber una ruta válida entre las VPC.

Prueba de conectividad para recopiladores de datos

La función de conectividad de prueba (introducida en marzo de 2025) tiene como objetivo ayudar a los usuarios finales a identificar las causas específicas de las fallas al configurar recopiladores de datos en Data Infrastructure Insights (DII) Workload Security. Esto permite a los usuarios autocorregir problemas relacionados con la comunicación de red o roles faltantes.

Esta función ayudará a los usuarios a determinar si todas las comprobaciones relacionadas con la red están en su lugar antes de configurar un recopilador de datos. Además, informará a los usuarios sobre las funciones a las que pueden acceder según la versión de ONTAP , los roles y los permisos asignados a ellos en ONTAP.

La conectividad de prueba no es compatible con los recopiladores del Directorio de usuarios

Requisitos previos para las pruebas de conexión

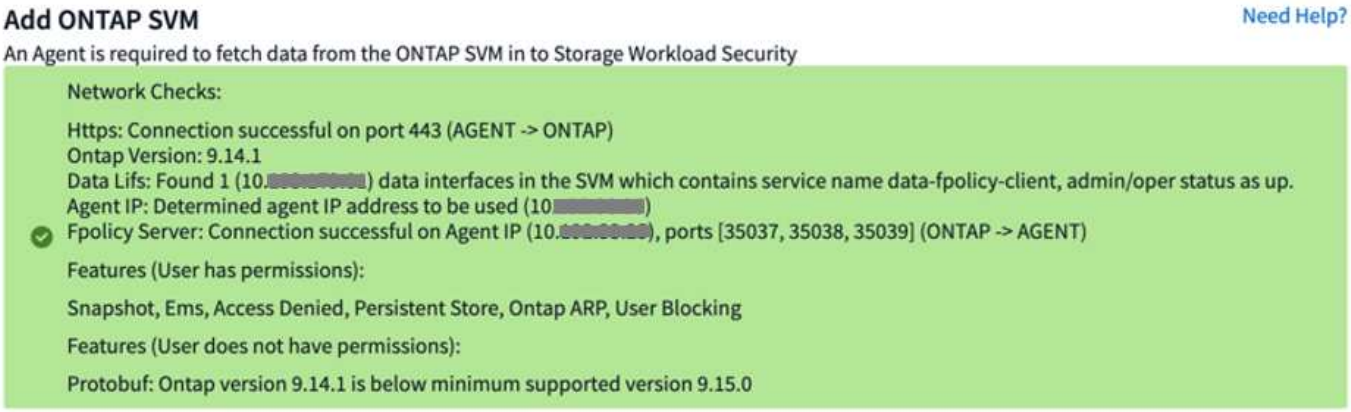
- Se necesitan credenciales de nivel de clúster para que esta función funcione completamente.
- La verificación de acceso a funciones no es compatible con el modo SVM.

- Si está utilizando credenciales de administración del clúster, no se necesitan permisos nuevos.
- Si está utilizando un usuario personalizado (por ejemplo, *csuser*), proporcione los permisos obligatorios y los permisos específicos para las funciones que desea utilizar.

Asegúrese de revisar elPermisos sección a continuación también.

Pruebe la conexión

El usuario puede ir a la página para agregar o editar recopilador, ingresar los detalles de nivel de clúster (en modo de clúster) o los detalles de nivel de SVM (en modo SVM) y hacer clic en el botón **Probar conexión**. Luego, Workload Security procesará la solicitud y mostrará un mensaje de éxito o fracaso apropiado.



Cosas a tener en cuenta para ONTAP Multi Admin Verify (MAV)

Es posible que algunas funciones, como la creación y eliminación de instantáneas o el bloqueo de usuarios (SMB), no funcionen según los comandos MAV añadidos en tu versión de ONTAP.

Sigue los pasos a continuación para añadir exclusiones a tus comandos MAV que permiten a Workload Security crear o eliminar instantáneas y bloquear usuarios.

Comandos para permitir crear y eliminar instantáneas:

```
multi-admin-verify rule modify -operation "volume snapshot create" -query
"-snapshot !*cloudsecure_*"
multi-admin-verify rule modify -operation "volume snapshot delete" -query
"-snapshot !*cloudsecure_*"
```

Comando para permitir el bloqueo de usuarios:

```
multi-admin-verify rule delete -operation set
```

Requisitos previos para el bloqueo del acceso de usuarios

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

Se necesitan credenciales de nivel de clúster para que esta característica funcione.

Si está utilizando credenciales de administración del clúster, no se necesitan permisos nuevos.

Si está utilizando un usuario personalizado (por ejemplo, *csuser*) con permisos otorgados al usuario, siga los pasos en"Bloqueo de acceso de usuarios" para dar permisos a Workload Security para bloquear al usuario.

Una nota sobre los permisos

Permisos al agregar mediante IP de administración de clúster:

Si no puede usar el usuario administrador de administración de clúster para permitir que Workload Security acceda al recopilador de datos de ONTAP SVM, puede crear un nuevo usuario llamado “csuser” con los roles que se muestran en los comandos a continuación. Utilice el nombre de usuario “csuser” y la contraseña “csuser” al configurar el recopilador de datos de seguridad de carga de trabajo para utilizar la IP de administración de clúster.

Nota: Puede crear un rol único para utilizarlo en todos los permisos de funciones de un usuario personalizado. Si hay un usuario existente, primero elimine el usuario y el rol existentes usando estos comandos:

```
security login delete -user-or-group-name csuser -application *
security login role delete -role csrole -cmddirname *
security login rest-role delete -role csrestrole -api *
security login rest-role delete -role arwrole -api *
```

Para crear un nuevo usuario, inicie sesión en ONTAP con el nombre de usuario y la 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 role create -role csrole -cmddirname "cluster application-
record" -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 a través de Vserver Management IP:

Si no puede usar el usuario administrador de administración de clúster para permitir que Workload Security acceda al recopilador de datos de ONTAP SVM, puede crear un nuevo usuario llamado “csuser” con los roles que se muestran en los comandos a continuación. Utilice el nombre de usuario “csuser” y la contraseña “csuser” al configurar el recopilador de datos de seguridad de carga de trabajo para utilizar la IP de administración de Vserver.

Nota: Puede crear un rol único para utilizarlo en todos los permisos de funciones de un usuario personalizado. Si hay un usuario existente, primero elimine el usuario y el rol existentes usando estos comandos:

```
security login delete -user-or-group-name csuser -application * -vserver
<vservername>
security login role delete -role csrole -cmddirname * -vserver
<vservername>
security login rest-role delete -role csrestrole -api * -vserver
<vservername>
```

Para crear un nuevo usuario, inicie sesión en ONTAP con el nombre de usuario y la contraseña del administrador de administración del clúster y ejecute los siguientes comandos en el servidor ONTAP . Para facilitar su uso, copie estos comandos en un editor de texto y reemplace <vservername> con el nombre de su Vserver antes de ejecutar 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 *Configuración avanzada* del recopilador. El modo Protobuf es compatible con ONTAP versión 9.15 y posteriores.

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

Se requieren permisos específicos para protobuf (es posible que algunos o todos ellos ya existan):

Modo clúster:

```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
Modo vserver:
```

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

Permisos para ONTAP Autonomous Ransomware Protection y acceso denegado a ONTAP

Si está utilizando credenciales de administración del clúster, no se necesitan permisos nuevos.

Si está utilizando un usuario personalizado (por ejemplo, *csuser*) con permisos otorgados al usuario, siga los pasos a continuación para otorgar permisos a Workload Security para recopilar información relacionada con ARP de ONTAP.

Para obtener más información, lea sobre"Integración con ONTAP Acceso denegado"

y"Integración con ONTAP Autonomous Ransomware Protection"

Configurar el recopilador de datos

Pasos para la configuración

1. Inicie sesión como administrador o propietario de cuenta en su entorno de Data Infrastructure Insights .
2. Haga clic en **Seguridad de la carga de trabajo > Recopiladores > +Recopiladores de datos**

   El sistema muestra los recopiladores de datos disponibles.
3. Coloque el cursor sobre el mosaico * NetApp SVM y haga clic en **+Monitor**.

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

Campo	Descripción
Nombre	Nombre único para el recopilador de datos
Agente	Seleccione un agente configurado de la lista.
Conectarse a través de IP de administración para:	Seleccione la IP del clúster o la IP de administración de SVM
Dirección IP de administración de clúster/SVM	La dirección IP del clúster o de la SVM, según su selección anterior.
Nombre de SVM	El nombre del SVM (este campo es obligatorio cuando se conecta a través de la IP del clúster)
Nombre de usuario	Nombre de usuario para acceder al SVM/Cluster Al agregar mediante IP del Cluster las opciones son: 1. Administrador de clúster 2. 'csuser' 3. Usuario de AD que tiene un rol similar al de csuser. Al agregar a través de IP SVM las opciones son: 4. vsadmin 5. 'csuser' 6. Nombre de usuario AD que tiene una función similar a csuser.
Password	Contraseña para el nombre de usuario anterior
Filtrar acciones/volúmenes	Elija si desea incluir o excluir acciones/volúmenes de la recopilación de eventos
Ingrese los nombres completos de los recursos compartidos que desea excluir o incluir	Lista separada por comas de acciones para excluir o incluir (según corresponda) de la recopilación de eventos

Ingrese los nombres completos de los volúmenes que desea excluir o incluir	Lista separada por comas de volúmenes para excluir o incluir (según corresponda) de la recopilación de eventos
Supervisar el acceso a carpetas	Cuando está marcada, habilita eventos para monitorear el acceso a la carpeta. Tenga en cuenta que la creación, el cambio de nombre y la eliminación de carpetas se supervisarán incluso sin esta opción seleccionada. Habilitar esta opción aumentará la cantidad de eventos monitoreados.
Establecer el tamaño del búfer de envío de ONTAP	Establece el tamaño del búfer de envío Fpolicy de ONTAP . Si se utiliza una versión de ONTAP anterior a 9.8p7 y se detectan problemas de rendimiento, se puede modificar el tamaño del búfer de envío de ONTAP para obtener un mejor rendimiento de ONTAP . Comuníquese con el soporte de NetApp si no ve esta opción y desea explorarla.

Después de terminar

- En la página Recopiladores de datos instalados, utilice el menú de opciones 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 al SVM de origen y otro al SVM de destino.
2. Los recopiladores de datos deben estar conectados mediante *Cluster IP*.
3. En cualquier momento, el recopilador de datos del SVM "en ejecución" actual se mostrará como *En ejecución*. El recopilador de datos del SVM "detenido" actual se mostrará como *Detenido*.
4. Siempre que se produzca un cambio, el estado del recopilador de datos cambiará de *En ejecución* a *Detenido* y viceversa.
5. El recopilador de datos tardará hasta dos minutos en pasar del estado *Detenido* al estado *En ejecución*.

Política de servicio

Si se utiliza la política de servicio con ONTAP **versión 9.9.1 o más reciente**, para conectarse al recopilador de origen 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 versiones de ONTAP anteriores a 9.9.1, no es necesario configurar *data-fpolicy-client*.

Recopilador de datos de reproducción y pausa

Si el recopilador de datos está en estado *En ejecución*, puede pausar la recopilación. Abra el menú de "tres puntos" del colector y seleccione PAUSA. Mientras el recopilador está en pausa, no se recopilan datos de ONTAP y no se envían datos del recopilador a ONTAP. Esto significa que no fluirán eventos de Fpolicy desde ONTAP al recopilador de datos, y desde allí a Data Infrastructure Insights.

Tenga en cuenta que si se crean nuevos volúmenes, etc. en ONTAP mientras el recopilador está en pausa, Workload Security no recopilará los datos y esos volúmenes, etc. no se reflejarán en los paneles ni en las tablas.

> No se puede pausar un recopilador si tiene usuarios restringidos. Restaure el acceso del usuario antes de pausar el recopilador.

Tenga en cuenta lo siguiente:

- La purga de instantáneas no se realizará según la configuración configurada en un recopilador en pausa.
- Los eventos EMS (como ONTAP ARP) no se procesarán en un recopilador en pausa. Esto significa que si ONTAP identifica un ataque de manipulación de archivos, Data Infrastructure Insights Workload Security no podrá adquirir ese evento.
- NO se enviarán correos electrónicos de notificaciones de salud para un recolector en pausa.
- No se admitirán acciones manuales o automáticas (como instantáneas o bloqueo de usuarios) en un recopilador en pausa.
- En las actualizaciones del agente o del recopilador, en los reinicios de la máquina virtual del agente o en el reinicio del servicio del agente, un recopilador en pausa permanecerá en estado *Pausado*.
- Si el recopilador de datos está en estado *Error*, no se puede cambiar al estado *Pausado*. El botón Pausa se habilitará solo si el estado del recopilador es *En ejecución*.
- Si el agente está desconectado, el recopilador no se puede cambiar al estado *Pausado*. El recolector pasará al estado *Detenido* y el botón Pausa se desactivará.

Almacén persistente

El almacenamiento persistente es compatible con ONTAP 9.14.1 y versiones posteriores. Tenga en cuenta que las instrucciones del nombre del volumen varían de ONTAP 9.14 a 9.15.

El almacenamiento persistente se puede habilitar 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 habilitar el almacenamiento persistente.

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

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

Modo clúster:

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "job show" -access
readonly
```

Modo vserver:

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"job show" -access readonly
```

Migrar recolectores

Puede migrar fácilmente un recopilador de seguridad de carga de trabajo de un agente a otro, lo que permite un equilibrio de carga eficiente de los recopiladores entre agentes.

Prerrequisitos

- El agente de origen debe estar en estado *conectado*.
- El recopilador que se va a migrar debe estar en estado *en ejecución*.

Nota:

- Migrate es compatible con recopiladores de directorios de datos y de usuarios.
- No se admite la migración de un recopilador para inquilinos administrados manualmente.

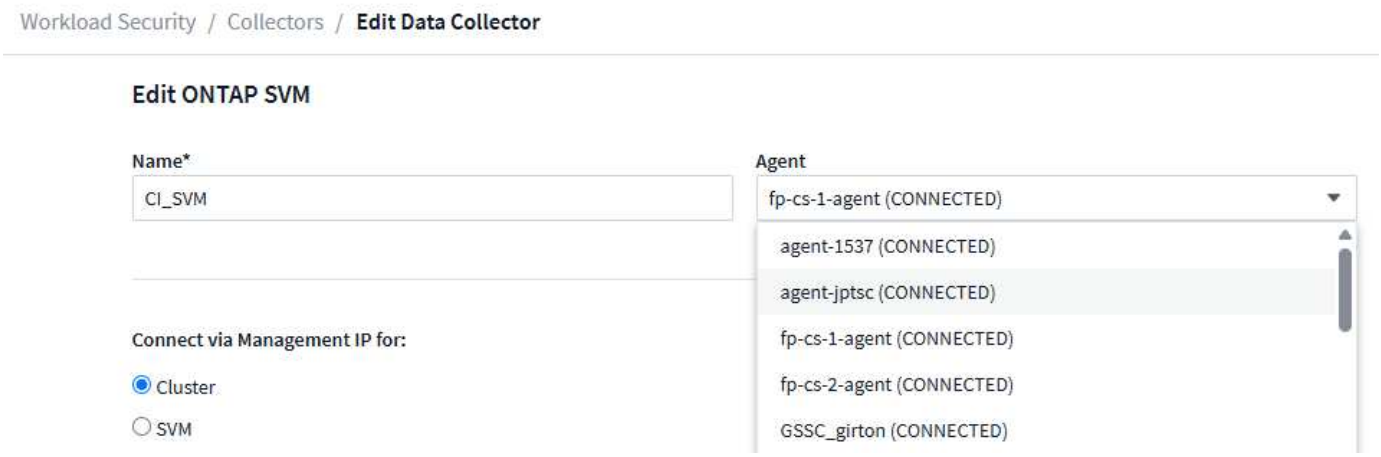
Migrar colector

Para migrar un recopilador, siga estos pasos:

1. Vaya a la página "Editar recopilador".
2. Seleccione un agente de destino del menú desplegable de agentes.
3. Haga clic en el botón "Guardar recopilador".

Seguridad de carga de trabajo procesará la solicitud. Tras una migración exitosa, el usuario será redirigido a la página de la lista de recopiladores. En caso de error, se mostrará un mensaje apropiado en la página de edición.

Nota: Cualquier cambio de configuración realizado previamente en la página "Editar recopilador" permanecerá aplicado cuando el recopilador se migre exitosamente al agente de destino.



Solución de problemas

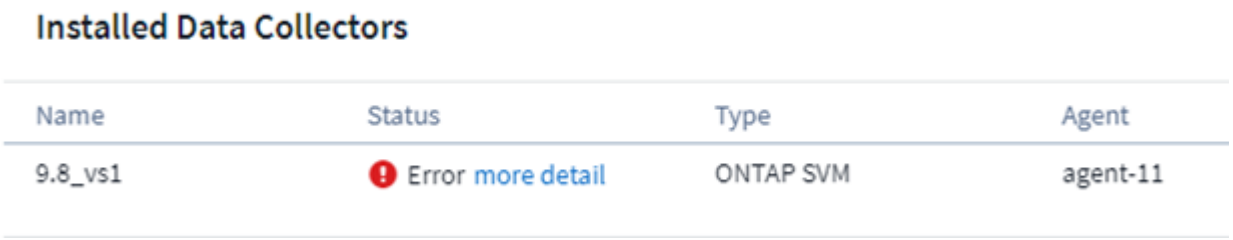
Ver el"Solución de problemas del recopilador SVM" Página para obtener sugerencias para la solución de problemas.

Solución de problemas del recopilador de datos ONTAP SVM

Workload Security utiliza recopiladores de datos para recopilar datos de acceso a archivos y usuarios de los dispositivos. Aquí puede encontrar sugerencias para solucionar problemas con este recopilador.

Ver el"Configuración del recopilador SVM" página para obtener instrucciones sobre cómo configurar este recopilador.

En caso de error, puede hacer clic en *más detalles* en la columna *Estado* de la página Recopiladores de datos instalados para obtener detalles sobre el error.



A continuación se describen los problemas conocidos y sus soluciones.

Problema: El recopilador de datos se ejecuta durante un tiempo y se detiene después de un tiempo aleatorio, y falla con: "Mensaje de error: el conector está en estado de error". Nombre del servicio: auditoría. Motivo del fallo: Servidor fpolicy externo sobrecargado. **Pruebe esto:** La tasa de eventos de ONTAP fue mucho más alta que lo que el cuadro del Agente puede manejar. Por lo tanto, la conexión se terminó.

Verifique el tráfico máximo en CloudSecure cuando ocurrió la desconexión. Puedes comprobarlo en la página **CloudSecure > Análisis forense de actividad > Toda la actividad**.

Si el tráfico agregado máximo es más alto que lo que el Agent Box puede manejar, consulte la página del Comprobador de tasa de eventos para obtener información sobre cómo dimensionar la implementación del recopilador en un Agent Box.

Si el Agente se instaló en el cuadro del Agente antes del 4 de marzo de 2021, ejecute los siguientes comandos en el cuadro del Agente:

```
echo 'net.core.rmem_max=8388608' >> /etc/sysctl.conf
echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf
sysctl -p
```

Reinicie el recopilador desde la interfaz de usuario después de cambiar el tamaño.

{vacío}

Problema: El recopilador informa el mensaje de error: “No se encontró ninguna dirección IP local en el conector que pueda acceder a las interfaces de datos del SVM”. **Pruebe esto:** Lo más probable es que esto se deba a un problema de red en el lado de ONTAP . Por favor siga estos pasos:

1. Asegúrese de que no haya firewalls en el servidor de datos SVM ni en el servidor de administración SVM que bloqueen la conexión desde el SVM.
2. Al agregar una SVM a través de una IP de administración de clúster, asegúrese de que la vida de los datos y la vida de administración de la SVM se puedan hacer ping desde la VM del agente. En caso de problemas, verifique la puerta de enlace, la máscara de red y las rutas para el LIF.

   También puede intentar iniciar sesión en el clúster a través de ssh usando la IP de administración del clúster y hacer ping a la IP del agente. Asegúrese de que la IP del agente se pueda ping:

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
   Name> -show-detail
   ```

   Si no se puede hacer ping, asegúrese de que la configuración de red en ONTAP sea correcta, para que se pueda hacer ping a la máquina del Agente.

3. Si ha intentado conectarse a través de la IP del clúster y no funciona, intente conectarse directamente a través de la IP de SVM. Consulte más arriba los pasos para conectarse a través de IP SVM.
4. Al agregar el recopilador a través de la IP de SVM y las credenciales de vsadmin, verifique si SVM Lif tiene habilitada la función Datos más administración. En este caso, hacer ping al SVM Lif funcionará, sin embargo, SSH al SVM Lif no funcionará. En caso afirmativo, cree un Lif de solo administración de SVM e intente conectarse a través de este Lif de solo administración de SVM.
5. Si aún no funciona, cree un nuevo SVM Lif e intente conectarse a través de ese Lif. Asegúrese de que la máscara de subred esté configurada correctamente.
6. Depuración avanzada:
   a. Iniciar un seguimiento de paquetes en ONTAP.
   b. Intente conectar un recopilador de datos al SVM desde la interfaz de usuario de CloudSecure.
   c. Espere hasta que aparezca el error. Detener el seguimiento de paquetes en ONTAP.

d. Abra el seguimiento de paquetes desde ONTAP. Está disponible en esta ubicación.

```
 https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
.. Asegúrese de que haya un SYN de ONTAP al cuadro del Agente.
.. Si no hay SYN de ONTAP , entonces es un problema con el firewall
en ONTAP.
.. Abra el firewall en ONTAP, para que ONTAP pueda conectarse al
cuadro del agente.
```

7. Si aún no funciona, consulte al equipo de redes para asegurarse de que ningún firewall externo esté bloqueando la conexión de ONTAP al cuadro del Agente.
8. Si nada de lo anterior resuelve el problema, abra un caso con"Soporte de Netapp" Para obtener más ayuda.

{vacío}

Problema: Mensaje: "No se pudo determinar el tipo de ONTAP para [nombre de host: <Dirección IP>. Motivo: Error de conexión al sistema de almacenamiento <Dirección IP>: El host no es accesible (Host inaccesible)" **Pruebe esto:**

1. Verifique que se haya proporcionado la dirección IP de administración de SVM o la IP de administración de clúster correcta.
2. Conéctese por SSH al SVM o al clúster al que desea conectarse. Una vez conectado, asegúrese de que el nombre de SVM o del clúster sea correcto.

{vacío}

Problema: Mensaje de error: "El conector está en estado de error. Servicio.nombre:auditoría. Motivo del fallo: "Servidor fpolicy externo finalizado". **Prueba esto:**

1. Lo más probable es que un firewall esté bloqueando los puertos necesarios en la máquina del agente. Verifique que el rango de puertos 35000-55000/tcp esté abierto para que la máquina agente se conecte desde la SVM. Asegúrese también de que no haya ningún firewall habilitado desde el lado de ONTAP que bloquee la comunicación con la máquina del agente.
2. Escriba el siguiente comando en el cuadro Agente y asegúrese de que el rango de puertos esté abierto.

   ```
   sudo iptables-save | grep 3500*
   ```

   El resultado de muestra debería verse así:

```
 -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate
NEW -j ACCEPT
. Inicie sesión en SVM, ingrese los siguientes comandos y verifique que
no haya ningún firewall configurado para bloquear la comunicación con
ONTAP.
```

```
system services firewall show
system services firewall policy show
```

"Comprobar los comandos del firewall"en el lado de ONTAP .

3. Conéctese mediante SSH al SVM/Cluster que desea monitorear. Haga ping al cuadro del agente desde la base de datos SVM (con soporte para protocolos CIFS y NFS) y asegúrese de que el ping funcione:

```
network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
Name> -show-detail
```

Si no se puede hacer ping, asegúrese de que la configuración de red en ONTAP sea correcta, para que se pueda hacer ping a la máquina del Agente.

4. Si se agrega un solo SVM dos veces a un inquilino a través de 2 recopiladores de datos, se mostrará este error. Eliminar uno de los recopiladores de datos a través de la interfaz de usuario. Luego reinicie el otro recopilador de datos a través de la interfaz de usuario. Luego, el recopilador de datos mostrará el estado “EN EJECUCIÓN” y comenzará a recibir eventos de SVM.

   Básicamente, en un inquilino, 1 SVM debe agregarse solo una vez, a través de 1 recopilador de datos. 1 SVM no debe agregarse dos veces a través de 2 recopiladores de datos.

5. En los casos en que se agregó el mismo SVM en dos entornos de seguridad de carga de trabajo diferentes (inquilinos), el último siempre tendrá éxito. El segundo recopilador configurará fpolicy con su propia dirección IP y expulsará al primero. Por lo tanto, el recopilador del primero dejará de recibir eventos y su servicio de "auditoría" entrará en estado de error. Para evitar esto, configure cada SVM en un solo entorno.
6. Este error también puede ocurrir si las políticas de servicio no están configuradas correctamente. Con ONTAP 9.8 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. Además, el servicio data-fpolicy-client debe estar asociado con los datos lif para el SVM monitoreado.

{vacío}

Problema: No se ven eventos en la página de actividad. **Prueba esto:**

1. Compruebe si el recopilador ONTAP está en estado “EN EJECUCIÓN”. Si es así, asegúrese de que se generen algunos eventos CIF en las máquinas virtuales del cliente CIF abriendo algunos archivos.
2. Si no se ven actividades, inicie sesión en SVM e ingrese el siguiente comando.

```
<SVM>event log show -source fpolicy
```

Asegúrese de que no haya errores relacionados con fpolicy.

3. Si no se ven actividades, inicie sesión en SVM. Introduzca el siguiente comando:

```
<SVM>fpolicy show
```

Verifique si la política fpolicy denominada con el prefijo “cloudsecure_” se ha configurado y el estado es “activado”. Si no se configura, lo más probable es que el agente no pueda ejecutar los comandos en la SVM. Asegúrese de que se hayan cumplido todos los requisitos previos descritos al principio de la página.

{vacío}

Problema: El recopilador de datos SVM está en estado de error y el mensaje de error es “El agente no pudo conectarse al recopilador”. **Pruebe esto:**

1. Lo más probable es que el agente esté sobrecargado y no pueda conectarse a los recopiladores de fuentes de datos.
2. Verifique cuántos recopiladores de fuentes de datos están conectados al agente.
3. Verifique también la velocidad del flujo de datos en la página “Toda la actividad” de la interfaz de usuario.
4. Si la cantidad de actividades por segundo es significativamente alta, instale otro Agente y mueva algunos de los Recopiladores de fuentes de datos al nuevo Agente.

{vacío}

Problema: El recopilador de datos de SVM muestra un mensaje de error como "fpolicy.server.connectError: el nodo no pudo establecer una conexión con el servidor FPolicy "12.195.15.146" (motivo: "Se agotó el tiempo de selección")" **Pruebe esto:** El firewall está habilitado en SVM/Cluster. Entonces, el motor fpolicy no puede conectarse al servidor fpolicy. Las CLI en ONTAP que se pueden utilizar para obtener más información son:

```
event log show -source fpolicy which shows the error
event log show -source fpolicy -fields event,action,description which
shows more details.
```

"Comprobar los comandos del firewall"en el lado de ONTAP .

{vacío}

Problema: Mensaje de error: “El conector está en estado de error. Nombre del servicio:auditoría. Motivo del error: No se encontró ninguna interfaz de datos válida (función: datos, protocolos de datos: NFS o CIFS o ambos, estado: activo) en la SVM. **Pruebe esto:** Asegúrese de que haya una interfaz operativa (que tenga

función de datos y protocolo de datos como CIFS/NFS).

{vacío}

Problema: El recopilador de datos entra en estado de Error y luego pasa al estado EN EJECUCIÓN después de un tiempo, para luego volver al estado de Error nuevamente. Este ciclo se repite. **Pruebe esto:** Esto suele suceder en el siguiente escenario:

1. Se agregaron varios recopiladores de datos.
2. A los recopiladores de datos que muestren este tipo de comportamiento se les agregará 1 SVM. Lo que significa que 2 o más recopiladores de datos están conectados a 1 SVM.
3. Asegúrese de que un recopilador de datos se conecte a solo una SVM.
4. Eliminar los demás recopiladores de datos que estén conectados al mismo SVM.

{vacío}

Problema: El conector está en estado de error. Nombre del servicio: auditoría. Motivo del error: No se pudo configurar (política en SVM svmname. Motivo: Valor no válido especificado para el elemento 'shares-to-include' dentro de 'fpolicy.policy.scope-modify: "Federal" **Pruebe esto:** *Los nombres de los recursos compartidos deben proporcionarse sin comillas. Edite la configuración de DSC de ONTAP SVM para corregir los nombres de los recursos compartidos.

Incluir y excluir acciones no está pensado para una lista larga de nombres de acciones. Utilice el filtrado por volumen en su lugar si tiene una gran cantidad de acciones para incluir o excluir.

{vacío}

Problema: Existen políticas fpolicies en el Cluster que no se utilizan. ¿Qué se debe hacer con ellos antes de instalar Workload Security? **Pruebe esto:** Se recomienda eliminar todas las configuraciones fpolicy existentes no utilizadas incluso si están en estado desconectado. Workload Security creará fpolicy con el prefijo "cloudsecure_". Se pueden eliminar todas las demás configuraciones de fpolicy no utilizadas.

Comando CLI para mostrar la lista fpolicy:

```
 fpolicy show
Pasos para eliminar configuraciones de fpolicy:
```

```
fpolicy disable -vserver <svmname> -policy-name <policy_name>
fpolicy policy scope delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy event delete -vserver <svmname> -event-name <event_list>
fpolicy policy external-engine delete -vserver <svmname> -engine-name
<engine_name>
```

{vacío}

Problema: Después de habilitar la seguridad de la carga de trabajo, el rendimiento de ONTAP se ve afectado: la latencia se vuelve esporádicamente alta, las IOP se vuelven esporádicamente bajas. **Pruebe esto:** Al usar ONTAP con Workload Security, a veces se pueden observar problemas de latencia en ONTAP. Hay varias razones posibles para esto, como se señala a continuación:"1372994" , "1415152" , "1438207" , "1479704" , "1354659" . Todos estos problemas están solucionados en ONTAP 9.13.1 y versiones posteriores; se recomienda encarecidamente utilizar una de estas versiones posteriores.

{vacío}

Problema: El recopilador de datos muestra el mensaje de error: “Error: No se pudo determinar el estado del recopilador en 2 reintentos, intente reiniciar el recopilador nuevamente (Código de error: AGENT008)”. **Prueba esto:**

1. En la página Recopiladores de datos, desplácese hacia la derecha del recopilador de datos que genera el error y haga clic en el menú de 3 puntos. Seleccione *Editar*. Introduzca nuevamente la contraseña del recopilador de datos. Guarde el recopilador de datos presionando el botón *Guardar*. El recopilador de datos se reiniciará y el error debería resolverse.
2. Es posible que la máquina del agente no tenga suficiente espacio en CPU o RAM; es por eso que los DSC están fallando. Verifique la cantidad de recopiladores de datos que se agregaron al agente en la máquina. Si es más de 20, aumente la capacidad de CPU y RAM de la máquina del Agente. Una vez que se aumenta la CPU y la RAM, los DSC pasarán al estado de inicialización y luego al estado de ejecución automáticamente. Consulta la guía de tallas en"esta página" .

{vacío}

Problema: El recopilador de datos genera un error cuando se selecciona el modo SVM. **Pruebe esto:** Al conectarse en modo SVM, si se utiliza la IP de administración del clúster para conectarse en lugar de la IP de administración de SVM, la conexión generará un error. Asegúrese de que se utilice la IP SVM correcta.

{vacío}

Problema: El recopilador de datos muestra un mensaje de error cuando la función Acceso denegado está habilitada: "El conector está en estado de error. Nombre del servicio: auditoría. Motivo del error: No se pudo configurar fpolicy en SVM test_svm. Motivo: El usuario no está autorizado." **Pruebe esto:** Es posible que al usuario le falten los permisos REST necesarios para la función Acceso denegado. Por favor, siga las instrucciones en"esta página" para establecer los permisos.

Reinicie el recopilador una vez establecidos los permisos.

{vacío}

Problema: El recopilador está en estado de error con el mensaje: El conector está en estado de error. Motivo del error: No se pudo configurar el almacenamiento persistente en SVM <Nombre de SVM>. Motivo: No se

---

puede encontrar un agregado adecuado para el volumen "<volumeName>" en SVM "<SVM Name>". Motivo: La información de rendimiento del agregado "<aggregateName>" no está disponible actualmente. Espere unos minutos e intente el comando nuevamente. Nombre del servicio: auditoría. Motivo del fallo: Error al configurar el almacén persistente en SVM <SVM Name>. Motivo: No se ha podido encontrar un agregado adecuado para el volumen "<volumeName>" en SVM "<SVM Name>". Razón: La información de rendimiento para el agregado "<aggregateName>" no está disponible actualmente. Espere unos minutos e inténtelo de nuevo.

Pruebe esto: Espere unos minutos y luego reinicie el recopilador.

{vacío}

Si aún tiene problemas, comuníquese con los enlaces de soporte mencionados en la página **Ayuda > Soporte**.

Configuración del recopilador Cloud Volumes ONTAP y Amazon FSx for NetApp ONTAP

Supervise el acceso de usuarios y archivos en su infraestructura de almacenamiento en la nube configurando los recopiladores de datos de Workload Security para Cloud Volumes ONTAP y Amazon FSx for NetApp ONTAP. Esta guía proporciona instrucciones paso a paso para implementar agentes en AWS y conectarlos a sus instancias de almacenamiento en la nube.

Configuración de almacenamiento de Cloud Volumes ONTAP

Consulte la documentación de OnCommand Cloud Volumes ONTAP para configurar una instancia de AWS de nodo único/HA 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 completada la configuración, siga los pasos para configurar su 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 en la nube disponibles donde sea posible. Por ejemplo: Amazon, Azure, Google Cloud.
- ONTAP Amazon FSx

Configuración de la máquina del agente

La máquina del agente debe configurarse 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. Se pueden seguir pasos equivalentes, según corresponda al proveedor de servicios en la nube, en Azure o Google Cloud para la instalación.

En AWS, utilice los siguientes pasos para configurar la máquina que se utilizará como agente de seguridad de carga de trabajo:

Utilice los siguientes pasos para configurar la máquina que se utilizará como agente de seguridad de carga de trabajo:

Pasos

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

Instalar el agente de seguridad de carga de trabajo

1. Inicie sesión como administrador o propietario de cuenta en su entorno de Data Infrastructure Insights .
2. Vaya a **Recopiladores** de seguridad de carga de trabajo y haga clic en la pestaña **Agentes**.
3. Haga clic en **+Agente** y especifique RHEL como la plataforma de destino.
4. Copie el comando de instalación del agente.
5. Pegue el comando de instalación del agente en la instancia RHEL EC2 en la que ha iniciado sesión. Esto instala el agente de seguridad de carga de trabajo, que proporciona toda la"Requisitos previos del agente" se cumplen.

Para conocer los pasos detallados, consulte este enlace: https://docs.netapp.com/us-en/cloudinsights/task_cs_add_agent.html#steps-to-install-agent

Solución de problemas

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

Problema	Resolución
El recopilador de datos muestra el error “Seguridad de la carga de trabajo: No se pudo determinar el tipo de ONTAP 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 desde el agente está agotando el tiempo de espera. Los grupos de seguridad de firewall y AWS tienen las reglas necesarias habilitadas para permitir la comunicación. Ya hay un agente implementado y también está en la misma cuenta de AWS. Este mismo agente se utiliza para conectar y supervisar los dispositivos NetApp restantes (y todos están funcionando).	Resuelva este problema agregando el segmento de red LIF fsxadmin a la regla de seguridad del agente. Se permiten todos los puertos si no está seguro acerca de ellos.

Gestión de usuarios

Las cuentas de usuario de Workload Security se administran a través de Data Infrastructure Insights.

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 que tenga privilegios de administrador puede crear o modificar usuarios y asignar a cada usuario uno de los siguientes roles de seguridad de carga de trabajo:

Role	Acceso de seguridad a la carga de trabajo
Administrador	Puede realizar todas las funciones de seguridad de carga de trabajo, incluidas las de alertas, análisis forense, recopiladores de datos, políticas de respuesta automatizadas y API para seguridad de carga de trabajo. Un administrador también puede invitar a otros usuarios, pero solo puede asignar roles de seguridad de carga de trabajo.
Usuario	Puede ver y administrar alertas y ver análisis forenses. El rol de usuario puede cambiar el estado de alerta, agregar una nota, tomar instantáneas manualmente y restringir el acceso de los usuarios.
Invitado	Puede ver alertas y análisis forenses. El rol de invitado no puede cambiar el estado de alerta, agregar una nota, tomar instantáneas manualmente ni restringir el acceso de los usuarios.

Pasos

1. Iniciar sesión en Seguridad de la carga de trabajo
2. En el menú, haga clic en **Admin > Gestión de usuarios**

   Serás redirigido a la página de Administración de usuarios de Data Infrastructure Insights.

3. Seleccione el rol deseado para cada usuario.

Al agregar un nuevo usuario, simplemente seleccione el rol deseado (generalmente Usuario o Invitado).

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

Comprobador de event rate: guía de dimensionamiento de agentes

Determina el tamaño óptimo de la máquina del Agent midiendo las tasas de eventos NFS y SMB generadas por tus SVMs antes de desplegar los data collectors. El script Event Rate Checker te ayuda a entender los límites de capacidad (máximo 50 data collectors por Agent) y asegura que tu infraestructura de Agent pueda manejar el volumen de eventos esperado para una detección de amenazas confiable.

Requisitos:

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

> Al ejecutar este script, no debe ejecutarse ningún recopilador de datos ONTAP SVM para el SVM para el cual se está determinando la tasa de eventos.

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
. Este script requiere que _sshpass_ esté instalado en la máquina Linux.
Hay dos formas de instalarlo:
```

   a. Ejecute el siguiente comando:

```
 linux_prompt> yum install sshpass
.. Si eso no funciona, descargue _sshpass_ a la máquina Linux desde
la web y ejecute el siguiente comando:
```

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

3. Proporcione los valores correctos cuando se le solicite. Vea un ejemplo a continuación.
4. El script tardará aproximadamente 5 minutos en ejecutarse.
5. Una vez completada la ejecución, el script imprimirá la tasa de eventos desde el SVM. Puede verificar la tasa de eventos por SVM en la salida de la consola:

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

Cada recopilador de datos SVM de Ontap se puede asociar con un único SVM, lo que significa que cada recopilador de datos podrá recibir la cantidad de eventos que genera un único SVM.

Tenga en cuenta lo siguiente:

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

Configuración de la máquina del agente	Número de recopiladores de datos de SVM	Tasa máxima de eventos que la máquina del agente puede manejar
4 núcleos, 16 GB	10 recopiladores de datos	20K eventos/seg

4 núcleos, 32 GB	20 recopiladores de datos	20K eventos/seg

B) Para calcular el total de eventos, agregue los eventos generados para todos los SVM para ese agente.

C) Si el script no se ejecuta durante las horas pico o si el tráfico pico es difícil de predecir, mantenga un margen de tasa de eventos del 30 %.

B + C debe ser menor que A, de lo contrario, la máquina del Agente no podrá realizar el monitoreo.

En otras palabras, la cantidad de recopiladores de datos que se pueden agregar a una sola máquina agente debe cumplir con la siguiente fórmula:

```
 Sum of all Event rate of all Data Source Collectors + Buffer Event rate
of 30% < 20000 events/second
Ver ellink:concept_cs_agent_requirements.html["Requisitos del agente"]
Página para requisitos previos y requisitos adicionales.
```

Ejemplo

Digamos que tenemos tres SVMS 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 la máquina del Agente en el nombre de archivo *fpolicy_stat_<SVM Name>.log* en el directorio de trabajo actual.

El script puede dar resultados erróneos en los siguientes casos:

- Se proporcionaron credenciales, IP o nombre SVM incorrectos.
- Una fpolicy ya existente con el mismo nombre, número de secuencia, etc. generará un 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]#
```

Solución de problemas

Pregunta	Respuesta

Si ejecuto este script en una SVM que ya está configurada para Seguridad de carga de trabajo, ¿solo utiliza la configuración fpolicy existente en la SVM o configura una temporal y ejecuta el proceso?	El verificador de tasa de eventos puede funcionar correctamente incluso para una SVM ya configurada para seguridad de carga de trabajo. No debería haber ningún impacto.
¿Puedo aumentar la cantidad de SVM en las que se puede ejecutar el script?	Sí. Simplemente edite el script y cambie el número máximo de SVM de 5 a cualquier número deseado.
Si aumento la cantidad 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 la cantidad de SVM en las que se puede ejecutar el script?	Sí. Debes editar el script y cambiar el número máximo de SVM de 5 a cualquier número deseado.
Si aumento la cantidad de SVM, ¿aumentará el tiempo de ejecución del script?	No. El script se ejecutará durante un máximo de 5 minutos, incluso si se aumenta la cantidad de SVM.
¿Qué sucede si ejecuto el Verificador de tasa de eventos con un agente existente?	Ejecutar el verificador de tasa de eventos en un agente ya existente puede provocar un aumento en la latencia en la SVM. Este aumento será de naturaleza temporal mientras se ejecuta el Comprobador de tasa de eventos.