Primeros pasos

Cloud Insights

NetApp
June 18, 2024

Tabla de contenidos

Primeros pasos

Introducción a Workload Security

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

La seguridad de carga de trabajo no está disponible en la edición federal de Cloud Insights.

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

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

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

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

Requisitos del agente de seguridad de cargas de trabajo

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

La seguridad de la carga de trabajo de almacenamiento no está disponible en la edición federal de Cloud Insights.

Componente	Requisitos de Linux
De NetApp	Un equipo que ejecuta una versión con licencia de uno de los siguientes: Red Hat Enterprise Linux 7.x, 8.x 64 bits, SELinux CentOS 7.x de 64 bits, SELinux CentOS 8 Stream, SELinux Ubuntu 20 a 22 64 bits Rocky 8.x de 64 bits, Rocky 9.x de 64 bits, SELinux SUSE Linux Enterprise Server 15 SP3, SUSE Linux Enterprise Server 15 SP4 y SELinux en SUSE 15 SP3 Este equipo no debe ejecutar ningún otro software de nivel de aplicación. Se recomienda un servidor dedicado.
Comandos	para la instalación es necesario descomprimir. Además, se requiere el comando 'efectuar su –' para la instalación, la ejecución de scripts y la desinstalación.
CPU	4 núcleos de CPU
Memoria	16 GB DE MEMORIA RAM
Espacio disponible en disco	El espacio en disco se debe asignar de esta manera: /Opt/netapp 36 GB (mínimo 35 GB de espacio libre tras la creación del sistema de archivos) Nota: Se recomienda asignar un poco de espacio adicional en el disco para permitir la creación del sistema de archivos. Asegúrese de que hay al menos 35 GB de espacio libre en el sistema de archivos. Si /opt es una carpeta montada de un almacenamiento NAS, asegúrese de que los usuarios locales tengan acceso a esta carpeta. Puede que el agente o el recopilador de datos no se instalen si los usuarios locales no tienen permiso para esta carpeta. consulte "resolución de problemas" para obtener más información.
Red	Conexión Ethernet de 100 Mbps a 1 Gbps, dirección IP estática, conectividad IP con todos los dispositivos y un puerto requerido para la instancia de seguridad de carga de trabajo (80 o 443).

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

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

Recomendaciones adicionales

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

Reglas de acceso a la red de cloud

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

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

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

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

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

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

Reglas dentro de la red

Protocolo	Puerto	Origen	Destino	Descripción
TCP	389(LDAP) 636 (LDAPS / start-tls)	Agente de Seguridad de Carga de Trabajo	URL del servidor LDAP	Conéctese a LDAP
TCP	443	Agente de Seguridad de Carga de Trabajo	Dirección IP de gestión del clúster o de SVM (según la configuración del recopilador SVM)	Comunicación API con ONTAP
TCP	35000 - 55000	Direcciones IP de LIF de datos de SVM	Agente de Seguridad de Carga de Trabajo	Comunicación de ONTAP al agente de seguridad de carga de trabajo para eventos de Fpolicy. Estos puertos deben abrirse hacia el agente de seguridad de carga de trabajo para que ONTAP le envíe eventos, incluido cualquier firewall del propio agente de seguridad de carga de trabajo (si está presente).
TCP	7	Agente de Seguridad de Carga de Trabajo	Direcciones IP de LIF de datos de SVM	Eco del agente a los LIF de datos de SVM

Protocolo	Puerto	Origen	Destino	Descripción
SSH	22	Agente de Seguridad de Carga de Trabajo	Gestión de clústeres	Necesario para el bloqueo de usuarios CIFS/SMB.

Ajuste de tamaño del sistema

Consulte "Comprobador de frecuencia de eventos" documentación para obtener información sobre el ajuste de tamaño.

Instalación de Workload Security Agent

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

La seguridad de carga de trabajo no está disponible en la edición federal de Cloud Insights.

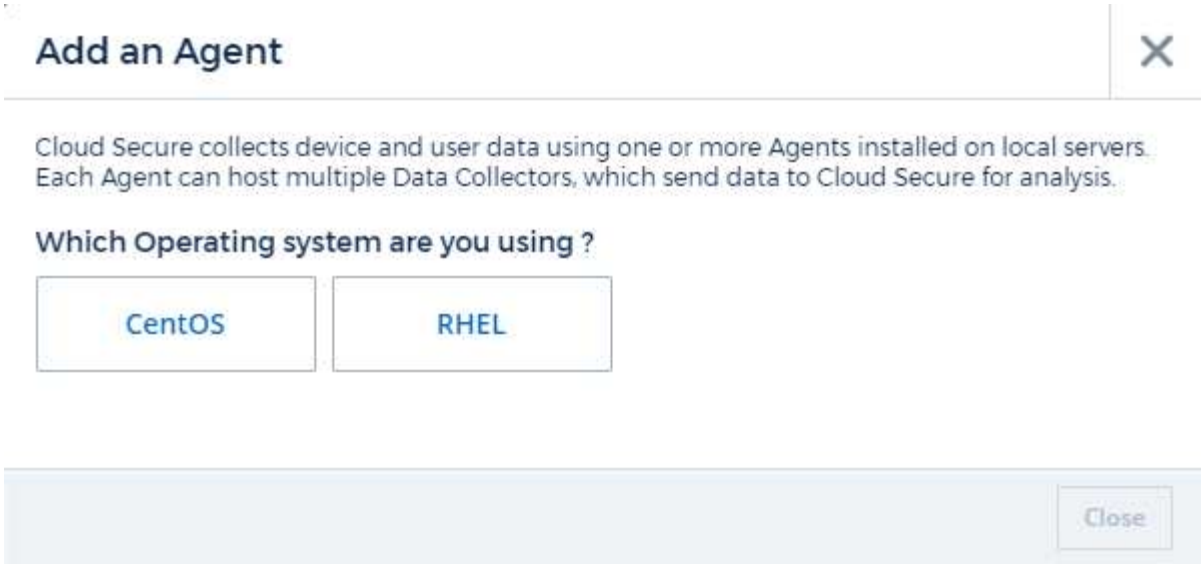
Antes de empezar

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

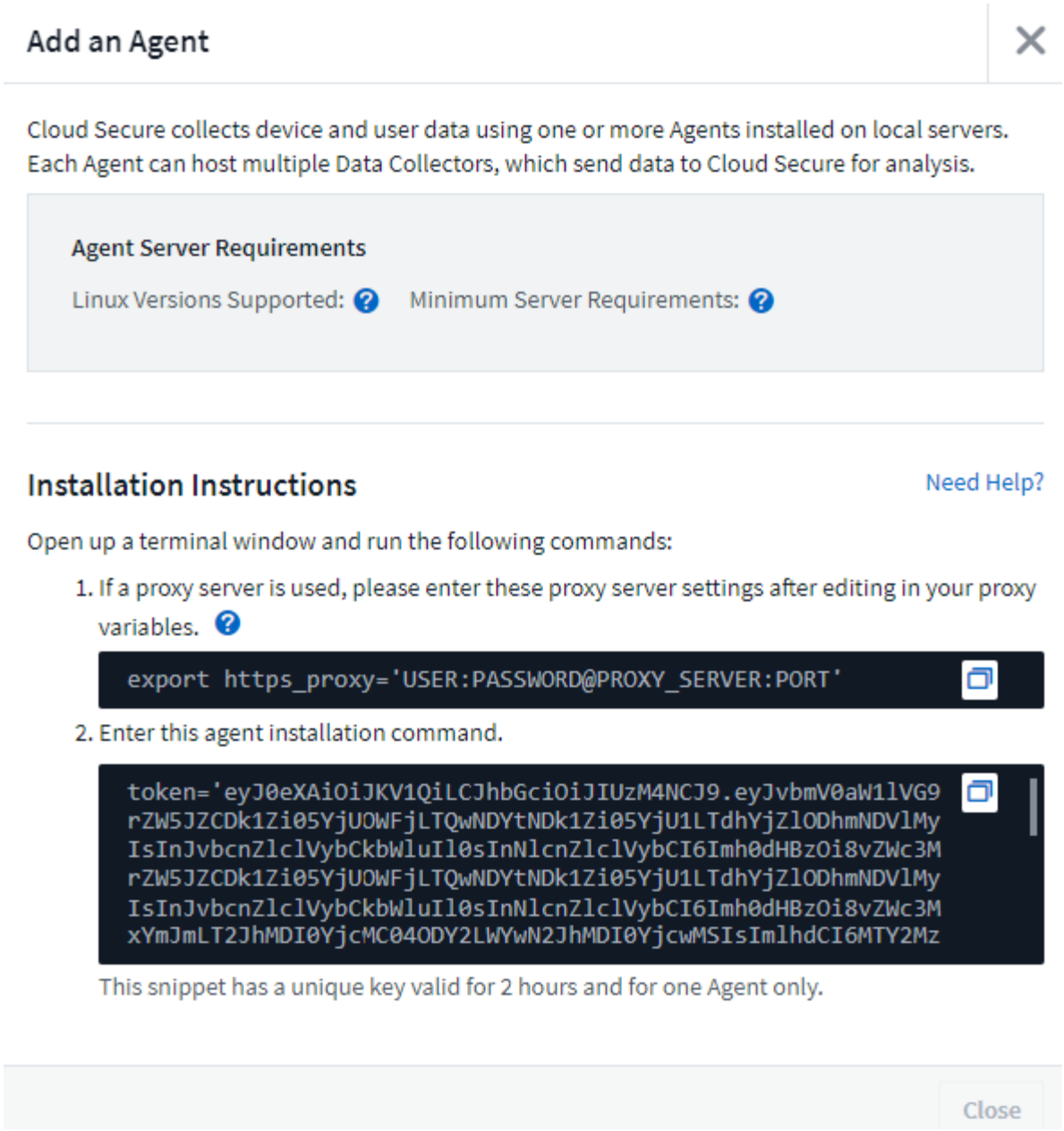
Pasos para instalar el agente

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

   El sistema muestra la página Agregar un agente:



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



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

Después de terminar

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

Configuración de red

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

Pasos

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

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

CentOS 7.x / RHEL 7.x:

1. `sudo iptables-save | grep 35000`

Salida de muestra:

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

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

Salida de muestra:

```
35000-55000/tcp
```

Solución de problemas de errores del agente

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

Problema:	Resolución:
La instalación del agente no puede crear la carpeta /opt/netapp/cloudsecure/agent/logs/agent.log y el archivo install.log no proporciona información relevante.	Este error se produce durante el arranque del agente. El error no se registra en los archivos de registro porque se produce antes de inicializar el registrador. El error se redirige a la salida estándar y es visible en el registro de servicios mediante el `journalctl -u cloudsecure-agent.service` comando. Este comando se puede usar para solucionar el problema con más detalle.
Se produce un error en la instalación del agente con ‘esta distribución de linux no es compatible. Salir de la instalación».	Este error aparece cuando intenta instalar el agente en un sistema no compatible. Consulte "Requisitos del agente".

Problema:	Resolución:
Error en la instalación del agente: "-bash: Unzip: Command not found"	Instale unzip y ejecute de nuevo el comando de instalación. Si se instala Yum en la máquina, intente “yum install unzip” para instalar el software de descompresión. Después, vuelva a copiar el comando desde la interfaz de usuario de instalación del agente y péguelo en la CLI para volver a ejecutar la instalación.
El agente se ha instalado y se estaba ejecutando. Sin embargo, el agente se ha detenido repentinamente.	SSH a la máquina del agente. Compruebe el estado del servicio del agente a través de `sudo systemctl status cloudsecure-agent.service`. 1. Compruebe si los registros muestran un mensaje “error al iniciar el servicio del demonio de seguridad de la carga de trabajo” . 2. Compruebe si el usuario cssys existe o no en el equipo del agente. Ejecute uno por uno los siguientes comandos con permiso root y compruebe si el usuario y grupo cssys existe. `sudo id cssys` `sudo groups cssys`3. Si no existe ninguno, una directiva de supervisión centralizada puede haber eliminado el usuario cssys. 4. Cree un usuario y un grupo cssys manualmente ejecutando los siguientes comandos. `sudo useradd cssys` `sudo groupadd cssys`5. Reinicie el servicio de agente después de eso ejecutando el siguiente comando: `sudo systemctl restart cloudsecure-agent.service`6. Si aún no se está ejecutando, compruebe las otras opciones de solución de problemas.
No se pueden agregar más de 50 recopiladores de datos a un agente.	Sólo se pueden agregar 50 recopiladores de datos a un agente. Puede ser una combinación de todos los tipos de recopilador, por ejemplo, Active Directory, SVM y otros recopiladores.
La interfaz de usuario muestra que el agente está en estado NOT_CONNECTED.	Pasos para reiniciar el agente. 1. SSH a la máquina del agente. 2. Reinicie el servicio de agente después de eso ejecutando el siguiente comando: `sudo systemctl restart cloudsecure-agent.service`3. Compruebe el estado del servicio del agente a través de `sudo systemctl status cloudsecure-agent.service`. 4. El agente debe pasar al estado CONECTADO.
El agente VM se encuentra detrás del proxy Zscaler y la instalación del agente falla. Debido a la inspección SSL del proxy de Zscaler, los certificados de seguridad de carga de trabajo se presentan como firmados por la CA de Zscaler, por lo que el agente no confía en la comunicación.	Desactive la inspección SSL en el proxy Zscaler para la URL *.cloudinsights.netapp.com. Si Zscaler realiza una inspección SSL y reemplaza los certificados, Workload Security no funcionará.

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

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

Eliminar un agente de seguridad de carga de trabajo

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

Eliminar un agente

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

Antes de empezar

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

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

Pasos para eliminar un agente:

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

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

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

   El sistema muestra la lista de agentes configurados.

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

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

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

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

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

Antes de empezar

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

Pasos para configurar un recopilador de directorios de usuarios

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

   El sistema muestra la pantalla Agregar directorio de usuario.

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

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

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

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

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

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

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

Estado	estado
Departamento	departamento
Foto	thumbnailphoto
DN de administrador	gerente
Grupos	Miembro de

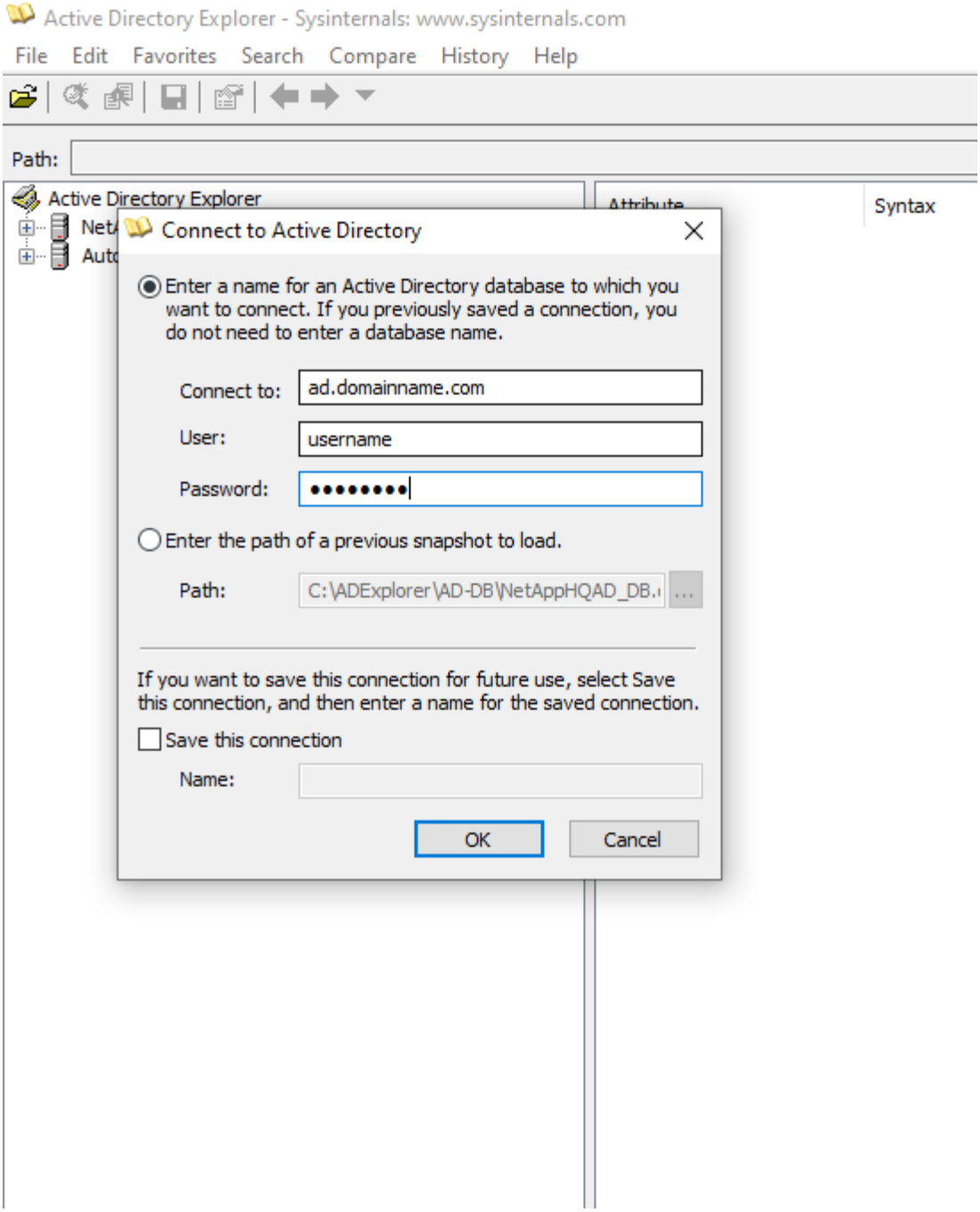
Prueba de la configuración del recopilador del directorio de usuarios

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

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

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

- Utilice el Explorador de AD para desplazarse por una base de datos 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.
  - Instale "Explorador DE ANUNCIOS" En cualquier equipo Windows que pueda conectarse al servidor AD.
  - Conéctese al servidor AD mediante el nombre de usuario/contraseña del servidor de directorio AD.



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

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

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

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

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

Configurar un recopilador de servidor de directorio LDAP

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

Antes de empezar

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

Pasos para configurar un recopilador de directorios de usuarios

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

   El sistema muestra la pantalla Agregar directorio de usuario.

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

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

--cuentas	--usuarios
--juan	--anna
ENLAZAR contraseña	Contraseña del servidor de directorio (es decir, contraseña para el nombre de usuario utilizado en DN de enlace)
Protocolo	ldap, ldaps, ldap-start-tls
Puertos	Seleccione el puerto

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

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

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

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

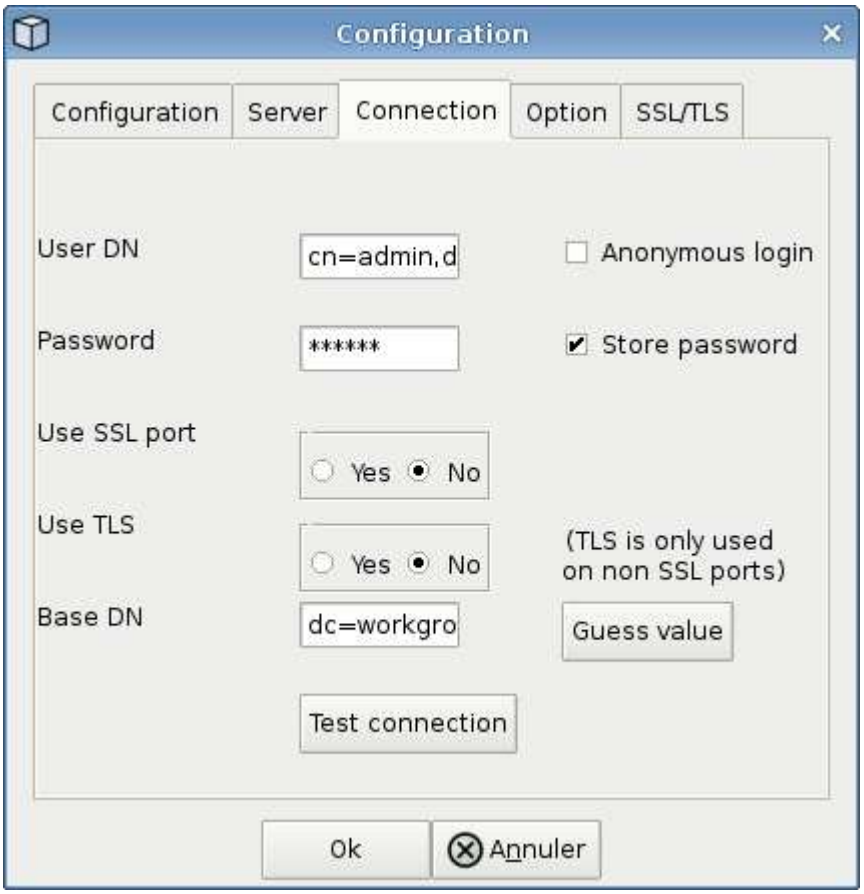
Prueba de la configuración del recopilador del directorio de usuarios

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

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

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

- Instale el Explorador de LDAP O Explorador LDAP de Java En cualquier equipo Windows que pueda conectarse al servidor LDAP.
- Conéctese al servidor LDAP con el nombre de usuario/contraseña del servidor de directorio LDAP.



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

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

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

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

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

Configurar el recopilador de datos de SVM de ONTAP

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

Antes de empezar

- Este recopilador de datos es compatible con lo siguiente:
  - Data ONTAP 9.2 y versiones posteriores. Para obtener el mejor rendimiento, utilice una versión de Data ONTAP superior a 9.13.1.
  - Protocolo SMB, versión 3.1 y versiones anteriores.
  - Protocolo NFS versión 4.0 y anteriores
  - ONTAP 9.4 y versiones posteriores admiten FlexGroup
  - ONTAP Select es compatible
- Solo se admiten SVM de tipo de datos. No se admiten las SVM con Infinite Volume.
- SVM tiene varios subtipos. De estos, sólo se admiten *default*, *SYNC_Source* y *SYNC_Destination*.
- Un agente "debe configurarse" antes de configurar recopiladores de datos.
- Asegúrese de que tiene un conector de directorio de usuario configurado correctamente; de lo contrario, los eventos mostrarán nombres de usuario codificados y no el nombre real del usuario (tal como se almacena en Active Directory) en la página “Activity Forensics”.
- Para obtener un rendimiento óptimo, debe configurar el servidor FPolicy para que esté en la misma subred que el sistema de almacenamiento.
- Debe añadir una SVM mediante uno de los siguientes dos métodos:
  - Mediante Cluster IP, SVM name y Cluster Management Username and Password. ***este es el método recomendado.***
    - El nombre de la SVM debe ser exactamente el que se muestra en ONTAP y distingue entre mayúsculas y minúsculas.
  - Mediante la administración de Vserver IP, nombre de usuario y contraseña de SVM
  - Si no puede o no desea utilizar el nombre de usuario y la contraseña de Administrator Cluster/SVM Management, puede crear un usuario personalizado con privilegios menores como se indica en la “Una nota sobre los permisos” a continuación. Este usuario personalizado se puede crear tanto para SVM como para el acceso a clústeres.
    - o también puede usar un usuario de AD con una función que tenga al menos los permisos de csrole como se menciona en la sección “una nota sobre los permisos” que aparece a continuación.

Consulte también la "Documentación de ONTAP".

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

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

Resultado de ejemplo:

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

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

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

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

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

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

Requisitos previos para bloqueo de acceso del usuario

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

Se necesitan credenciales para que esta función funcione.

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

Si utiliza un usuario personalizado (por ejemplo, *csuser*) con permisos proporcionados al usuario, siga los

pasos que se indican a continuación para otorgar permisos a Workload Security para bloquear al usuario.

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

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

Una nota sobre los permisos

Permisos al agregar mediante IP de administración de clúster:

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

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

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

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

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

Permisos al agregar mediante IP de administración de Vserver:

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

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

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

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

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

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

Permisos para la protección autónoma frente a ransomware de ONTAP

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

Si utiliza un usuario personalizado (por ejemplo, *csuser*) con permisos proporcionados al usuario, siga los

pasos que se indican a continuación para otorgar permisos a Seguridad de carga de trabajo para recopilar información relacionada con ARP desde ONTAP.

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

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

Para obtener más información, lea acerca de "Integración con la protección autónoma de ransomware de ONTAP"

Se han denegado los permisos para el acceso a ONTAP

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

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

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

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

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

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

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

Configure el recopilador de datos

Pasos para la configuración

1. Inicie sesión como administrador o propietario de cuenta en su entorno de Cloud Insights.

2. Haga clic en **Workload Security > Collectors > +Data Collectors**

   El sistema muestra los colectores de datos disponibles.

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

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

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

Después de terminar

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

Configuración recomendada para Metro Cluster

Se recomienda lo siguiente para Metro Cluster:

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

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

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

Política de servicio

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

Ejemplo:

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

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

Reproducir-Pausa del recopilador de datos

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

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

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

Tenga en cuenta lo siguiente:

- La purga de snapshots no se producirá de acuerdo con la configuración configurada en un recopilador en

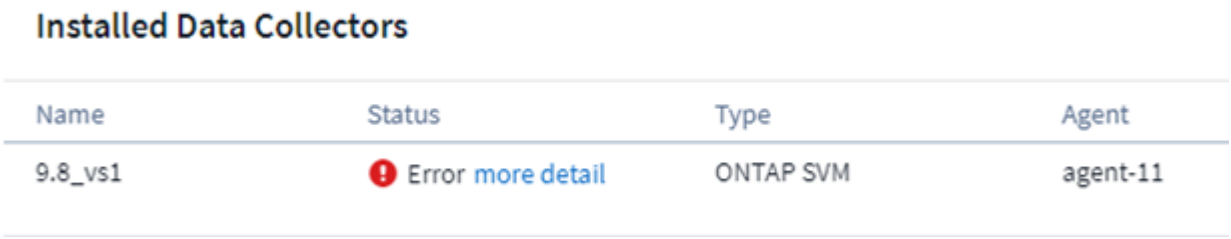
pausa.

- Los eventos de EMS (como ARP de ONTAP) no se procesarán en un recopilador en pausa. Esto significa que si ONTAP identifica un ataque de ransomware, la seguridad de carga de trabajo Cloud Insights no podrá adquirir ese evento.
- NO se enviarán correos electrónicos de notificaciones de estado para un recopilador en pausa.
- Las acciones manuales o automáticas (como Instantánea o Bloqueo de usuarios) no se admitirán en un recopilador en pausa.
- En las actualizaciones de agente o recopilador, la VM del agente se reinicia o reinicia el servicio del agente, un recopilador en pausa permanecerá en estado *Paused*.
- Si el recopilador de datos está en estado *Error*, el recopilador no se puede cambiar al estado *Paused*. El botón Pausa solo se activará si el estado del recopilador es *Running*.
- Si el agente está desconectado, el recopilador no se puede cambiar al estado *Paused*. El recopilador pasará al estado *STOP* y el botón Pause se desactivará.

Resolución de problemas

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

En caso de error, haga clic en *more detail* en la columna *Status* para obtener más información sobre el error.



Problema:	Resolución:
El recopilador de datos se ejecuta durante algún tiempo y se detiene después de un tiempo aleatorio, con el error "mensaje de error: El conector está en estado de error. Nombre del servicio: Auditoría. Motivo del fallo: Servidor de fpolicy externo sobrecargado."	La velocidad de eventos de ONTAP era mucho mayor que la que puede manejar el cuadro Agente. Por lo tanto, la conexión finalizó. Compruebe el tráfico máximo en CloudSecure cuando se haya realizado la desconexión. Esto puede comprobar en la página **CloudSecure > Activity Forensics > All Activity**. Si el tráfico agregado pico es superior al que puede controlar Agent Box, consulte la página Comprobador de tasa de eventos sobre cómo ajustar el tamaño de la implementación de Collector en un cuadro de agente. Si el Agente fue instalado en el cuadro Agente antes del 4 de marzo de 2021, ejecute los siguientes comandos en el cuadro Agente: Echo 'net.core.rmem_max=8388608' >> /etc/sysctl.conf echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf sysctl -p después de reiniciar el colector.

Problema:	Resolución:
El recopilador informa de un mensaje de error: “No se ha encontrado ninguna dirección IP local en el conector que pueda llegar a las interfaces de datos de la SVM”.	Lo más probable es que esto se deba a un problema de red en ONTAP. Siga estos pasos: 1. Asegúrese de que no haya ningún firewall en el LIF de datos de SVM o en el LIF de gestión que bloqueen la conexión desde la SVM. 2. Al añadir una SVM a través de una IP de administración de clúster, asegúrese de que el LIF de datos y el LIF de gestión de la SVM se pueden pingable desde el equipo virtual del agente. En caso de problemas, compruebe la puerta de enlace, la máscara de red y las rutas del LIF. También puede intentar iniciar sesión en el clúster a través de ssh mediante la IP de administración del clúster y hacer ping a la IP del agente. Asegúrese de que la IP del agente es pingable: *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, de modo que el equipo del agente sea pingable. 3. Si ha intentado realizar la conexión a través de la IP del clúster y no funciona, intente realizar la conexión directamente a través de la IP de SVM. Consulte los pasos anteriores para conectar mediante IP de SVM. 4. Al añadir el recopilador a través de las credenciales de SVM IP y vsadmin, compruebe si la SVM Lif tiene el rol Data más Mgmt habilitado. En este caso, ping a la SVM Lif funcionará, sin embargo SSH a la SVM Lif no funcionará. Si la respuesta es sí, cree una Lif de solo para gestión de SVM y pruebe a conectarse a través de esta Lif de gestión de SVM. 5. Si todavía no funciona, cree una nueva SVM Lif e intente conectarse a través de esa 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 a la SVM desde la interfaz de usuario de CloudSecure. c) Espere hasta que aparezca el error. Detenga el seguimiento de paquetes en ONTAP. d) Abra el rastreo de paquetes desde ONTAP. Está disponible en esta ubicación

Problema:	Resolución:
Mensaje: "No se ha podido determinar el tipo de ONTAP para [hostname: <IP Address>. Motivo: Error de conexión con Storage System <IP Address>: No se puede acceder al host (no se puede acceder al host)"	1. Compruebe que se ha proporcionado la dirección IP de administración de SVM o la IP de administración de clúster correctas. 2. SSH a la SVM o el clúster al que pretende conectarse. Una vez que esté conectado, asegúrese de que la SVM o el nombre del clúster sean correctos.
Mensaje de error: "El conector está en estado de error. service.name: Auditoría. Motivo del fallo: El servidor de fpolicy externo ha finalizado."	1. Lo más probable es que un firewall esté bloqueando los puertos necesarios en el equipo del agente. Compruebe que el intervalo de puertos 35000-55000/tcp está abierto para que la máquina del agente se conecte desde la SVM. Asegúrese también de que no hay firewalls habilitados desde la comunicación de bloqueo del lado ONTAP al equipo agente. 2. Escriba el siguiente comando en el cuadro Agente y asegúrese de que el intervalo de puertos está abierto. _Sudo iptables-save

Problema:	Resolución:
grep 3500*_ la salida de la muestra debería ser: *-A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate NEW -j ACCEPT* 3. Inicie sesión en SVM, introduzca los siguientes comandos y compruebe que no hay ningún firewall configurado para bloquear la comunicación con ONTAP. *servidor de seguridad show servidor de seguridad de los servicios del sistema muestra_"Compruebe los comandos del firewall" En el lado ONTAP. 4. SSH a la SVM/clúster que desea supervisar. Haga ping en la casilla Agent desde el LIF de datos de la SVM (con compatibilidad con CIFS y protocolos NFS) y asegúrese de que funciona ping: _Network ping -vserver <vserver name> -Destination <Agent IP> -lif <Lif Name> -show-detail* Si no se pueden pingable, asegúrese de que la configuración de red en ONTAP sea correcta, de modo que el agente se pueda pingable. 5.Si se agrega una única SVM dos veces a un inquilino a través de 2 recopiladores de datos, se mostrará este error. Elimine uno de los recopiladores de datos a través de la interfaz de usuario. A continuación, reinicie el otro recopilador de datos a través de la interfaz de usuario. A continuación, el recopilador de datos mostrará el estado “RUNNING” y comenzará a recibir eventos de SVM. Básicamente, en un inquilino, se debe añadir 1 SVM solo una vez, mediante 1 recopilador de datos. 1 SVM no debe añadirse dos veces a través de 2 recopiladores de datos. 6. En los casos en los que se añadió la misma SVM en dos entornos de seguridad de carga de trabajo (inquilinos) distintos, el último tendrá siempre éxito. El segundo colector configurará fpolicy con su propia dirección IP y la pondrá en marcha la primera. De modo que el cobrador en el primero dejará de recibir eventos y su servicio de "auditoria" entrará en estado de error. Para evitar esto, configure cada SVM en un único entorno. 7. 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 origen de datos, se necesita el servicio cliente-fpolicy-data junto con el servicio de datos-nfs y/o data-cifs. Además, el servicio de cliente-fpolicy-data debe estar asociado a los LIF de datos de la SVM supervisada.	No se ven eventos en la página de actividad.

Problema:	Resolución:
1. Compruebe si el colector de ONTAP está en el estado "EN EJECUCIÓN". Si la respuesta es sí, asegúrese de que algunos eventos de cifs se generan en las máquinas virtuales del cliente cifs abriendo algunos archivos. 2. Si no se ve ninguna actividad, inicie sesión en la SVM e introduzca el siguiente comando. *<SVM> learlog show -source fpolicy* por favor, asegúrese de que no hay errores relacionados con fpolicy. 3. Si no se ve ninguna actividad, inicie sesión en el SVM. Introduzca el siguiente comando *<SVM> policy show* Compruebe si se ha establecido la directiva fpolicy llamada con el prefijo “cloudsecure_” y el estado es “on”. Si no se establece, lo más probable es que el agente no pueda ejecutar los comandos en la SVM. Asegúrese de que se han seguido todos los requisitos previos descritos al principio de la página.	El colector de datos SVM está en estado de error y el mensaje Ererrror es “el agente no ha podido conectarse al recopilador”.
1. Lo más probable es que el agente esté sobrecargado y no pueda conectarse a los recopiladores de origen de datos. 2. Compruebe cuántos recopiladores de origen de datos están conectados al agente. 3. Compruebe también el flujo de datos en la página “All Activity” de la interfaz de usuario. 4. Si el número de actividades por segundo es significativamente alto, instale otro agente y mueva algunos de los colectores de origen de datos al nuevo agente.	El recopilador de datos de SVM muestra el mensaje de error "fpolicy.server.connectError: Node Failed to establecer una conexión con el servidor FPolicy "12.195.15.146" (Reason: "Select Timed out")"
El firewall está habilitado en SVM/Cluster. Por lo tanto, fpolicy Engine no puede conectarse al servidor fpolicy. Las CLI de ONTAP que pueden utilizarse para obtener más información son: Event log show -source fpolicy que muestra el error event log show -source fpolicy -fields event,action,description que muestra más detalles."Compruebe los comandos del firewall" En el lado ONTAP.	Mensaje de error: “El conector está en estado de error. Nombre del servicio:audit. Motivo del fallo: No hay una interfaz de datos válida (función: Datos, protocolos de datos: NFS o CIFS o ambos, estado: Up) encontrado en la SVM.”
Compruebe que hay una interfaz operativa (teniendo la función de protocolo de datos y de datos como CIFS/NFS).	El recopilador de datos entra en el estado error y, a continuación, pasa al estado EN EJECUCIÓN después de algún tiempo y, a continuación, vuelve a error. Este ciclo se repite.
Esto ocurre normalmente en el siguiente escenario: 1. Se han agregado varios recopiladores de datos. 2. Los recopiladores de datos que muestran este tipo de comportamiento tendrán 1 SVM agregado a estos recopiladores de datos. Esto significa que 2 o más recopiladores de datos están conectados a 1 SVM. 3. Asegúrese de que 1 recopilador de datos se conecta a solo 1 SVM. 4. Elimine los otros recopiladores de datos que estén conectados a la misma SVM.	El conector está en estado de error. Nombre del servicio: Auditoría. Motivo del fallo: No se puede configurar (política en svmname de SVM. Motivo: Se ha especificado un valor no válido para el elemento "hay que incluir" dentro de "fpolicy.policy.scope-modify: "Federal"

Problema:	Resolución:
Los nombres de los recursos compartidos deben indicarse sin comillas. Edite la configuración DSC de la SVM ONTAP para corregir los nombres de los recursos compartidos. *Include y exclude shares* no está destinado a una larga lista de nombres de recursos compartidos. En su lugar, utilice el filtrado por volumen si tiene un gran número de recursos compartidos que incluir o excluir.	Existen fPolicies en el Cluster que no se utilizan. ¿Qué debería hacer con esas personas antes de instalar Workload Security?
Se recomienda eliminar toda la configuración existente de fpolicy sin usar 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 de la CLI para mostrar la lista de fpolicy: *Fpolicy show* pasos para eliminar las configuraciones de fpolicy: *Fpolicy disable -vserver <svmname> -policy-name <policy_name> fpolicy scope delete -vserver <svmname> -policy-name <policy_name> fpolicy delete -vserver <svmname> -policy-name <policy_name> <svmname> fpolicy event delete -vserver <svmname> <engine_name> -event-name <event_list>* _fpolicy Engine	Después de habilitar la seguridad de cargas de trabajo, el rendimiento de la ONTAP se ve afectado: La latencia se vuelve esporádicamente alta, la tasa de IOPS se hace más baja de forma esporádica.
Mientras se utiliza ONTAP con seguridad de carga de trabajo, a veces se pueden ver problemas de latencia en ONTAP. Hay una serie de posibles razones para esto, como se indica en los siguientes: "1372994", "1415152", "1438207", "1479704", "1354659". Todos estos problemas se solucionan en ONTAP 9.13.1 y versiones posteriores; se recomienda encarecidamente usar una de estas versiones posteriores.	El recopilador de datos está en error, muestra este mensaje de error. “Error: El conector está en estado de error. Nombre del servicio: Auditoría. Motivo del fallo: No se puede configurar la política en SVM_test. Motivo: Falta el valor del campo zapi: Eventos. “
Empiece con una nueva SVM solo con el servicio NFS configurado. Añadir un recopilador de datos de SVM de ONTAP en Workload Security. CIFS se configura como un protocolo permitido para la SVM mientras se añade el recopilador de datos de la SVM de ONTAP en Workload Security. Espere hasta que el recopilador de datos de Workload Security muestre un error. Dado que el servidor CIFS NO está configurado en la SVM, este error, tal como se muestra en la izquierda, se muestra con Workload Security. Edite el recopilador de datos de la SVM de ONTAP y anule la comprobación de CIFS como protocolo permitido. Guarde el recopilador de datos. Empezará a funcionar únicamente con el protocolo NFS habilitado.	El recopilador de datos muestra el mensaje de error: “Error: No se pudo determinar el estado del recopilador en 2 reintentos, intente reiniciar el colector de nuevo (código de error: AGENT008)”.

Si todavía tiene problemas, póngase en contacto con los enlaces de soporte mencionados en la página **Ayuda > Soporte**.

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

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

Configuración del almacenamiento de Cloud Volumes ONTAP

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

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

Plataformas compatibles

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

Configuración de máquina de agente

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

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

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

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

Pasos

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

Instale el agente de seguridad de carga de trabajo

1. Inicie sesión como administrador o propietario de cuenta en su entorno de Cloud Insights.

2. Navegue a Workload Security **Collectors** y haga clic en la pestaña **Agentes**.
3. Haga clic en **+Agent** y especifique RHEL como plataforma de destino.
4. Copie el comando instalación del agente.
5. Pegue el comando Agent Installation en la instancia de RHEL EC2 en la que ha iniciado sesión. De esta forma se instala el agente de seguridad de la carga de trabajo, proporcionando todo el "Requisitos previos del agente" son cumplidos.

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

Resolución de problemas

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

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

Gestión de usuarios

Las cuentas de usuario de Workload Security se gestionan mediante Cloud Insights.

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

Función	Acceso de seguridad de cargas de trabajo
Administrador	Puede realizar todas las funciones de seguridad de carga de trabajo, incluidas las de Alertas, Forensics, recopiladores de datos, directivas de respuesta automatizadas y API para Workload Security. Un administrador también puede invitar a otros usuarios, pero sólo puede asignar funciones de seguridad de carga de trabajo.

Usuario	Puede ver y gestionar alertas y visualizar información forense. El rol de usuario puede cambiar el estado de alerta, añadir una nota, tomar instantáneas manualmente y restringir el acceso de usuario.
Invitado	Puede ver Alertas y Forensics. El rol de invitado no puede cambiar el estado de alerta, agregar una nota, tomar instantáneas manualmente o restringir el acceso de usuario.

Pasos

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

   Se le reenviará a la página Gestión de usuarios de Cloud Insights.

3. Seleccione el rol que desee para cada usuario.

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

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

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

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

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

Exigencias legales:

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

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

Pasos:

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

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

a. Ejecute el siguiente comando:

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

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

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

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

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

Tenga en cuenta lo siguiente:

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

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

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

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

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

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

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

Ejemplo

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

Aplicamos la fórmula:

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

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

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

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

A continuación se muestra un ejemplo de ejecución de script:

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

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

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

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

Resolución de problemas

Pregunta	Responda

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