Começando

Data Infrastructure Insights

NetApp
February 11, 2026

Índice

Começando

Introdução à segurança da carga de trabalho

O Workload Security ajuda você a monitorar a atividade do usuário e detectar possíveis ameaças à segurança em seu ambiente de armazenamento. Antes de iniciar o monitoramento, é necessário configurar agentes, coletores de dados e serviços de diretório para estabelecer a base para um monitoramento de segurança abrangente.

O sistema de segurança de carga de trabalho usa um agente para coletar dados de acesso de sistemas de armazenamento e informações de usuários de servidores de serviços de diretório.

Você precisa configurar o seguinte antes de começar a coletar dados:

Tarefa	Informações relacionadas
Configurar um agente	"Requisitos do agente" "Adicionar agente"
Configurar um conector de diretório de usuário	"Adicionar conector de diretório de usuário"
Configurar coletores de dados	Clique em **Segurança de carga de trabalho > Coletores** Clique no coletor de dados que deseja configurar. Consulte a seção "Referência do Fornecedor do Coletor de Dados" na documentação para obter informações sobre o coletor.
Criar contas de usuários	"Gerenciar contas de usuário"

O Workload Security também pode ser integrado a outras ferramentas. Por exemplo,"veja este guia" sobre integração com o Splunk.

Requisitos do agente de segurança de carga de trabalho

Implante os Agentes de Workload Security em servidores dedicados que atendam aos requisitos mínimos de sistema operacional, CPU, memória e espaço em disco para garantir o desempenho ideal de monitoramento e detecção de ameaças. Este guia especifica os requisitos de hardware e rede necessários antes de "instalando seu Workload Security Agent", incluindo distribuições Linux compatíveis, regras de conectividade de rede e orientações para dimensionamento do sistema.

Componente	Requisitos do Linux
Sistema operacional	Um computador executando uma versão licenciada de um dos seguintes: * AlmaLinux 9.4 (64 bits) a 9.5 (64 bits), 10 (64 bits), incluindo SELinux * CentOS Stream 9 (64 bits) * Debian 11 (64 bits), 12 (64 bits), incluindo 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), incluindo SELinux * Red Hat Enterprise Linux 8.10 (64 bits), 9.1 (64 bits) a 9.6 (64 bits), 10 (64 bits), incluindo SELinux * Rocky 9.4 (64 bits) a 9.6 (64 bits), incluindo SELinux * SUSE Linux Enterprise Server 15 SP4 (64 bits) a 15 SP6 (64 bits), incluindo SELinux * Ubuntu 20.04 LTS (64 bits), 22.04 LTS (64 bits), 24.04 LTS (64 bits) Este computador não deve executar nenhum outro software de nível de aplicativo. Um servidor dedicado é recomendado.
Comandos	'unzip' é necessário para a instalação. Além disso, o comando 'sudo su –' é necessário para instalação, execução de scripts e desinstalação.
CPU	4 núcleos de CPU
Memória	16 GB de RAM
Espaço em disco disponível	O espaço em disco deve ser alocado desta maneira: /opt/netapp 36 GB (mínimo de 35 GB de espaço livre após a criação do sistema de arquivos) Observação: é recomendável alocar um pouco mais de espaço em disco para permitir a criação do sistema de arquivos. Certifique-se de que haja pelo menos 35 GB de espaço livre no sistema de arquivos. Se /opt for uma pasta montada de um armazenamento NAS, certifique-se de que os usuários locais tenham acesso a essa pasta. O agente ou o coletor de dados pode falhar na instalação se os usuários locais não tiverem permissão para esta pasta. veja o"solução de problemas" seção para mais detalhes.
Rede	Conexão Ethernet de 100 Mbps a 1 Gbps, endereço IP estático, conectividade IP para todos os dispositivos e uma porta necessária para a instância do Workload Security (80 ou 443).

Observação: o agente do Workload Security pode ser instalado na mesma máquina que uma unidade de aquisição e/ou agente do Data Infrastructure Insights . No entanto, é uma prática recomendada instalá-los em máquinas separadas. Caso eles estejam instalados na mesma máquina, aloque espaço em disco conforme mostrado abaixo:

Espaço em disco disponível	50-55 GB Para Linux, o espaço em disco deve ser alocado desta maneira: /opt/netapp 25-30 GB /var/log/netapp 25 GB

Recomendações adicionais

- É altamente recomendável sincronizar o horário no sistema ONTAP e na máquina do agente usando **Network Time Protocol (NTP)** ou **Simple Network Time Protocol (SNTP)**.

Regras de acesso à rede em nuvem

Para ambientes de segurança de carga de trabalho **baseados nos EUA**:

Protocolo	Porta	Fonte	Destino	Descrição
TCP	443	Agente de Segurança de Carga de Trabalho	<nome_do_site>.cs01.cloudinsights.netapp.com <nome_do_site>.c01.cloudinsights.netapp.com <nome_do_site>.c02.cloudinsights.netapp.com	Acesso a Data Infrastructure Insights
TCP	443	Agente de Segurança de Carga de Trabalho	agentlogin.cs01.cloudinsights.netapp.com	Acesso a serviços de autenticação

Para ambientes de segurança de carga de trabalho **baseados na Europa**:

Protocolo	Porta	Fonte	Destino	Descrição
TCP	443	Agente de Segurança de Carga de Trabalho	<nome_do_site>.cs01-eu-1.cloudinsights.netapp.com <nome_do_site>.c01-eu-1.cloudinsights.netapp.com <nome_do_site>.c02-eu-1.cloudinsights.netapp.com	Acesso a Data Infrastructure Insights
TCP	443	Agente de Segurança de Carga de Trabalho	agentlogin.cs01-eu-1.cloudinsights.netapp.com	Acesso a serviços de autenticação

Para ambientes de segurança de carga de trabalho **baseados em APAC**:

Protocolo	Porta	Fonte	Destino	Descrição
TCP	443	Agente de Segurança de Carga de Trabalho	<nome_do_site>.cs01-ap-1.cloudinsights.netapp.com <nome_do_site>.c01-ap-1.cloudinsights.netapp.com <nome_do_site>.c02-ap-1.cloudinsights.netapp.com	Acesso a Data Infrastructure Insights
TCP	443	Agente de Segurança de Carga de Trabalho	agentlogin.cs01-ap-1.cloudinsights.netapp.com	Acesso a serviços de autenticação

Regras na rede

Protocolo	Porta	Fonte	Destino	Descrição
TCP	389(LDAP) 636 (LDAPs / start-tls)	Agente de Segurança de Carga de Trabalho	URL do servidor LDAP	Conectar ao LDAP
TCP	443	Agente de Segurança de Carga de Trabalho	Endereço IP de gerenciamento de cluster ou SVM (dependendo da configuração do coletor SVM)	Comunicação de API com ONTAP

Protocolo	Porta	Fonte	Destino	Descrição
TCP	35000 - 55000	Endereços IP LIF de dados SVM	Agente de Segurança de Carga de Trabalho	Comunicação do ONTAP com o Agente de Segurança de Carga de Trabalho para eventos Fpolicy. Essas portas devem ser abertas para o Agente de Segurança de Carga de Trabalho para que o ONTAP envie eventos para ele, incluindo qualquer firewall no próprio Agente de Segurança de Carga de Trabalho (se presente). OBSERVAÇÃO: você não precisa reservar **todas** essas portas, mas as portas que você reservar para isso devem estar dentro desse intervalo. É recomendável começar reservando ~100 portas e aumentar se necessário.

Protocolo	Porta	Fonte	Destino	Descrição
TCP	35000-55000	IP de gerenciamento de cluster	Agente de Segurança de Carga de Trabalho	Comunicação do IP de gerenciamento de cluster do ONTAP com o agente de segurança de carga de trabalho para **eventos EMS**. Essas portas devem ser abertas para o Agente de Segurança de Carga de Trabalho para que o ONTAP envie **eventos EMS** para ele, incluindo qualquer firewall no próprio Agente de Segurança de Carga de Trabalho (se presente). OBSERVAÇÃO: você não precisa reservar **todas** essas portas, mas as portas que você reservar para isso devem estar dentro desse intervalo. É recomendável começar reservando ~100 portas e aumentar se necessário.
SSH	22	Agente de Segurança de Carga de Trabalho	Gerenciamento de cluster	Necessário para bloqueio de usuários CIFS/SMB.

Dimensionamento do sistema

Veja o"Verificador de Taxa de Eventos" documentação para obter informações sobre dimensionamento.

Implantar Agentes de Segurança de Carga de Trabalho

Os agentes de segurança de carga de trabalho são essenciais para monitorar a atividade do usuário e detectar possíveis ameaças à segurança em toda a sua infraestrutura de armazenamento. Este guia fornece instruções de instalação passo a passo, melhores práticas para gerenciamento de agentes (incluindo recursos de pausa/retomada e fixação/desfixação) e requisitos de configuração pós-implantação. Antes de começar,

certifique-se de que seu servidor de agentes atenda aos requisitos. "requisitos do sistema".

Antes de começar

- O privilégio sudo é necessário para instalação, execução de scripts e desinstalação.
- Ao instalar o agente, um usuário local *cssys* e um grupo local *cssys* são criados na máquina. Se as configurações de permissão não permitirem a criação de um usuário local e, em vez disso, exigirem o Active Directory, um usuário com o nome de usuário *cssys* deverá ser criado no servidor Active Directory.
- Você pode ler sobre a segurança do Data Infrastructure Insights"aqui" .

Melhores práticas

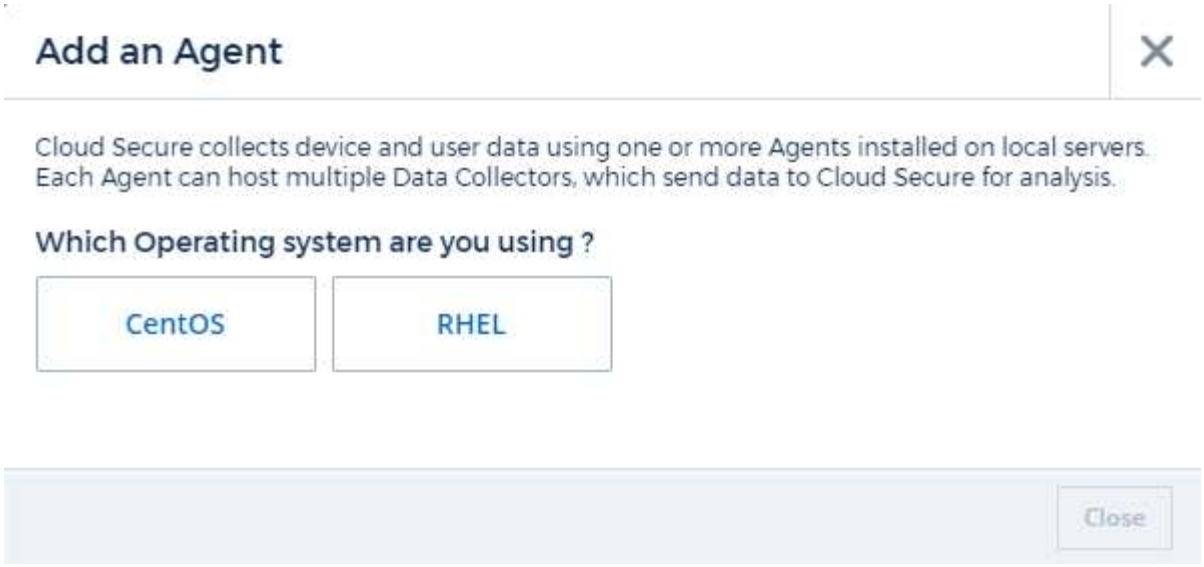
Antes de configurar seu agente do Workload Security, leve em consideração o seguinte.

Pausar e retomar	Pausa: Remove as políticas do ONTAP. Normalmente utilizado quando os clientes realizam atividades de manutenção prolongadas que podem levar um tempo considerável, como reinicializações de máquinas virtuais de agentes ou substituições de armazenamento. Resumo: Adiciona fpolicies de volta ao ONTAP.
Fixar e desafixar	O Unpin busca imediatamente a versão mais recente (se disponível) e atualiza o agente e o coletor. Durante esta atualização, o fpolicies será desconectado e reconectado. Essa funcionalidade foi desenvolvida para clientes que desejam controlar o momento das atualizações automáticas. Veja abaixo parainstruções de fixação/desfixação .
Abordagem recomendada	Para configurações grandes, é aconselhável usar Pin e Unpin em vez de pausar os coletores. Não é necessário pausar e retomar ao usar as funções de fixar e desafixar. Os clientes podem manter seus agentes e coletores atualizados e, ao receberem uma notificação por e-mail sobre uma nova versão, têm um prazo de 30 dias para atualizar os agentes seletivamente, um por um. Essa abordagem minimiza o impacto da latência nas fpolicies e proporciona maior controle sobre o processo de atualização.

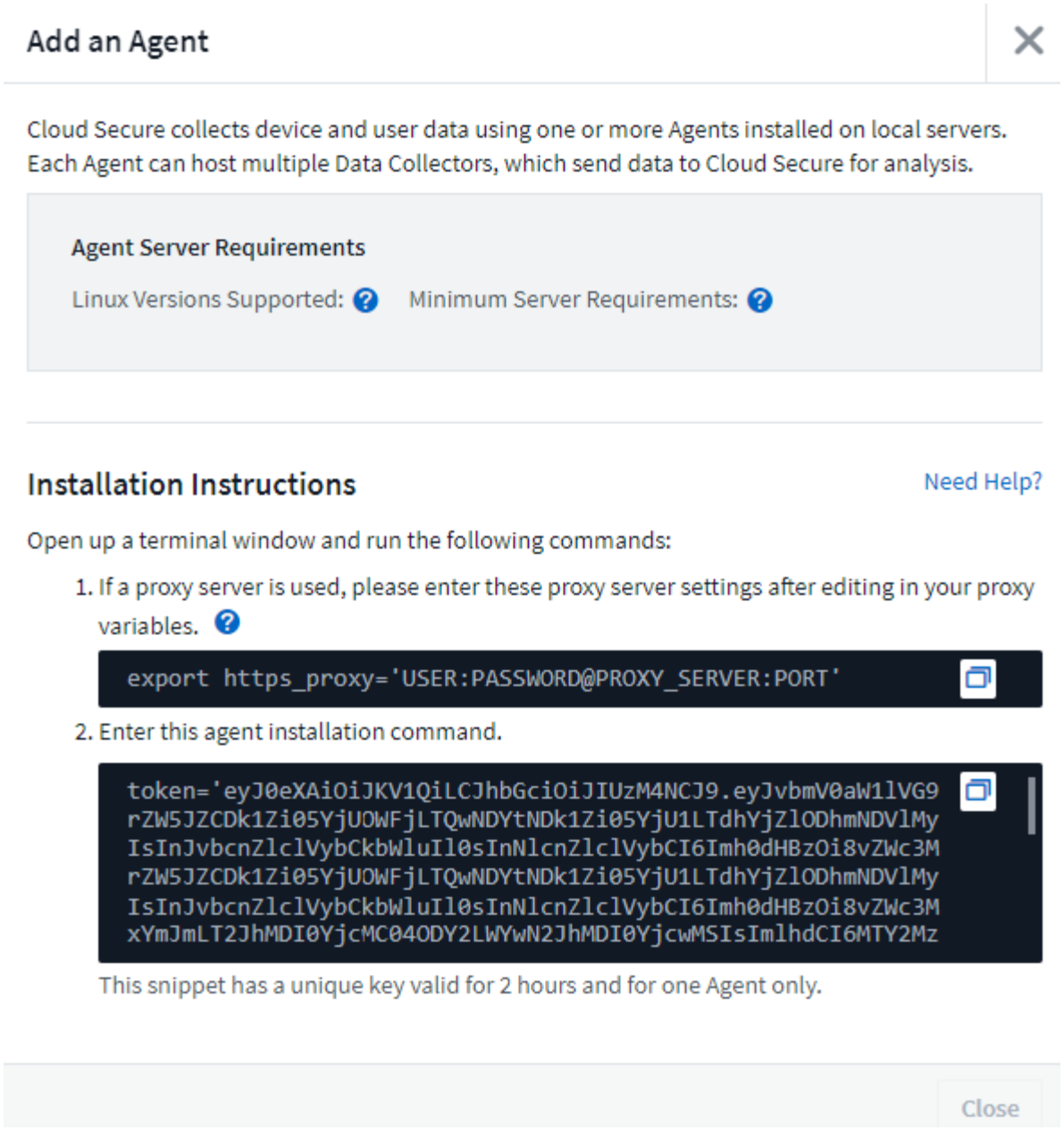
Etapas para instalar o agente

1. Efetue login como Administrador ou Proprietário da conta no seu ambiente de segurança de carga de trabalho.
2. Selecione **Colecionadores > Agentes > +Agente**

   O sistema exibe a página Adicionar um Agente:



3. Verifique se o servidor do agente atende aos requisitos mínimos do sistema.
4. Para verificar se o servidor do agente está executando uma versão compatível do Linux, clique em *Versões compatíveis (i)*.
5. Se sua rede estiver usando um servidor proxy, defina os detalhes do servidor proxy seguindo as instruções na seção Proxy.



6. Clique no ícone Copiar para a área de transferência para copiar o comando de instalação.
7. Execute o comando de instalação em uma janela de terminal.
8. O sistema exibe a seguinte mensagem quando a instalação é concluída com sucesso:

Depois que você terminar

1. Você precisa configurar um"Coletor de diretório de usuário" .
2. Você precisa configurar um ou mais coletores de dados.

Configuração de rede

Execute os seguintes comandos no sistema local para abrir portas que serão usadas pelo Workload Security. Se houver uma preocupação de segurança em relação ao intervalo de portas, você pode usar um intervalo de portas menor, por exemplo, *35000:35100*. Cada SVM usa duas portas.

Passos

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

Siga os próximos passos de acordo com sua plataforma:

CentOS 7.x / RHEL 7.x:

1. `sudo iptables-save | grep 35000`

Saída de exemplo:

```
 -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)

Saída de exemplo:

```
35000-55000/tcp
```

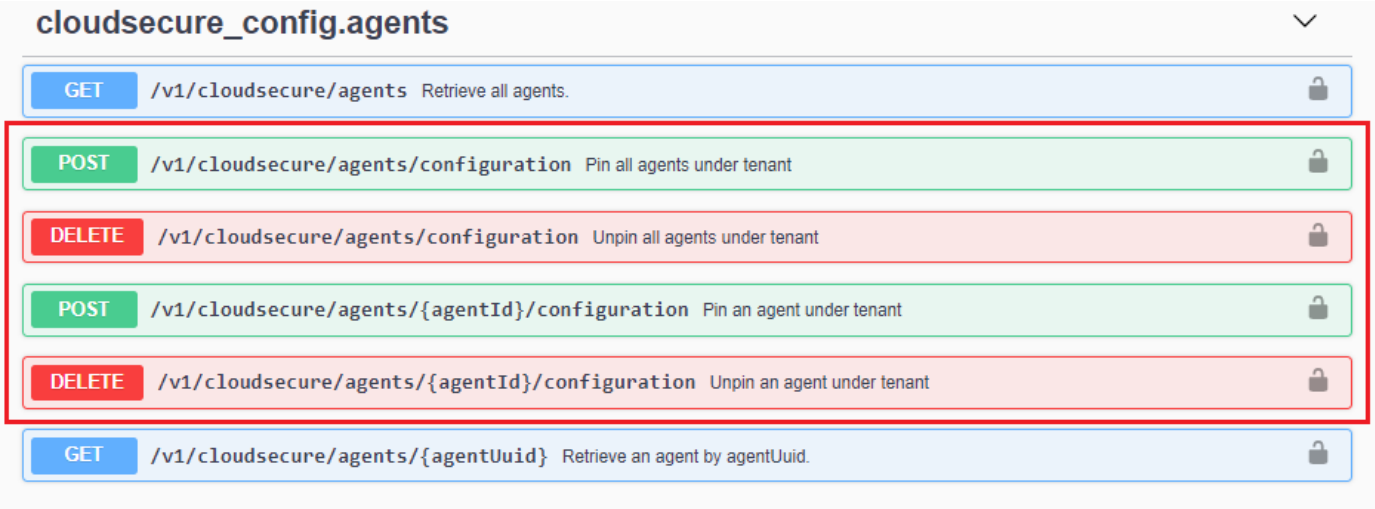
"Fixando" um Agente na versão atual

Por padrão, o Data Infrastructure Insights Workload Security atualiza os agentes automaticamente. Alguns clientes podem querer pausar a atualização automática, o que deixa um Agente em sua versão atual até que ocorra uma das seguintes situações:

- O cliente retoma as atualizações automáticas do Agente.
- 30 dias se passaram. Observe que os 30 dias começam no dia da atualização mais recente do Agente, não no dia em que o Agente é pausado.

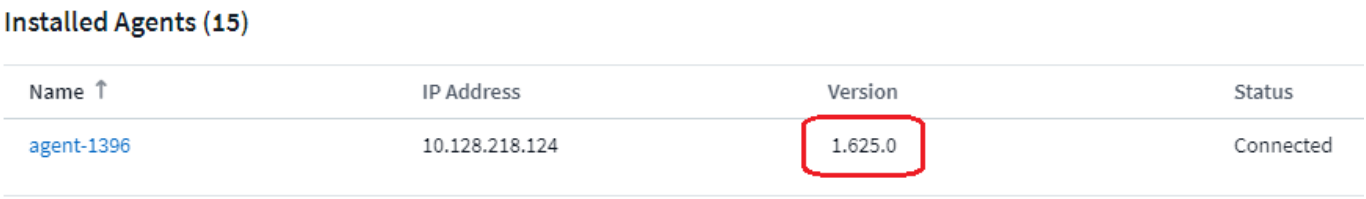
Em cada um desses casos, o agente será atualizado na próxima atualização do Workload Security.

Para pausar ou retomar atualizações automáticas do agente, use as APIs *cloudsecure_config.agents*:



Observe que pode levar até cinco minutos para que a ação de pausa ou retomada entre em vigor.

Você pode visualizar as versões atuais do seu agente na página **Segurança da carga de trabalho > Coletores**, na guia **Agentes**.



Solução de problemas de erros do agente

Problemas conhecidos e suas soluções são descritos na tabela a seguir.

Problema:	Resolução:
A instalação do agente falha ao criar a pasta /opt/netapp/cloudsecure/agent/logs/agent.log e o arquivo install.log não fornece informações relevantes.	Este erro ocorre durante a inicialização do agente. O erro não é registrado nos arquivos de log porque ocorre antes do logger ser inicializado. O erro é redirecionado para a saída padrão e fica visível no log de serviço usando o `journalctl -u cloudsecure-agent.service` comando. Este comando pode ser usado para solucionar o problema posteriormente.
A instalação do agente falha com 'Esta distribuição Linux não é suportada. Saindo da instalação'.	Este erro aparece quando você tenta instalar o Agente em um sistema não suportado. Ver "Requisitos do agente" .
A instalação do agente falhou com o erro: "-bash: unzip: comando não encontrado"	Instale, descompacte e execute o comando de instalação novamente. Se o Yum estiver instalado na máquina, tente “yum install unzip” para instalar o software de descompactação. Depois disso, copie novamente o comando da interface de instalação do agente e cole-o na CLI para executar a instalação novamente.

Problema:	Resolução:
O agente foi instalado e estava em execução. No entanto, o agente parou de repente.	SSH para a máquina do agente. Verifique o status do serviço do agente através de `sudo systemctl status cloudsecure-agent.service` . 1. Verifique se os logs mostram a mensagem “Falha ao iniciar o serviço daemon do Workload Security”. 2. Verifique se o usuário cssys existe na máquina do agente ou não. Execute os seguintes comandos um por um com permissão de root e verifique se o usuário e o grupo cssys existem. `sudo id cssys` `sudo groups cssys` 3. Se não houver nenhuma, uma política de monitoramento centralizada pode ter excluído o usuário cssys. 4. Crie o usuário e o grupo cssys manualmente executando os seguintes comandos. `sudo useradd cssys` `sudo groupadd cssys` 5. Reinicie o serviço do agente depois disso executando o seguinte comando: `sudo systemctl restart cloudsecure-agent.service` 6. Se ainda não estiver funcionando, verifique as outras opções de solução de problemas.
Não é possível adicionar mais de 50 coletores de dados a um agente.	Apenas 50 coletores de dados podem ser adicionados a um agente. Isso pode ser uma combinação de todos os tipos de coletores, por exemplo, Active Directory, SVM e outros coletores.
A interface do usuário mostra que o agente está no estado NOT_CONNECTED.	Etapas para reiniciar o Agente. 1. SSH para a máquina do agente. 2. Reinicie o serviço do agente depois disso executando o seguinte comando: `sudo systemctl restart cloudsecure-agent.service` 3. Verifique o status do serviço do agente através de `sudo systemctl status cloudsecure-agent.service` . 4. O agente deve ir para o estado CONECTADO.
A VM do agente está atrás do proxy Zscaler e a instalação do agente está falhando. Devido à inspeção SSL do proxy Zscaler, os certificados de segurança da carga de trabalho são apresentados como assinados pela CA do Zscaler, portanto, o agente não confia na comunicação.	Desabilite a inspeção SSL no proxy Zscaler para a URL *.cloudinsights.netapp.com. Se o Zscaler fizer a inspeção SSL e substituir os certificados, o Workload Security não funcionará.

Problema:	Resolução:
Ao instalar o agente, a instalação trava após a descompactação.	O comando “chmod 755 -Rf” está falhando. O comando falha quando o comando de instalação do agente está sendo executado por um usuário sudo não root que tem arquivos no diretório de trabalho pertencentes a outro usuário, e as permissões desses arquivos não podem ser alteradas. Devido à falha do comando chmod, o restante da instalação não é executado. 1. Crie um novo diretório chamado “cloudsecure”. 2. Vá até esse diretório. 3. Copie e cole o comando de instalação completo “token=…… … ./cloudsecure-agent-install.sh” e pressione Enter. 4. A instalação deve poder prosseguir.
Se o agente ainda não conseguir se conectar ao SaaS, abra um caso com o Suporte da NetApp . Forneça o número de série do Data Infrastructure Insights para abrir um caso e anexe logs ao caso, conforme observado.	Para anexar logs ao caso: 1. Execute o seguinte script com permissão de root e compartilhe o arquivo de saída (cloudsecure-agent-symptoms.zip). a. /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh 2. Execute os seguintes comandos um por um com permissão de root e compartilhe a saída. a. id cssys b. groups cssys c. cat /etc/os-release
O script cloudsecure-agent-symptom-collector.sh falha com o seguinte erro. [root@machine tmp]# /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh Coletando log de serviço Coletando logs de aplicativo Coletando configurações de agente Tirando instantâneo de status de serviço Tirando instantâneo da estrutura de diretório do agente ……. ……. /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh: linha 52: zip: comando não encontrado ERRO: Falha ao criar /tmp/cloudsecure-agent-symptoms.zip	A ferramenta Zip não está instalada. Instale a ferramenta zip executando o comando “yum install zip”. Em seguida, execute o cloudsecure-agent-symptom-collector.sh novamente.
A instalação do agente falha com useradd: não é possível criar o diretório /home/cssys	Este erro pode ocorrer se o diretório de login do usuário não puder ser criado em /home, devido à falta de permissões. A solução alternativa seria criar um usuário cssys e adicionar seu diretório de login manualmente usando o seguinte comando: *sudo useradd user_name -m -d HOME_DIR* -m :Cria o diretório inicial do usuário se ele não existir. -d: O novo usuário é criado usando HOME_DIR como valor para o diretório de login do usuário. Por exemplo, *sudo useradd cssys -m -d /cssys*, adiciona um usuário *cssys* e cria seu diretório de login como root.

Problema:	Resolução:
O agente não está em execução após a instalação. *Systemctl status cloudsecure-agent.service* mostra o seguinte: [root@demo ~]# systemctl status cloudsecure-agent.service agent.service – Serviço Daemon do Agente de Segurança de Carga de Trabalho Carregado: carregado (/usr/lib/systemd/system/cloudsecure-agent.service; habilitado; predefinição do fornecedor: desabilitada) Ativo: ativando (reinicialização automática) (Resultado: código de saída) desde ter 2021-08-03 21:12:26 PDT; 2s atrás Processo: 25889 ExecStart=/bin/bash /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent (código=exited status=126) PID principal: 25889 (código=exited, status=126), 03 de agosto 21:12:26 demo systemd[1]: cloudsecure-agent.service: processo principal saiu, código=exited, status=126/n/a 03 de agosto 21:12:26 demo systemd[1]: Unidade cloudsecure-agent.service entrou em estado de falha. 03 de agosto 21:12:26 demo systemd[1]: cloudsecure-agent.service falhou.	Isso pode estar falhando porque o usuário *cssys* pode não ter permissão para instalar. Se /opt/netapp for uma montagem NFS e se o usuário *cssys* não tiver acesso a esta pasta, a instalação falhará. *cssys* é um usuário local criado pelo instalador do Workload Security que pode não ter permissão para acessar o compartilhamento montado. Você pode verificar isso tentando acessar /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent usando o usuário *cssys*. Se retornar “Permissão negada”, a permissão de instalação não está presente. Em vez de uma pasta montada, instale em um diretório local da máquina.
O agente foi conectado inicialmente por meio de um servidor proxy e o proxy foi definido durante a instalação do agente. Agora o servidor proxy mudou. Como a configuração de proxy do Agente pode ser alterada?	Você pode editar o agent.properties para adicionar os detalhes do proxy. Siga estes passos: 1. Mude para a pasta que contém o arquivo de propriedades: cd /opt/netapp/cloudsecure/conf 2. Usando seu editor de texto favorito, abra o arquivo *agent.properties* para edição. 3. Adicione ou modifique as seguintes linhas: AGENT_PROXY_HOST=scspa1950329001.vm.netapp.com AGENT_PROXY_PORT=80 AGENT_PROXY_USER=pxuser AGENT_PROXY_PASSWORD=pass1234 4. Salve o arquivo. 5. Reinicie o agente: sudo systemctl restart cloudsecure-agent.service

Excluindo um agente de segurança de carga de trabalho

Quando você exclui um Agente de Segurança de Carga de Trabalho, todos os coletores de dados associados ao Agente devem ser excluídos primeiro.

Excluindo um Agente

A exclusão de um Agente exclui todos os Coletores de Dados associados ao Agente. Se você planeja configurar os coletores de dados com um agente diferente, crie um backup das configurações do Coletor de Dados antes de excluir o Agente.

Antes de começar

1. Certifique-se de que todos os coletores de dados associados ao agente sejam excluídos do portal de segurança de carga de trabalho.

   Observação: ignore esta etapa se todos os coletores associados estiverem no estado PARADO.

Etapas para excluir um agente:

1. Faça SSH na VM do agente e execute o seguinte comando. Quando solicitado, digite "y" para continuar.

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

2. Clique em **Segurança de Carga de Trabalho > Coletores > Agentes**

   O sistema exibe a lista de Agentes configurados.

3. Clique no menu de opções do Agente que você está excluindo.
4. Clique em **Excluir**.

   O sistema exibe a página **Excluir Agente**.

5. Clique em **Excluir** para confirmar a exclusão.

Configurando um coletor de diretório de usuário do Active Directory (AD)

O Workload Security pode ser configurado para coletar atributos de usuário de servidores do Active Directory.

Antes de começar

- Você deve ser um administrador ou proprietário da conta do Data Infrastructure Insights para executar esta tarefa.
- Você deve ter o endereço IP do servidor que hospeda o servidor do Active Directory.
- Um agente deve ser configurado antes de você configurar um conector de diretório de usuários.

Etapas para configurar um coletor de diretório de usuário

1. No menu Segurança de Carga de Trabalho, clique em: **Coletores > Coletores de Diretório de Usuário > + Coletor de Diretório de Usuário** e selecione **Active Directory**

   O sistema exibe a tela Adicionar Diretório de Usuário.

Configure o Coletor de Diretório do Usuário inserindo os dados necessários nas seguintes tabelas:

Nome	Descrição
Nome	Nome exclusivo para o diretório do usuário. Por exemplo *GlobalADCollector*
Agente	Selecione um agente configurado na lista
IP do servidor/nome de domínio	Endereço IP ou Nome de Domínio Totalmente Qualificado (FQDN) do servidor que hospeda o diretório ativo

Nome da Floresta	Nível de floresta da estrutura de diretório. O nome da floresta permite ambos os formatos a seguir: *x.y.z* ⇒ nome de domínio direto como você tem no seu SVM. [Exemplo: hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ Nomes distintos relativos [Exemplo: DC=hq,DC=companyname,DC=com] Ou você pode especificar como o seguinte: *OU=engineering,DC=hq,DC=companyname,DC=com* [para filtrar por engenharia de UO específica] *CN=username,OU=engineering,DC=companyname, DC=netapp, DC=com* [para obter apenas um usuário específico com <username> da UO <engineering>] *CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com ,O= companyname,L=Boston,S=MA,C=US* [para obter todos os usuários do Acrobat dentro dos usuários dessa organização] Domínios confiáveis do Active Directory também são suportados.
Vincular DN	Usuário autorizado a pesquisar no diretório. Por exemplo: *nomedeusuário@nomedaempresa.com* ou *nomedeusuário@nomedodomínio.com* Além disso, é necessária a permissão Somente Leitura do Domínio. O usuário deve ser membro do grupo de segurança *Controladores de domínio somente leitura*.
Senha BIND	Senha do servidor de diretório (ou seja, senha para nome de usuário usado no Bind DN)
Protocolo	ldap, ldaps, ldap-start-tls
Portos	Selecione a porta

Insira os seguintes atributos obrigatórios do Directory Server se os nomes de atributos padrão tiverem sido modificados no Active Directory. Na maioria das vezes, esses nomes de atributos *não* são modificados no Active Directory. Nesse caso, você pode simplesmente prosseguir com o nome de atributo padrão.

Atributos	Nome do atributo no servidor de diretório
Nome de exibição	nome
SID	objetosid
Nome de usuário	sAMAccountName

Clique em Incluir atributos opcionais para adicionar qualquer um dos seguintes atributos:

Atributos	Nome do atributo no servidor de diretório
Endereço de email	correspondência
Número de telefone	número de telefone
Papel	título
País	co
Estado	estado

Departamento	departamento
Foto	foto em miniatura
GerenteDN	gerente
Grupos	membro de

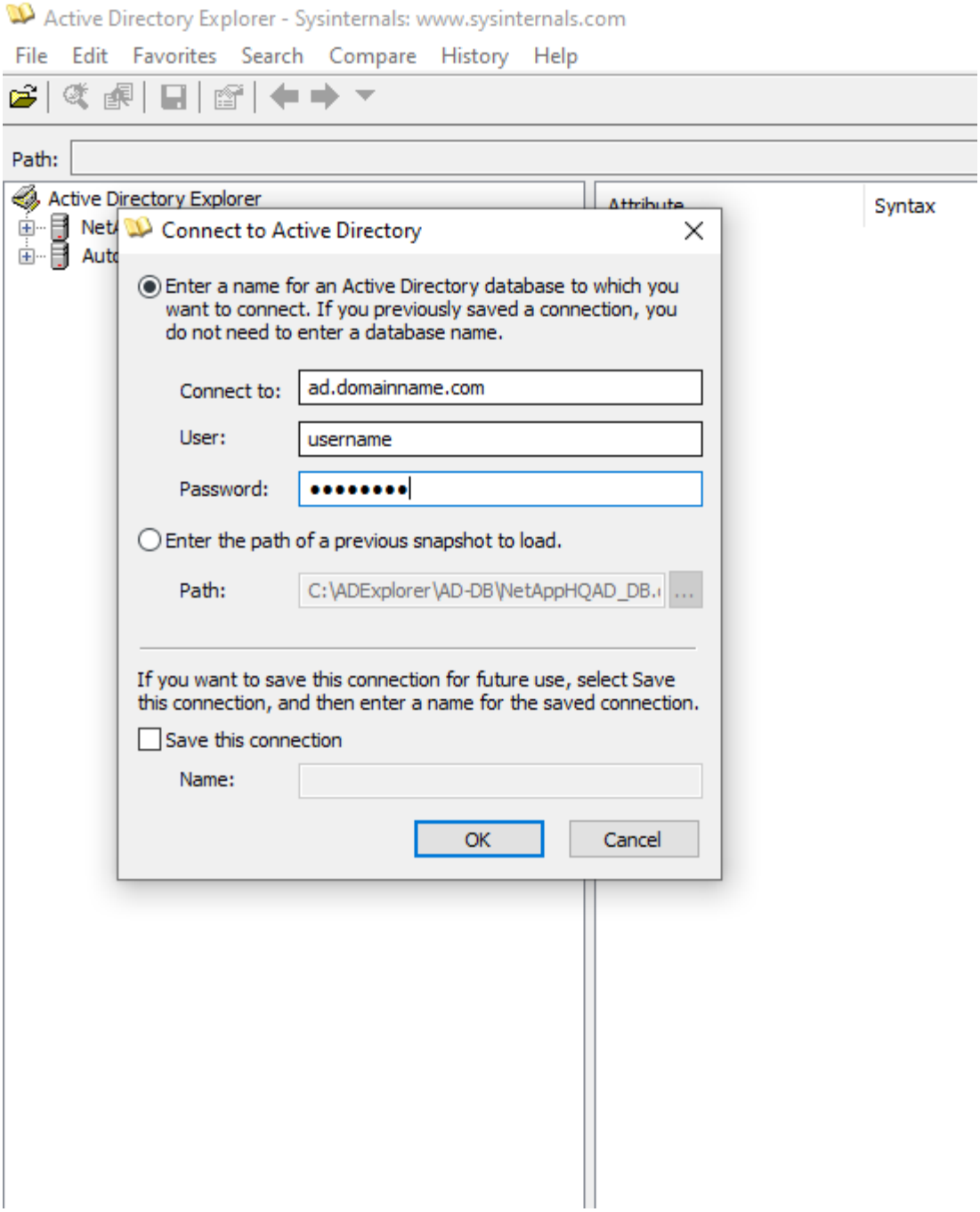
Testando a configuração do coletor de diretório do usuário

Você pode validar permissões de usuário LDAP e definições de atributos usando os seguintes procedimentos:

- Use o seguinte comando para validar a permissão do usuário LDAP do 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
```

- Use o AD Explorer para navegar em um banco de dados do AD, visualizar propriedades e atributos de objetos, visualizar permissões, visualizar o esquema de um objeto e executar pesquisas sofisticadas que você pode salvar e executar novamente.
  - Instalar"Explorador de anúncios" em qualquer máquina Windows que possa se conectar ao servidor AD.
  - Conecte-se ao servidor AD usando o nome de usuário/senha do servidor de diretório do AD.



Solução de problemas de erros de configuração do coletor de diretório de usuário

A tabela a seguir descreve problemas conhecidos e soluções que podem ocorrer durante a configuração do coletor:

Problema:	Resolução:
Adicionar um conector de diretório de usuário resulta no estado "Erro". O erro diz: “Credenciais inválidas fornecidas para o servidor LDAP”.	Nome de usuário ou senha fornecidos incorretos. Edite e forneça o nome de usuário e a senha corretos.

Problema:	Resolução:
Adicionar um conector de diretório de usuário resulta no estado "Erro". O erro diz: “Falha ao obter o objeto correspondente a DN=DC=hq,DC=domainname,DC=com fornecido como nome da floresta”.	Nome de floresta incorreto fornecido. Edite e forneça o nome correto da floresta.
Os atributos opcionais do usuário do domínio não estão aparecendo na página Perfil do usuário do Workload Security.	Isso provavelmente ocorre devido a uma incompatibilidade entre os nomes dos atributos opcionais adicionados no CloudSecure e os nomes dos atributos reais no Active Directory. Edite e forneça o(s) nome(s) correto(s) do(s) atributo(s) opcional(is).
Coletor de dados em estado de erro com "Falha ao recuperar usuários LDAP. Motivo da falha: Não é possível conectar no servidor, a conexão é nula"	Reinicie o coletor clicando no botão *Reiniciar*.
Adicionar um conector de diretório de usuário resulta no estado "Erro".	Certifique-se de ter fornecido valores válidos para os campos obrigatórios (Servidor, nome da floresta, DN de vinculação, Senha de vinculação). Certifique-se de que a entrada bind-DN seja sempre fornecida como 'Administrador@<nome_da_floresta_de_domínio>' ou como uma conta de usuário com privilégios de administrador de domínio.
Adicionar um conector de diretório de usuário resulta no estado 'RETENTANDO'. Exibe o erro “Não foi possível definir o estado do coletor, motivo pelo qual o comando TCP [Connect(localhost:35012,None,List(),Some(,seconds),true)] falhou devido a java.net.ConnectionException:Connection refused.”	IP ou FQDN incorreto fornecido para o servidor AD. Edite e forneça o endereço IP ou FQDN correto.
Adicionar um conector de diretório de usuário resulta no estado "Erro". O erro diz: “Falha ao estabelecer conexão LDAP”.	IP ou FQDN incorreto fornecido para o servidor AD. Edite e forneça o endereço IP ou FQDN correto.
Adicionar um conector de diretório de usuário resulta no estado "Erro". O erro diz: “Falha ao carregar as configurações. Motivo: A configuração da fonte de dados tem um erro. Motivo específico: /connector/conf/application.conf: 70: ldap.ldap-port tem o tipo STRING em vez de NUMBER”	Valor incorreto fornecido para a Porta. Tente usar os valores de porta padrão ou o número de porta correto para o servidor AD.
Comecei com os atributos obrigatórios e funcionou. Após adicionar os opcionais, os dados dos atributos opcionais não estão sendo buscados do AD.	Isso provavelmente ocorre devido a uma incompatibilidade entre os atributos opcionais adicionados no CloudSecure e os nomes de atributos reais no Active Directory. Edite e forneça o nome correto do atributo obrigatório ou opcional.
Após reiniciar o coletor, quando a sincronização do AD ocorrerá?	A sincronização do AD ocorrerá imediatamente após a reinicialização do coletor. Levará aproximadamente 15 minutos para buscar dados de aproximadamente 300 mil usuários e será atualizado automaticamente a cada 12 horas.

Problema:	Resolução:
Os dados do usuário são sincronizados do AD para o CloudSecure. Quando os dados serão excluídos?	Os dados do usuário são retidos por 13 meses caso não haja atualização. Se o inquilino for excluído, os dados serão excluídos.
O conector do diretório do usuário resulta no estado 'Erro'. "O conector está em estado de erro. Nome do serviço: usersLdap. Motivo da falha: Falha ao recuperar usuários LDAP. Motivo da falha: 80090308: LdapErr: DSID-0C090453, comentário: erro AcceptSecurityContext, dados 52e, v3839"	Nome de floresta incorreto fornecido. Veja acima como fornecer o nome correto da floresta.
O número de telefone não está sendo preenchido na página de perfil do usuário.	Isso provavelmente ocorre devido a um problema de mapeamento de atributos com o Active Directory. 1. Edite o coletor específico do Active Directory que está buscando as informações do usuário do Active Directory. 2. Observe que, nos atributos opcionais, há um campo chamado “Número de telefone” mapeado para o atributo 'telephonenumber' do Active Directory. 4. Agora, use a ferramenta Active Directory Explorer conforme descrito acima para navegar no Active Directory e ver o nome do atributo correto. 3. Certifique-se de que no Active Directory haja um atributo chamado 'telephonenumber' que realmente tenha o número de telefone do usuário. 5. Digamos que no Active Directory ele foi modificado para 'phonenumber'. 6. Em seguida, edite o coletor do diretório de usuários do CloudSecure. Na seção de atributos opcionais, substitua 'telephonenumber' por 'phonenumber'. 7. Salve o coletor do Active Directory, o coletor será reiniciado e obterá o número de telefone do usuário e o exibirá na página de perfil do usuário.
Se o certificado de criptografia (SSL) estiver habilitado no servidor Active Directory (AD), o Workload Security User Directory Collector não poderá se conectar ao servidor AD.	Desabilite a criptografia do servidor AD antes de configurar um coletor de diretório de usuário. Depois que os detalhes do usuário forem obtidos, eles permanecerão lá por 13 meses. Se o servidor AD for desconectado após a busca dos detalhes do usuário, os usuários recém-adicionados no AD não serão buscados. Para buscar novamente, o coletor de diretório do usuário precisa estar conectado ao AD.
Os dados do Active Directory estão presentes no CloudInsights Security. Deseja excluir todas as informações do usuário do CloudInsights.	Não é possível excluir SOMENTE informações de usuários do Active Directory do CloudInsights Security. Para excluir o usuário, o locatário completo precisa ser excluído.

Configurando um coletor de servidor de diretório LDAP

Configure o Workload Security para coletar atributos de usuário de servidores de diretório LDAP.

Antes de começar

- Você deve ser um administrador ou proprietário da conta do Data Infrastructure Insights para executar esta tarefa.
- Você deve ter o endereço IP do servidor que hospeda o servidor do diretório LDAP.
- Um agente deve ser configurado antes de você configurar um conector de diretório LDAP.

Etapas para configurar um coletor de diretório de usuário

1. No menu Segurança de Carga de Trabalho, clique em: **Coletores > Coletores de Diretório de Usuário > + Coletor de Diretório de Usuário** e selecione **Servidor de Diretório LDAP**

   O sistema exibe a tela Adicionar Diretório de Usuário.

Configure o Coletor de Diretório do Usuário inserindo os dados necessários nas seguintes tabelas:

Nome	Descrição
Nome	Nome exclusivo para o diretório do usuário. Por exemplo *GlobalLDAPCollector*
Agente	Selecione um agente configurado na lista
IP do servidor/nome de domínio	Endereço IP ou Nome de Domínio Totalmente Qualificado (FQDN) do servidor que hospeda o Servidor de Diretório LDAP
Base de Pesquisa	Base de pesquisa do servidor LDAP A Base de pesquisa permite ambos os formatos a seguir: *x.y.z* ⇒ nome de domínio direto como você tem no seu SVM. [Exemplo: hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ Nomes distintos relativos [Exemplo: DC=hq,DC=companyname,DC=com] Ou você pode especificar como o seguinte: *OU=engineering,DC=hq,DC=companyname,DC=com* [para filtrar por engenharia de UO específica] *CN=username,OU=engineering,DC=companyname, DC=netapp, DC=com* [para obter apenas um usuário específico com <username> da UO <engineering>] *CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com ,O= companyname,L=Boston,S=MA,C=US* [para obter todos os usuários do Acrobat dentro dos usuários dessa organização]
Vincular DN	Usuário autorizado a pesquisar no diretório. Por exemplo: 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 um usuário john@dorp.company.com. dorp.company.com
--contas	--Usuários
--John	--Anna
Senha BIND	Senha do servidor de diretório (ou seja, senha para nome de usuário usado no Bind DN)

Protocolo	ldap, ldaps, ldap-start-tls
Portos	Selecione a porta

Insira os seguintes atributos obrigatórios do Directory Server se os nomes de atributos padrão tiverem sido modificados no Directory Server LDAP. Na maioria das vezes, esses nomes de atributos *não* são modificados no Servidor de Diretório LDAP. Nesse caso, você pode simplesmente prosseguir com o nome de atributo padrão.

Atributos	Nome do atributo no servidor de diretório
Nome de exibição	nome
UNIXID	número de identificação
Nome de usuário	uid

Clique em Incluir atributos opcionais para adicionar qualquer um dos seguintes atributos:

Atributos	Nome do atributo no servidor de diretório
Endereço de email	correspondência
Número de telefone	número de telefone
Papel	título
País	co
Estado	estado
Departamento	número do departamento
Foto	foto
GerenteDN	gerente
Grupos	membro de

Testando a configuração do coletor de diretório do usuário

Você pode validar permissões de usuário LDAP e definições de atributos usando os seguintes procedimentos:

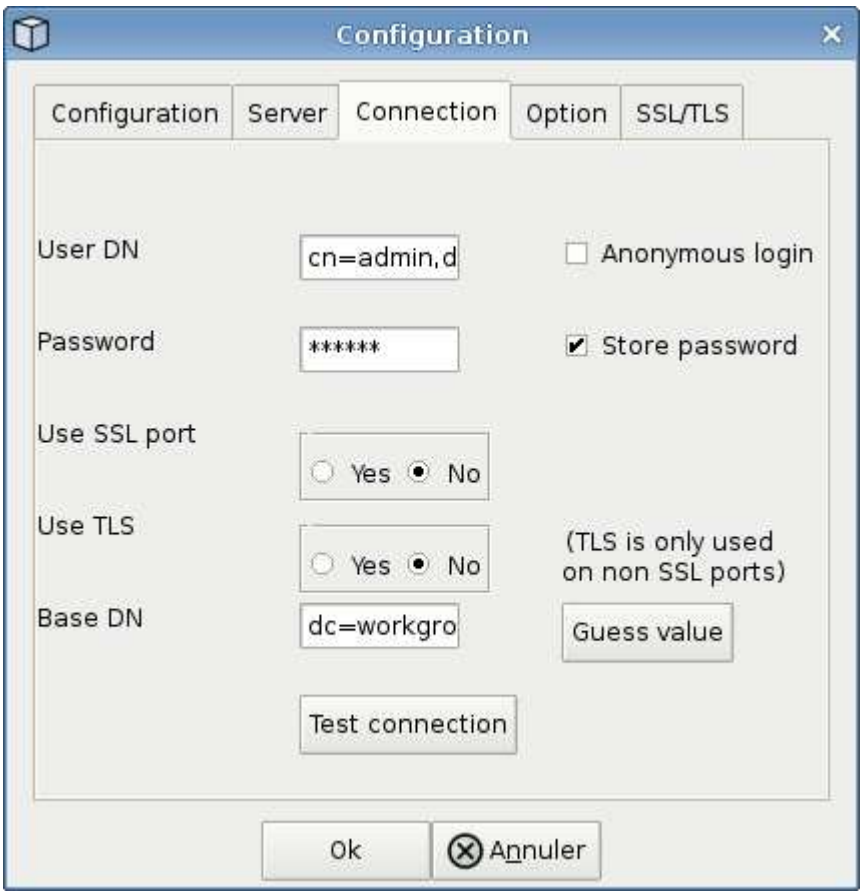
- Use o seguinte comando para validar a permissão do usuário LDAP do Workload Security:

```
 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
* Use o LDAP Explorer para navegar em um banco de dados LDAP, visualizar
propriedades e atributos de objetos, visualizar permissões, visualizar o
esquema de um objeto e executar pesquisas sofisticadas que você pode
salvar e reexecutar.
```

  - Instalar o LDAP Explorer(http://ldaptool.sourceforge.net/) ou Java LDAP Explorer(http://jxplorer.org/)

em qualquer máquina Windows que possa se conectar ao servidor LDAP.

- Conecte-se ao servidor LDAP usando o nome de usuário/senha do servidor de diretório LDAP.



Solução de problemas de erros de configuração do coletor de diretório LDAP

A tabela a seguir descreve problemas conhecidos e soluções que podem ocorrer durante a configuração do coletor:

Problema:	Resolução:
Adicionar um conector de diretório LDAP resulta no estado 'Erro'. O erro diz: “Credenciais inválidas fornecidas para o servidor LDAP”.	DN de vinculação ou senha de vinculação ou base de pesquisa incorreta fornecida. Edite e forneça as informações corretas.
Adicionar um conector de diretório LDAP resulta no estado 'Erro'. O erro diz: “Falha ao obter o objeto correspondente a DN=DC=hq,DC=domainname,DC=com fornecido como nome da floresta”.	Base de pesquisa fornecida incorreta. Edite e forneça o nome correto da floresta.
Os atributos opcionais do usuário do domínio não estão aparecendo na página Perfil do usuário do Workload Security.	Isso provavelmente ocorre devido a uma incompatibilidade entre os nomes dos atributos opcionais adicionados no CloudSecure e os nomes dos atributos reais no Active Directory. Os campos diferenciam maiúsculas de minúsculas. Edite e forneça o(s) nome(s) correto(s) do(s) atributo(s) opcional(is).

Problema:	Resolução:
Coletor de dados em estado de erro com "Falha ao recuperar usuários LDAP. Motivo da falha: Não é possível conectar no servidor, a conexão é nula"	Reinicie o coletor clicando no botão *Reiniciar*.
Adicionar um conector de diretório LDAP resulta no estado 'Erro'.	Certifique-se de ter fornecido valores válidos para os campos obrigatórios (Servidor, nome da floresta, DN de vinculação, Senha de vinculação). Certifique-se de que a entrada bind-DN seja sempre fornecida como uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=companyname,dc=com.
Adicionar um conector de diretório LDAP resulta no estado 'RETRYING'. Exibe o erro “Falha ao determinar a integridade do coletor, portanto, tente novamente”	Certifique-se de que o IP do servidor e a base de pesquisa corretos sejam fornecidos ////
Ao adicionar o diretório LDAP, o seguinte erro é exibido: “Falha ao determinar a integridade do coletor em 2 tentativas, tente reiniciar o coletor novamente (Código de erro: AGENT008)”	Garanta que o IP do servidor e a base de pesquisa corretos sejam fornecidos
Adicionar um conector de diretório LDAP resulta no estado 'RETRYING'. Exibe o erro “Não foi possível definir o estado do coletor, motivo pelo qual o comando TCP [Connect(localhost:35012,None,List(),Some(,seconds),true)] falhou devido a java.net.ConnectionException:Connection refused.”	IP ou FQDN incorreto fornecido para o servidor AD. Edite e forneça o endereço IP ou FQDN correto. ////
Adicionar um conector de diretório LDAP resulta no estado 'Erro'. O erro diz: “Falha ao estabelecer conexão LDAP”.	IP ou FQDN incorreto fornecido para o servidor LDAP. Edite e forneça o endereço IP ou FQDN correto. Ou valor incorreto para a porta fornecida. Tente usar os valores de porta padrão ou o número de porta correto para o servidor LDAP.
Adicionar um conector de diretório LDAP resulta no estado 'Erro'. O erro diz: “Falha ao carregar as configurações. Motivo: A configuração da fonte de dados tem um erro. Motivo específico: /connector/conf/application.conf: 70: ldap.ldap-port tem o tipo STRING em vez de NUMBER”	Valor incorreto fornecido para a Porta. Tente usar os valores de porta padrão ou o número de porta correto para o servidor AD.
Comecei com os atributos obrigatórios e funcionou. Após adicionar os opcionais, os dados dos atributos opcionais não estão sendo buscados do AD.	Isso provavelmente ocorre devido a uma incompatibilidade entre os atributos opcionais adicionados no CloudSecure e os nomes de atributos reais no Active Directory. Edite e forneça o nome correto do atributo obrigatório ou opcional.
Após reiniciar o coletor, quando a sincronização do LDAP ocorrerá?	A sincronização do LDAP ocorrerá imediatamente após a reinicialização do coletor. Levará aproximadamente 15 minutos para buscar dados de aproximadamente 300 mil usuários e será atualizado automaticamente a cada 12 horas.

Problema:	Resolução:
Os dados do usuário são sincronizados do LDAP para o CloudSecure. Quando os dados serão excluídos?	Os dados do usuário são retidos por 13 meses caso não haja atualização. Se o inquilino for excluído, os dados serão excluídos.
O conector do diretório LDAP resulta no estado 'Erro'. "O conector está em estado de erro. Nome do serviço: usersLdap. Motivo da falha: Falha ao recuperar usuários LDAP. Motivo da falha: 80090308: LdapErr: DSID-0C090453, comentário: erro AcceptSecurityContext, dados 52e, v3839"	Nome de floresta incorreto fornecido. Veja acima como fornecer o nome correto da floresta.
O número de telefone não está sendo preenchido na página de perfil do usuário.	Isso provavelmente ocorre devido a um problema de mapeamento de atributos com o Active Directory. 1. Edite o coletor específico do Active Directory que está buscando as informações do usuário do Active Directory. 2. Observe que, nos atributos opcionais, há um campo chamado “Número de telefone” mapeado para o atributo 'telephonenumber' do Active Directory. 4. Agora, use a ferramenta Active Directory Explorer conforme descrito acima para navegar no servidor de diretório LDAP e ver o nome do atributo correto. 3. Certifique-se de que no diretório LDAP haja um atributo chamado 'telephonenumber' que realmente tenha o número de telefone do usuário. 5. Digamos que no diretório LDAP ele foi modificado para 'número de telefone'. 6. Em seguida, edite o coletor do diretório de usuários do CloudSecure. Na seção de atributos opcionais, substitua 'telephonenumber' por 'phonenumber'. 7. Salve o coletor do Active Directory, o coletor será reiniciado e obterá o número de telefone do usuário e o exibirá na página de perfil do usuário.
Se o certificado de criptografia (SSL) estiver habilitado no servidor Active Directory (AD), o Workload Security User Directory Collector não poderá se conectar ao servidor AD.	Desabilite a criptografia do servidor AD antes de configurar um coletor de diretório de usuário. Depois que os detalhes do usuário forem obtidos, eles permanecerão lá por 13 meses. Se o servidor AD for desconectado após a busca dos detalhes do usuário, os usuários recém-adicionados no AD não serão buscados. Para buscar novamente o coletor de diretório do usuário, é necessário estar conectado ao AD.

Configurando o coletor de dados ONTAP SVM

O ONTAP SVM Data Collector permite que o Workload Security monitore atividades de acesso a arquivos e usuários em máquinas virtuais de armazenamento (SVMs) do NetApp ONTAP . Este guia orienta você na configuração e no gerenciamento do coletor de dados SVM para fornecer monitoramento de segurança abrangente do seu ambiente ONTAP .

Antes de começar

- Este coletor de dados é compatível com o seguinte:
  - Data ONTAP 9.2 e versões posteriores. Para melhor desempenho, use uma versão do Data ONTAP superior a 9.13.1.
  - Protocolo SMB versão 3.1 e anteriores.
  - Versões do NFS até e incluindo o NFS 4.1 (observe que o NFS 4.1 é compatível com o ONTAP 9.15 ou posterior).
  - O Flexgroup é compatível com o ONTAP 9.4 e versões posteriores
  - O FlexCache é compatível com NFS com ONTAP 9.7 e versões posteriores.
  - O FlexCache é compatível com SMB com ONTAP 9.14.1 e versões posteriores.
  - ONTAP Select é suportado
- Somente SVMs de tipo de dados são suportados. SVMs com volumes infinitos não são suportados.
- O SVM tem vários subtipos. Destes, apenas *default*, *sync_source* e *sync_destination* são suportados.
- Um agente"deve ser configurado" antes de poder configurar coletores de dados.
- Certifique-se de ter um Conector de Diretório de Usuário configurado corretamente, caso contrário, os eventos mostrarão nomes de usuários codificados e não o nome real do usuário (conforme armazenado no Active Directory) na página “Análise Forense de Atividades”.
- O ONTAP Persistent Store é compatível a partir da versão 9.14.1.
- Para um desempenho ideal, você deve configurar o servidor FPolicy para estar na mesma sub-rede que o sistema de armazenamento.
- Para obter as melhores práticas e recomendações abrangentes sobre a configuração do Workload Security FPolicy, consulte o"Artigo da Base de Conhecimento sobre as Melhores Práticas da FPolicy" .
- Você deve adicionar um SVM usando um dos dois métodos a seguir:
  - Usando o IP do cluster, o nome do SVM e o nome de usuário e a senha de gerenciamento do cluster. ***Este é o método recomendado.***
    - O nome do SVM deve ser exatamente como mostrado no ONTAP e diferencia maiúsculas de minúsculas.
  - Usando o IP, nome de usuário e senha de gerenciamento do SVM Vserver
  - Se você não puder ou não quiser usar o nome de usuário e a senha completos do administrador de cluster/gerenciamento de SVM, você pode criar um usuário personalizado com privilégios menores, conforme mencionado no“Uma nota sobre permissões” seção abaixo. Este usuário personalizado pode ser criado para acesso SVM ou Cluster.
    - Você também pode usar um usuário do AD com uma função que tenha pelo menos as permissões de csrole, conforme mencionado na seção "Uma observação sobre permissões" abaixo. Consulte também o"Documentação do ONTAP" .
- Certifique-se de que os aplicativos corretos estejam definidos para o SVM executando o seguinte comando:

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

Exemplo de saída:

```
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.
```

- Certifique-se de que o SVM tenha um servidor CIFS configurado: clustershell:> `vserver cifs show`

  O sistema retorna o nome do Vserver, o nome do servidor CIFS e campos adicionais.

- Defina uma senha para o usuário vsadmin do SVM. Se estiver usando um usuário personalizado ou um usuário administrador de cluster, pule esta etapa. clustershell:> `security login password -username vsadmin -vserver svmname`
- Desbloqueie o usuário vsadmin do SVM para acesso externo. Se estiver usando um usuário personalizado ou um usuário administrador de cluster, pule esta etapa. clustershell:> `security login unlock -username vsadmin -vserver svmname`
- Certifique-se de que a política de firewall do LIF de dados esteja definida como 'mgmt' (não 'data'). Pule esta etapa se estiver usando um gerenciamento dedicado para adicionar o SVM. clustershell:> `network interface modify -lif <SVM_data_LIF_name> -firewall-policy mgmt`
- Quando um firewall estiver habilitado, você deverá ter uma exceção definida para permitir o tráfego TCP para a porta usando o Data ONTAP Data Collector.

  Ver"Requisitos do agente" para obter informações de configuração. Isso se aplica a agentes locais e agentes instalados na nuvem.

- Quando um agente é instalado em uma instância do AWS EC2 para monitorar um SVM do Cloud ONTAP , o agente e o armazenamento devem estar na mesma VPC. Se estiverem em VPCs separadas, deve haver uma rota válida entre as VPCs.

Teste de conectividade para coletores de dados

O recurso de conectividade de teste (lançado em março de 2025) visa ajudar os usuários finais a identificar as causas específicas de falhas ao configurar coletores de dados no Data Infrastructure Insights (DII) Workload Security. Isso permite que os usuários corrijam problemas relacionados à comunicação de rede ou funções ausentes.

Este recurso ajudará os usuários a determinar se todas as verificações relacionadas à rede estão em vigor antes de configurar um coletor de dados. Além disso, ele informará os usuários sobre os recursos que eles podem acessar com base na versão do ONTAP , funções e permissões atribuídas a eles no ONTAP.

A conectividade de teste não é suportada para coletores de diretório de usuários

Pré-requisitos para teste de conexão

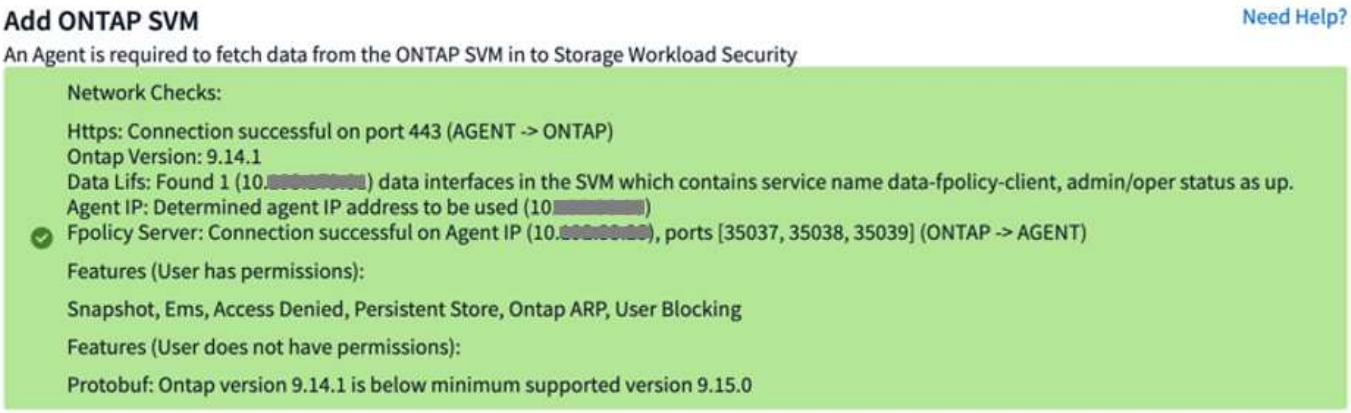
- Credenciais em nível de cluster são necessárias para que esse recurso funcione completamente.
- A verificação de acesso a recursos não é suportada no modo SVM.

- Se você estiver usando credenciais de administração de cluster, nenhuma nova permissão será necessária.
- Se você estiver usando um usuário personalizado (por exemplo, *csuser*), forneça as permissões obrigatórias e as permissões específicas dos recursos que deseja usar.

Não deixe de revisar oPermissões seção abaixo também.

Teste a conexão

O usuário pode ir para a página adicionar/editar coletor, inserir os detalhes do nível do cluster (no Modo Cluster) ou os detalhes do nível do SVM (no Modo SVM) e clicar no botão **Testar conexão**. O Workload Security processará a solicitação e exibirá uma mensagem apropriada de sucesso ou falha.



Pontos importantes a observar para ONTAP Multi Admin Verify (MAV)

Algumas funcionalidades, como a criação e exclusão de snapshots ou o bloqueio de usuários (SMB), podem não funcionar com base nos comandos MAV adicionados em sua versão do ONTAP.

Siga os passos abaixo para adicionar exclusões aos seus comandos MAV que permitem que o Workload Security crie ou exclua snapshots e bloqueie usuários.

Comandos para permitir snapshot create e delete:

```
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 o bloqueio de usuário:

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

Pré-requisitos para bloqueio de acesso do usuário

Tenha em mente o seguinte para"Bloqueio de acesso do usuário" :

Credenciais em nível de cluster são necessárias para que esse recurso funcione.

Se você estiver usando credenciais de administração de cluster, nenhuma nova permissão será necessária.

Se você estiver usando um usuário personalizado (por exemplo, *csuser*) com permissões dadas ao usuário, siga as etapas em"Bloqueio de acesso do usuário" para dar permissões ao Workload Security para bloquear o usuário.

Uma nota sobre permissões

Permissões ao adicionar via IP de gerenciamento de cluster:

Se você não puder usar o usuário administrador de gerenciamento de cluster para permitir que o Workload Security acesse o coletor de dados ONTAP SVM, você pode criar um novo usuário chamado “csuser” com as funções mostradas nos comandos abaixo. Use o nome de usuário “csuser” e a senha “csuser” ao configurar o coletor de dados do Workload Security para usar o IP de gerenciamento de cluster.

Observação: você pode criar uma única função para usar em todas as permissões de recursos de um usuário personalizado. Se houver um usuário existente, primeiro exclua o usuário e a função existentes usando estes 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 criar o novo usuário, efetue login no ONTAP com o nome de usuário/senha do Administrador de gerenciamento de cluster e execute os seguintes comandos no 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
```

Permissões ao adicionar via IP de gerenciamento do Vserver:

Se você não puder usar o usuário administrador de gerenciamento de cluster para permitir que o Workload Security acesse o coletor de dados ONTAP SVM, você pode criar um novo usuário chamado “csuser” com as funções mostradas nos comandos abaixo. Use o nome de usuário “csuser” e a senha “csuser” ao configurar o coletor de dados do Workload Security para usar o IP de gerenciamento do Vserver.

Observação: você pode criar uma única função para usar em todas as permissões de recursos de um usuário personalizado. Se houver um usuário existente, primeiro exclua o usuário e a função existentes usando estes 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 criar o novo usuário, efetue login no ONTAP com o nome de usuário/senha do Administrador de gerenciamento de cluster e execute os seguintes comandos no servidor ONTAP . Para facilitar, copie esses comandos para um editor de texto e substitua <vservername> pelo nome do seu Vserver antes de executar esses comandos no 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

O Workload Security configurará o mecanismo FPolicy no modo protobuf quando esta opção estiver habilitada nas configurações de *Configuração Avançada* do coletor. O modo protobuf é suportado no ONTAP versão 9.15 e posteriores.

Mais detalhes sobre esse recurso podem ser encontrados em"Documentação do ONTAP" .

Permissões específicas são necessárias para protobuf (algumas ou todas elas podem já existir):

Modo de cluster:

```
 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
```

Permissões para proteção autônoma contra ransomware ONTAP e acesso negado ao ONTAP

Se você estiver usando credenciais de administração de cluster, nenhuma nova permissão será necessária.

Se você estiver usando um usuário personalizado (por exemplo, *csuser*) com permissões dadas ao usuário, siga as etapas abaixo para dar permissões ao Workload Security para coletar informações relacionadas ao ARP do ONTAP.

Para mais informações, leia sobre"Integração com ONTAP Acesso negado"

e"Integração com a Proteção Autônoma contra Ransomware ONTAP"

Configurar o coletor de dados

Etapas para configuração

1. Efetue login como administrador ou proprietário da conta no seu ambiente do Data Infrastructure Insights .
2. Clique em **Segurança de Carga de Trabalho > Coletores > +Coletores de Dados**

   O sistema exibe os Coletores de Dados disponíveis.
3. Passe o mouse sobre o bloco * NetApp SVM e clique em **+Monitor**.

   O sistema exibe a página de configuração do ONTAP SVM. Insira os dados necessários para cada campo.

Campo	Descrição
Nome	Nome exclusivo para o coletor de dados
Agente	Selecione um agente configurado na lista.
Conecte-se via IP de gerenciamento para:	Selecione o IP do cluster ou o IP de gerenciamento do SVM
Endereço IP de gerenciamento de cluster/SVM	O endereço IP do cluster ou do SVM, dependendo da sua seleção acima.
Nome SVM	O nome do SVM (este campo é obrigatório ao conectar via IP do cluster)
Nome de usuário	Nome de usuário para acessar o SVM/Cluster Ao adicionar via IP do Cluster, as opções são: 1. Administrador de cluster 2. 'csuser' 3. Usuário AD com função semelhante à do csuser. Ao adicionar via IP SVM, as opções são: 4. vsadmin 5. 'csuser' 6. Nome de usuário do AD com função semelhante ao csuser.
Senha	Senha para o nome de usuário acima
Filtrar Ações/Volumes	Escolha se deseja incluir ou excluir Ações/Volumes da coleta de eventos
Insira os nomes completos dos compartilhamentos para excluir/incluir	Lista separada por vírgulas de ações a serem excluídas ou incluídas (conforme apropriado) da coleta de eventos

Insira os nomes completos dos volumes a serem excluídos/incluídos	Lista separada por vírgulas de volumes a serem excluídos ou incluídos (conforme apropriado) da coleção de eventos
Monitorar acesso à pasta	Quando marcada, habilita eventos para monitoramento de acesso a pastas. Observe que a criação/renomeação e exclusão de pastas serão monitoradas mesmo sem esta opção selecionada. Habilitar isso aumentará o número de eventos monitorados.
Definir tamanho do buffer de envio ONTAP	Define o tamanho do buffer de envio do ONTAP Fpolicy. Se uma versão do ONTAP anterior à 9.8p7 for usada e houver problemas de desempenho, o tamanho do buffer de envio do ONTAP poderá ser alterado para obter melhor desempenho do ONTAP . Entre em contato com o Suporte da NetApp se você não vir esta opção e quiser explorá-la.

Depois que você terminar

- Na página Coletores de dados instalados, use o menu de opções à direita de cada coletor para editar o coletor de dados. Você pode reiniciar o coletor de dados ou editar os atributos de configuração do coletor de dados.

Configuração recomendada para MetroCluster

O seguinte é recomendado para MetroCluster:

1. Conecte dois coletores de dados, um ao SVM de origem e outro ao SVM de destino.
2. Os coletores de dados devem ser conectados por *Cluster IP*.
3. A qualquer momento, o coletor de dados do SVM 'em execução' atual será exibido como *Em execução*. O coletor de dados do SVM 'parado' atual será exibido como *Parado*.
4. Sempre que houver uma alternância, o estado do coletor de dados mudará de *Em execução* para *Parado* e vice-versa.
5. Levará até dois minutos para que o coletor de dados passe do estado *Parado* para o estado *Em execução*.

Política de Serviço

Se estiver usando a política de serviço com o ONTAP **versão 9.9.1 ou mais recente**, para se conectar ao Coletor de Fonte de Dados, o serviço *data-fpolicy-client* será necessário junto com o serviço de dados *data-nfs* e/ou *data-cifs*.

Exemplo:

```
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)
```

Em versões do ONTAP anteriores à 9.9.1, *data-fpolicy-client* não precisa ser definido.

Coletor de dados de reprodução e pausa

Se o Coletor de Dados estiver no estado *Em execução*, você pode pausar a coleta. Abra o menu "três pontos" do coletor e selecione PAUSAR. Enquanto o coletor estiver pausado, nenhum dado será coletado do ONTAP e nenhum dado será enviado do coletor para o ONTAP. Isso significa que nenhum evento Fpolicy fluirá do ONTAP para o coletor de dados e de lá para o Data Infrastructure Insights.

Observe que se novos volumes, etc., forem criados no ONTAP enquanto o coletor estiver em pausa, o Workload Security não coletará os dados e esses volumes, etc., não serão refletidos nos painéis ou tabelas.

Um coletor não pode ser pausado se tiver usuários restritos. Restaure o acesso do usuário antes de pausar o coletor.

Tenha em mente o seguinte:

- A limpeza de instantâneos não ocorrerá de acordo com as configurações definidas em um coletor pausado.
- Eventos EMS (como ONTAP ARP) não serão processados em um coletor pausado. Isso significa que, se ONTAP identificar um ataque de adulteração de arquivo, Data Infrastructure Insights Workload Security não poderá adquirir esse evento.
- E-mails de notificação de saúde NÃO serão enviados para um coletor pausado.
- Ações manuais ou automáticas (como Snapshot ou Bloqueio de usuário) não serão suportadas em um coletor pausado.
- Em atualizações de agente ou coletor, reinicializações/reinicializações de VM de agente ou reinicialização de serviço de agente, um coletor pausado permanecerá no estado *Pausado*.
- Se o coletor de dados estiver no estado *Erro*, o coletor não poderá ser alterado para o estado *Pausado*. O botão Pausar será habilitado somente se o estado do coletor for *Em execução*.
- Se o agente for desconectado, o coletor não poderá ser alterado para o estado *Pausado*. O coletor entrará no estado *Parado* e o botão Pausar será desabilitado.

Armazenamento Persistente

O armazenamento persistente é compatível com o ONTAP 9.14.1 e posteriores. Observe que as instruções de nome de volume variam do ONTAP 9.14 para o 9.15.

O Armazenamento Persistente pode ser habilitado marcando a caixa de seleção na página de edição/adição do coletor. Após selecionar a caixa de seleção, um campo de texto é exibido para aceitar o nome do volume. O nome do volume é um campo obrigatório para habilitar o Armazenamento Persistente.

- Para o ONTAP 9.14.1, você deve criar o volume antes de habilitar o recurso e fornecer o mesmo nome no campo *Nome do volume*. O tamanho de volume recomendado é 16 GB.
- Para o ONTAP 9.15.1, o volume será criado automaticamente com tamanho de 16 GB pelo coletor, usando o nome fornecido no campo *Nome do volume*.

Permissões específicas são necessárias para o Persistent Store (algumas ou todas elas podem já existir):

Modo de cluster:

```
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 Coletores

Você pode migrar facilmente um coletor de segurança de carga de trabalho de um agente para outro, permitindo um balanceamento de carga eficiente de coletores entre agentes.

Pré-requisitos

- O agente de origem deve estar no estado *conectado*.
- O coletor a ser migrado deve estar no estado *em execução*.

Observação:

- O Migrate é suportado tanto para coletores de Dados quanto para coletores de Diretório de Usuário.
- A migração de um coletor não é suportada para locatários gerenciados manualmente.

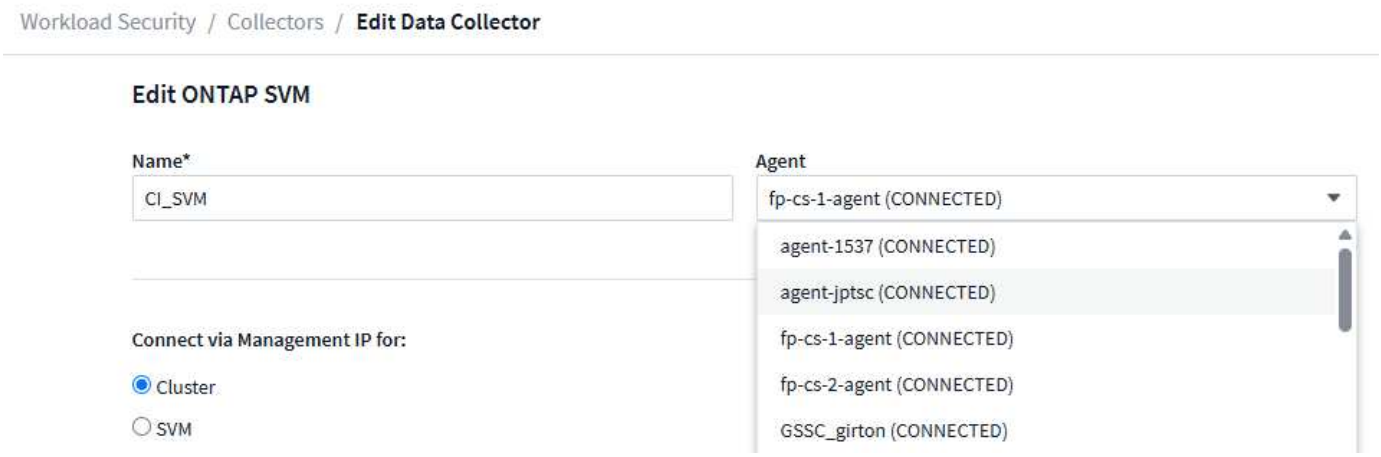
Migrar coletor

Para migrar um coletor, siga estas etapas:

1. Vá para a página "Editar Colecionador".
2. Selecione um agente de destino no menu suspenso de agentes.
3. Clique no botão "Salvar Coletor".

O Workload Security processará a solicitação. Após a migração bem-sucedida, o usuário será redirecionado para a página da lista de coletores. Em caso de falha, uma mensagem apropriada será exibida na página de edição.

Observação: quaisquer alterações de configuração feitas anteriormente na página "Editar coletor" permanecerão aplicadas quando o coletor for migrado com sucesso para o agente de destino.



Solução de problemas

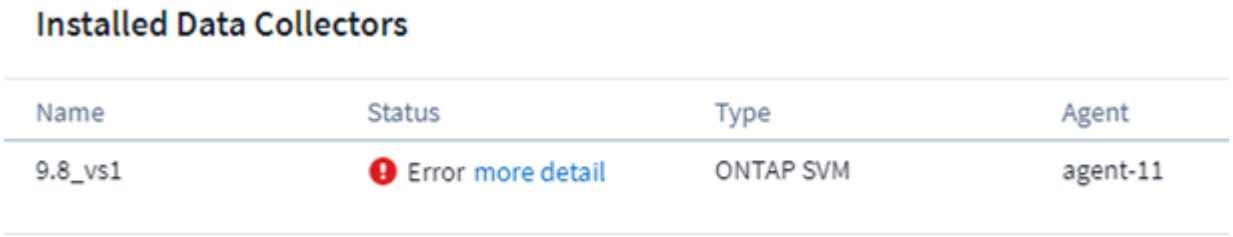
Veja o"Solução de problemas do coletor SVM" página para dicas de solução de problemas.

Solução de problemas do coletor de dados ONTAP SVM

O Workload Security usa coletores de dados para coletar dados de acesso de arquivos e usuários de dispositivos. Aqui você pode encontrar dicas para solucionar problemas com este coletor.

Veja o"Configurando o coletor SVM" página para obter instruções sobre como configurar este coletor.

Em caso de erro, você pode clicar em *mais detalhes* na coluna *Status* da página Coletores de Dados Instalados para obter detalhes sobre o erro.



Problemas conhecidos e suas soluções são descritos abaixo.

Problema: O Data Collector é executado por algum tempo e para após um tempo aleatório, falhando com: "Mensagem de erro: O conector está em estado de erro. Nome do serviço: auditoria. Motivo da falha: Servidor fpolicy externo sobrecarregado." **Tente isto:** A taxa de eventos do ONTAP era muito maior do que a caixa do Agente pode suportar. Por isso a conexão foi encerrada.

Verifique o pico de tráfego no CloudSecure quando a desconexão ocorreu. Você pode verificar isso na página **CloudSecure > Análise forense de atividades > Todas as atividades**.

Se o tráfego agregado de pico for maior do que o Agent Box pode suportar, consulte a página Event Rate Checker sobre como dimensionar a implantação do Collector em um Agent Box.

Se o Agente foi instalado na caixa do Agente antes de 4 de março de 2021, execute os seguintes comandos

na caixa do Agente:

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

Reinicie o coletor pela interface do usuário após o redimensionamento.

{vazio}

Problema: O coletor relata a mensagem de erro: “Nenhum endereço IP local encontrado no conector que possa alcançar as interfaces de dados do SVM”. **Tente isto:** Isso provavelmente ocorre devido a um problema de rede no lado do ONTAP . Siga estes passos:

1. Certifique-se de que não haja firewalls no servidor de dados do SVM ou no servidor de gerenciamento que estejam bloqueando a conexão do SVM.
2. Ao adicionar um SVM por meio de um IP de gerenciamento de cluster, certifique-se de que o tempo de vida de dados e o tempo de vida de gerenciamento do SVM possam ser executados por ping a partir da VM do agente. Em caso de problemas, verifique o gateway, a máscara de rede e as rotas do lif.

   Você também pode tentar fazer login no cluster via ssh usando o IP de gerenciamento do cluster e fazer ping no IP do agente. Certifique-se de que o IP do agente pode ser executado em ping:

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

   Se não for possível fazer ping, certifique-se de que as configurações de rede no ONTAP estejam corretas para que a máquina do agente seja possível fazer ping.
3. Se você tentou se conectar via IP do Cluster e não está funcionando, tente se conectar diretamente via IP do SVM. Veja acima as etapas para conectar via IP SVM.
4. Ao adicionar o coletor via IP do SVM e credenciais vsadmin, verifique se o SVM Lif tem a função Dados mais Gerenciamento habilitada. Neste caso, o ping para o SVM Lif funcionará, porém o SSH para o SVM Lif não funcionará. Em caso afirmativo, crie um SVM Mgmt Only Lif e tente conectar-se por meio deste SVM management only Lif.
5. Se ainda não estiver funcionando, crie um novo SVM Lif e tente conectar-se através desse Lif. Certifique-se de que a máscara de sub-rede esteja definida corretamente.
6. Depuração avançada:
   a. Inicie um rastreamento de pacotes no ONTAP.
   b. Tente conectar um coletor de dados ao SVM pela interface do usuário do CloudSecure.
   c. Aguarde até que o erro apareça. Pare o rastreamento de pacotes no ONTAP.
   d. Abra o rastreamento de pacotes do ONTAP. Está disponível neste local

```
 https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
.. Certifique-se de que haja um SYN do ONTAP para a caixa do Agente.
.. Se não houver SYN do ONTAP , então é um problema com o firewall no
ONTAP.
.. Abra o firewall no ONTAP para que o ONTAP consiga conectar a caixa
do agente.
```

7. Se ainda não estiver funcionando, consulte a equipe de rede para garantir que nenhum firewall externo esteja bloqueando a conexão do ONTAP para a caixa do agente.
8. Se nenhuma das opções acima resolver o problema, abra um caso com"Suporte Netapp" para obter mais assistência.

{vazio}

Problema: Mensagem: "Falha ao determinar o tipo ONTAP para [nome do host: <Endereço IP>. Motivo: Erro de conexão com o Sistema de Armazenamento <Endereço IP>: Host inacessível (Host inacessível)" **Tente isto:**

1. Verifique se o endereço IP de gerenciamento do SVM ou o IP de gerenciamento do cluster correto foi fornecido.
2. SSH para o SVM ou o cluster ao qual você pretende se conectar. Depois de conectado, certifique-se de que o nome do SVM ou do cluster esteja correto.

{vazio}

Problema: Mensagem de erro: "O conector está em estado de erro. Nome do serviço: auditoria. Motivo da falha: Servidor fpolicy externo encerrado." **Experimente isto:**

1. É mais provável que um firewall esteja bloqueando as portas necessárias na máquina do agente. Verifique se o intervalo de portas 35000-55000/tcp está aberto para que a máquina do agente se conecte ao SVM. Certifique-se também de que não haja firewalls habilitados no lado do ONTAP bloqueando a comunicação com a máquina do agente.
2. Digite o seguinte comando na caixa Agente e certifique-se de que o intervalo de portas esteja aberto.

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

   A saída de exemplo deve ser semelhante a:

   ```
    -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate
   NEW -j ACCEPT
   . Efetue login no SVM, insira os seguintes comandos e verifique se
   nenhum firewall está definido para bloquear a comunicação com o ONTAP.
   ```

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

"Verifique os comandos do firewall"no lado ONTAP .

3. SSH para o SVM/Cluster que você deseja monitorar. Execute ping na caixa do agente a partir do data life do SVM (com suporte aos protocolos CIFS e NFS) e verifique se o ping está funcionando:

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

Se não for possível fazer ping, certifique-se de que as configurações de rede no ONTAP estejam corretas para que a máquina do agente seja possível fazer ping.

4. Se um único SVM for adicionado duas vezes a um locatário por meio de 2 coletores de dados, esse erro será exibido. Exclua um dos coletores de dados por meio da interface do usuário. Em seguida, reinicie o outro coletor de dados por meio da interface do usuário. Em seguida, o coletor de dados mostrará o status “RUNNING” e começará a receber eventos do SVM.

   Basicamente, em um locatário, 1 SVM deve ser adicionado apenas uma vez, por meio de 1 coletor de dados. 1 SVM não deve ser adicionado duas vezes por meio de 2 coletores de dados.

5. Em casos em que o mesmo SVM foi adicionado em dois ambientes de segurança de carga de trabalho diferentes (locatários), o último sempre terá sucesso. O segundo coletor configurará o fpolicy com seu próprio endereço IP e expulsará o primeiro. Então o coletor no primeiro deixará de receber eventos e seu serviço de "auditoria" entrará em estado de erro. Para evitar isso, configure cada SVM em um único ambiente.
6. Esse erro também pode ocorrer se as políticas de serviço não estiverem configuradas corretamente. Com o ONTAP 9.8 ou posterior, para se conectar ao Data Source Collector, o serviço data-fpolicy-client é necessário junto com o serviço de dados data-nfs e/ou data-cifs. Além disso, o serviço data-fpolicy-client deve ser associado ao(s) data lif(s) do SVM monitorado.

{vazio}

Problema: Nenhum evento visto na página de atividades. **Experimente isto:**

1. Verifique se o coletor ONTAP está no estado “RUNNING”. Em caso afirmativo, certifique-se de que alguns eventos cifs estejam sendo gerados nas VMs do cliente cifs abrindo alguns arquivos.
2. Se nenhuma atividade for vista, faça login no SVM e digite o seguinte comando.

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

Certifique-se de que não haja erros relacionados à fpolicy.

3. Se nenhuma atividade for vista, faça login no SVM. Digite o seguinte comando:

```
<SVM>fpolicy show
```

Verifique se a política fpolicy nomeada com prefixo “cloudsecure_” foi definida e o status é “on”. Se não estiver definido, provavelmente o Agente não conseguirá executar os comandos no SVM. Certifique-se de que todos os pré-requisitos descritos no início da página foram seguidos.

{vazio}

Problema: O coletor de dados SVM está em estado de erro e a mensagem de erro é “O agente falhou ao conectar ao coletor” **Tente isto:**

1. Provavelmente o Agente está sobrecarregado e não consegue se conectar aos coletores da Fonte de Dados.
2. Verifique quantos coletores de fonte de dados estão conectados ao agente.
3. Verifique também a taxa de fluxo de dados na página “Todas as atividades” na interface do usuário.
4. Se o número de atividades por segundo for significativamente alto, instale outro Agente e mova alguns dos Coletores de Fonte de Dados para o novo Agente.

{vazio}

Problema: O SVM Data Collector exibe a mensagem de erro "fpolicy.server.connectError: O nó falhou ao estabelecer uma conexão com o servidor FPolicy "12.195.15.146" (motivo: "Tempo limite de seleção esgotado")" **Tente isto:** O firewall está habilitado no SVM/Cluster. Portanto, o mecanismo fpolicy não consegue se conectar ao servidor fpolicy. Os CLIs no ONTAP que podem ser usados para obter mais informações são:

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

"Verifique os comandos do firewall"no lado ONTAP .

{vazio}

Problema: Mensagem de erro: “O conector está em estado de erro. Nome do serviço: auditoria. Motivo da falha: Nenhuma interface de dados válida (função: dados, protocolos de dados: NFS ou CIFS ou ambos, status: ativo) encontrada no SVM.” **Tente isto:** Certifique-se de que haja uma interface operacional (com função de dados e protocolo de dados como CIFS/NFS).

{vazio}

Problema: O coletor de dados entra no estado de erro e depois entra no estado de execução após algum

tempo, e depois volta ao estado de erro novamente. Este ciclo se repete. **Tente isto:** Isso normalmente acontece no seguinte cenário:

1. Vários coletores de dados foram adicionados.
2. Os coletores de dados que mostram esse tipo de comportamento terão 1 SVM adicionado a esses coletores de dados. Isso significa que 2 ou mais coletores de dados estão conectados a 1 SVM.
3. Garanta que 1 coletor de dados se conecte a apenas 1 SVM.
4. Exclua os outros coletores de dados que estão conectados ao mesmo SVM.

{vazio}

Problema: O conector está em estado de erro. Nome do serviço: auditoria. Motivo da falha: Falha na configuração (política no SVM svmname. Motivo: Valor inválido especificado para o elemento 'shares-to-include' em 'fpolicy.policy.scope-modify: "Federal' **Tente isto:** *Os nomes dos compartilhamentos precisam ser fornecidos sem aspas. Edite a configuração do ONTAP SVM DSC para corrigir os nomes de compartilhamento.

Incluir e excluir compartilhamentos não se destina a uma longa lista de nomes de compartilhamentos. Em vez disso, use a filtragem por volume se você tiver um grande número de compartilhamentos para incluir ou excluir.

{vazio}

Problema: Há fpolicies existentes no Cluster que não estão sendo utilizadas. O que deve ser feito com eles antes da instalação do Workload Security? **Tente isto:** É recomendável excluir todas as configurações fpolicy existentes e não utilizadas, mesmo que estejam em estado desconectado. O Workload Security criará fpolicy com o prefixo "cloudsecure_". Todas as outras configurações fpolicy não utilizadas podem ser excluídas.

Comando CLI para mostrar a lista fpolicy:

```
 fpolicy show
Etapas para excluir configurações do 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>
```

{vazio}

Problema: Após habilitar a Segurança de Carga de Trabalho, o desempenho do ONTAP é afetado: a latência

torna-se esporadicamente alta e o número de operações de entrada/saída (IOPS) torna-se esporadicamente baixo. **Experimente isto:** Ao usar o ONTAP com Segurança de Carga de Trabalho, às vezes podem ocorrer problemas de latência no ONTAP. Existem diversas razões possíveis para isso, conforme observado a seguir:"1372994" , "1415152" , "1438207" , "1479704" , "1354659" . Todos esses problemas foram corrigidos no ONTAP 9.13.1 e posteriores; é altamente recomendável usar uma dessas versões posteriores.

{vazio}

Problema: O Data Collector mostra a mensagem de erro: “Erro: Falha ao determinar a integridade do coletor em 2 tentativas, tente reiniciar o coletor novamente (Código de erro: AGENT008)”. **Experimente isto:**

1. Na página Coletores de dados, role para a direita do coletor de dados que está apresentando o erro e clique no menu de 3 pontos. Selecione *Editar*. Digite a senha do coletor de dados novamente. Salve o coletor de dados pressionando o botão *Salvar*. O Data Collector será reiniciado e o erro deverá ser resolvido.
2. A máquina do agente pode não ter espaço suficiente para CPU ou RAM, e é por isso que os DSCs estão falhando. Verifique o número de Coletores de Dados adicionados ao Agente na máquina. Se for maior que 20, aumente a capacidade da CPU e da RAM da máquina do agente. Quando a CPU e a RAM forem aumentadas, os DSCs entrarão no estado Inicializando e depois em Execução automaticamente. Consulte o guia de tamanhos em"esta página" .

{vazio}

Problema: O coletor de dados está apresentando erro quando o modo SVM é selecionado. **Tente isto:** Ao conectar no modo SVM, se o IP de gerenciamento do cluster for usado para conectar em vez do IP de gerenciamento do SVM, a conexão falhará. Certifique-se de que o IP SVM correto seja usado.

{vazio}

Problema: O coletor de dados mostra uma mensagem de erro quando o recurso Acesso negado está habilitado: "O conector está em estado de erro. Nome do serviço: auditoria. Motivo da falha: Falha ao configurar fpolicy no SVM test_svm. Motivo: O usuário não está autorizado." **Tente isto:** O usuário pode não ter as permissões REST necessárias para o recurso Acesso negado. Por favor, siga as instruções em"esta página" para definir as permissões.

Reinicie o coletor depois que as permissões forem definidas.

{vazio}

Problema: O coletor está em estado de erro com a mensagem: O conector está em estado de erro. Motivo da falha: Falha ao configurar o armazenamento persistente na SVM <Nome da SVM>. Motivo: Não foi possível encontrar um agregado adequado para o volume "<volumeName>" na SVM "<SVM Name>". Motivo: As informações de desempenho para o agregado "<aggregateName>" não estão disponíveis no momento. Aguarde alguns minutos e tente o comando novamente. Nome do serviço: auditoria. Motivo da falha: Falha ao configurar o armazenamento persistente no SVM<SVM name="">.</SVM> Motivo: Não foi possível encontrar um agregado adequado para o volume "<volumeName>" no SVM "<SVM name="">".</SVM></volumeName> Motivo: as informações de desempenho para a agregação "<aggregateName>" não estão disponíveis no

momento.</aggregateName> Aguarde alguns minutos e tente o comando novamente.

Experimente isto: Aguarde alguns minutos e reinicie o Collector.

{vazio}

Se você ainda estiver enfrentando problemas, entre em contato com os links de suporte mencionados na página **Ajuda > Suporte**.

Configurando o Cloud Volumes ONTAP e o Amazon FSx for NetApp ONTAP

Monitore o acesso a arquivos e usuários em toda a sua infraestrutura de armazenamento em nuvem configurando coletores de dados do Workload Security para Cloud Volumes ONTAP e Amazon FSx for NetApp ONTAP. Este guia fornece instruções passo a passo para implantar agentes na AWS e conectá-los às suas instâncias de armazenamento em nuvem.

Configuração de armazenamento Cloud Volumes ONTAP

Consulte a documentação do OnCommand Cloud Volumes ONTAP para configurar uma instância AWS de nó único/HA para hospedar o Workload Security Agent:https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html[]

Após a conclusão da configuração, siga as etapas para configurar seu SVM:https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html[]

Plataformas suportadas

- Cloud Volumes ONTAP, suportado por todos os provedores de serviços de nuvem disponíveis, sempre que disponível. Por exemplo: Amazon, Azure, Google Cloud.
- ONTAP Amazon FSx

Configuração da máquina do agente

A máquina do agente deve ser configurada nas respectivas sub-redes dos provedores de serviços de nuvem. Leia mais sobre acesso à rede em [Requisitos do agente].

Abaixo estão as etapas para instalação do agente na AWS. Etapas equivalentes, conforme aplicáveis ao provedor de serviços de nuvem, podem ser seguidas no Azure ou no Google Cloud para a instalação.

Na AWS, use as seguintes etapas para configurar a máquina a ser usada como um Agente de Segurança de Carga de Trabalho:

Use as seguintes etapas para configurar a máquina a ser usada como um Agente de Segurança de Carga de Trabalho:

Passos

1. Efetue login no console da AWS, navegue até a página EC2-Instances e selecione *Launch instance*.

2. Selecione uma AMI RHEL ou CentOS com a versão apropriada, conforme mencionado nesta página:https://docs.netapp.com/us-en/cloudinsights/concept_cs_agent_requirements.html[]
3. Selecione a VPC e a sub-rede em que a instância do Cloud ONTAP reside.
4. Selecione *t2.xlarge* (4 vcpus e 16 GB de RAM) como recursos alocados.
    a. Crie a instância do EC2.
5. Instale os pacotes Linux necessários usando o gerenciador de pacotes YUM:
    a. Instale *wget* e *descompacte* os pacotes nativos do Linux.

Instalar o Agente de Segurança de Carga de Trabalho

1. Efetue login como administrador ou proprietário da conta no seu ambiente do Data Infrastructure Insights .
2. Navegue até Workload Security **Collectors** e clique na aba **Agents**.
3. Clique em **+Agente** e especifique RHEL como a plataforma de destino.
4. Copie o comando de instalação do agente.
5. Cole o comando de instalação do agente na instância RHEL EC2 na qual você está conectado. Isso instala o agente de segurança de carga de trabalho, fornecendo todos os"Pré-requisitos do agente" são atendidas.

Para obter etapas detalhadas, consulte este xref:./ https://docs.netapp.com/us-en/cloudinsights/task_cs_add_agent.html#steps-to-install-agent

Solução de problemas

Problemas conhecidos e suas soluções são descritos na tabela a seguir.

Problema	Resolução
O erro “Segurança da carga de trabalho: falha ao determinar o tipo ONTAP para o coletor de dados Amazon FxSN” é exibido pelo Coletor de dados. O cliente não consegue adicionar o novo coletor de dados do Amazon FSxN ao Workload Security. A conexão com o cluster FSxN na porta 443 do agente está expirando. Os grupos de segurança do firewall e da AWS têm as regras necessárias habilitadas para permitir a comunicação. Um agente já está implantado e também está na mesma conta da AWS. Este mesmo agente é usado para conectar e monitorar os dispositivos NetApp restantes (e todos eles estão funcionando).	Resolva esse problema adicionando o segmento de rede LIF fsxadmin à regra de segurança do agente. Permitir todas as portas caso você não tenha certeza sobre elas.

Gerenciamento de usuários

As contas de usuário do Workload Security são gerenciadas pelo Data Infrastructure Insights.

O Data Infrastructure Insights fornece quatro níveis de conta de usuário: Proprietário da conta, Administrador, Usuário e Convidado. Cada conta recebe níveis de permissão específicos. Uma conta de usuário com privilégios de administrador pode criar ou modificar usuários e atribuir a cada usuário uma das seguintes

funções de segurança de carga de trabalho:

Papel	Acesso de segurança de carga de trabalho
Administrador	Pode executar todas as funções de segurança de carga de trabalho, incluindo aquelas para alertas, análises forenses, coletores de dados, políticas de resposta automatizadas e APIs para segurança de carga de trabalho. Um administrador também pode convidar outros usuários, mas só pode atribuir funções de segurança de carga de trabalho.
Usuário	Pode visualizar e gerenciar alertas e visualizar análises forenses. A função do usuário pode alterar o status do alerta, adicionar uma nota, tirar instantâneos manualmente e restringir o acesso do usuário.
Convidado	Pode visualizar alertas e análises forenses. A função de convidado não pode alterar o status do alerta, adicionar uma nota, tirar instantâneos manualmente ou restringir o acesso do usuário.

Passos

1. Faça login no Workload Security
2. No menu, clique em **Admin > Gerenciamento de usuários**

   Você será encaminhado para a página de Gerenciamento de Usuários do Data Infrastructure Insights.

3. Selecione a função desejada para cada usuário.

Ao adicionar um novo usuário, basta selecionar a função desejada (geralmente Usuário ou Convidado).

Mais informações sobre contas e funções de usuário podem ser encontradas em Data Infrastructure Insights"Função do usuário" documentação.

Verificador de Taxa de Eventos: guia de dimensionamento de agentes

Determine o dimensionamento ideal das máquinas do Agente medindo as taxas de eventos NFS e SMB geradas por suas SVMs antes de implantar os coletores de dados. O script Event Rate Checker ajuda você a entender os limites de capacidade (máximo 50 coletores de dados por Agente) e garante que sua infraestrutura de Agente possa lidar com o volume de eventos esperado para uma detecção confiável de ameaças.

Requisitos:

- IP de cluster
- Nome de usuário e senha do administrador do cluster

Ao executar este script, nenhum coletor de dados ONTAP SVM deve estar em execução para o SVM para o qual a taxa de eventos está sendo determinada.

Passos:

1. Instale o Agente seguindo as instruções do CloudSecure.
2. Depois que o agente estiver instalado, execute o script *server_data_rate_checker.sh* como um usuário sudo:

```
 /opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
. Este script requer que o _sshpass_ esteja instalado na máquina Linux.
Existem duas maneiras de instalá-lo:
```

   a. Execute o seguinte comando:

```
 linux_prompt> yum install sshpass
.. Se isso não funcionar, baixe o _sshpass_ para a máquina Linux da
web e execute o seguinte comando:
```

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

3. Forneça os valores corretos quando solicitado. Veja um exemplo abaixo.
4. O script levará aproximadamente 5 minutos para ser executado.
5. Após a conclusão da execução, o script imprimirá a taxa de eventos do SVM. Você pode verificar a taxa de eventos por SVM na saída do console:

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

Cada coletor de dados Ontap SVM pode ser associado a um único SVM, o que significa que cada coletor de dados poderá receber o número de eventos que um único SVM gera.

Tenha em mente o seguinte:

A) Use esta tabela como um guia geral de dimensionamento. Você pode aumentar o número de núcleos e/ou memória para aumentar o número de coletores de dados suportados, até um máximo de 50 coletores de dados:

Configuração da máquina do agente	Número de coletores de dados SVM	Taxa máxima de eventos que a máquina do agente pode manipular
4 núcleos, 16 GB	10 coletores de dados	20 mil eventos/seg
4 núcleos, 32 GB	20 coletores de dados	20 mil eventos/seg

B) Para calcular o total de eventos, some os Eventos gerados para todos os SVMs daquele agente.

C) Se o script não for executado durante os horários de pico ou se o tráfego de pico for difícil de prever, mantenha um buffer de taxa de eventos de 30%.

B + C deve ser menor que A, caso contrário a máquina do agente não conseguirá monitorar.

Em outras palavras, o número de coletores de dados que podem ser adicionados a uma única máquina agente deve obedecer à fórmula abaixo:

```
 Sum of all Event rate of all Data Source Collectors + Buffer Event rate
of 30% < 20000 events/second
Veja olink:concept_cs_agent_requirements.html["Requisitos do agente"]
página para pré-requisitos e requisitos adicionais.
```

Exemplo

Digamos que temos três SVMS gerando taxas de eventos de 100, 200 e 300 eventos por segundo, respectivamente.

Aplicamos a 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.
```

A saída do console está disponível na máquina do agente no arquivo *fpolicy_stat_<Nome do SVM>.log* no diretório de trabalho atual.

O script pode dar resultados errôneos nos seguintes casos:

- Credenciais, IP ou nome SVM incorretos foram fornecidos.
- Uma fpolicy já existente com o mesmo nome, número de sequência, etc. dará erro.
- O script é interrompido abruptamente durante a execução.

Um exemplo de execução de script é mostrado abaixo:

```
[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]#
```

Solução de problemas

Pergunta	Responder

Se eu executar esse script em um SVM que já está configurado para Workload Security, ele usará apenas a configuração fpolicy existente no SVM ou configurará uma temporária e executará o processo?	O Event Rate Checker pode ser executado corretamente mesmo para um SVM já configurado para Workload Security. Não deve haver impacto.
Posso aumentar o número de SVMs nas quais o script pode ser executado?	Sim. Basta editar o script e alterar o número máximo de SVMs de 5 para qualquer número desejado.
Se eu aumentar o número de SVMs, o tempo de execução do script aumentará?	Não. O script será executado por no máximo 5 minutos, mesmo que o número de SVMs seja aumentado.
Posso aumentar o número de SVMs nas quais o script pode ser executado?	Sim. Você precisa editar o script e alterar o número máximo de SVMs de 5 para qualquer número desejado.
Se eu aumentar o número de SVMs, o tempo de execução do script aumentará?	Não. O script será executado por no máximo 5 minutos, mesmo que o número de SVMs seja aumentado.
O que acontece se eu executar o Event Rate Checker com um agente existente?	Executar o Event Rate Checker em um agente já existente pode causar um aumento na latência no SVM. Esse aumento será temporário por natureza enquanto o Verificador de taxas de eventos estiver em execução.

Informações sobre direitos autorais

Informações sobre marcas comerciais