Como começar

Data Infrastructure Insights

NetApp
October 08, 2025

Índice

Como começar

Introdução ao Workload Security

Há tarefas de configuração que precisam ser concluídas antes de começar a usar o Workload Security para monitorar a atividade do usuário.

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" "**Vídeo**: Implantação de agentes"
Configure um conetor do diretório de usuários	"Adicionar conetor do diretório do utilizador" "**Vídeo**: Conexão do ative Directory"
Configurar coletores de dados	Clique em **Workload Security > Collectors** clique no coletor de dados que deseja configurar. Consulte a seção Referência do fornecedor do coletor de dados da documentação. "**Vídeo**: Conexão ONTAP SVM"
Crie contas de usuários	"Gerir contas de utilizador"
Solução de problemas	"**Vídeo**: Resolução de problemas"

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

Requisitos do Agente de Segurança de carga de trabalho

Você deve"instalar um agente de segurança de carga de trabalho" para obter informações de seus coletores de dados. Antes de instalar o Agente, certifique-se de que seu ambiente atenda aos requisitos de sistema operacional, CPU, memória e espaço em disco.

Componente	Requisito 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 disponível em disco	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) Nota: Recomenda-se alocar um pouco de espaço em disco extra 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 a partir de um armazenamento nas, certifique-se de que os utilizadores locais têm acesso a esta pasta. O Agent ou Data Collector pode falhar na instalação se os usuários locais não tiverem permissão para essa pasta. Consulte "solução de problemas"a seção para obter mais detalhes.
Rede	Conexão Ethernet de 100 Mbps a 1 Gbps, endereço IP estático, conetividade IP a todos os dispositivos e uma porta necessária para a instância de segurança de carga de trabalho (80 ou 443).

Observação: O agente 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. No caso de estes estarem instalados na mesma máquina, atribua espaço em disco, conforme ilustrado abaixo:

Espaço disponível em disco	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 a hora no sistema ONTAP e na máquina do agente usando **Protocolo de tempo de rede (NTP)** ou **Protocolo de tempo de rede simples (SNTP)**.

Regras de acesso à rede na 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	<site_name>.cs01.cloudinsights.NetApp.com <site_name>.c01.cloudinsights.NetApp.com <site_name>.c02.cloudinsights.NetApp.com	Acesso ao Data Infrastructure Insights
TCP	443	Agente de segurança de carga de trabalho	agentlogin.cs01.cloudinsights.netapp.com	Acesso aos 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	<site_name>.cs01-eu-1.cloudinsights.NetApp.com <site_name>.c01-eu-1.cloudinsights.NetApp.com <site_name>.c02-eu-1.cloudinsights.NetApp.com	Acesso ao Data Infrastructure Insights
TCP	443	Agente de segurança de carga de trabalho	agentlogin.cs01-eu-1.cloudinsights.netapp.com	Acesso aos serviços de autenticação

Para ambientes de segurança de workload **baseados na APAC**:

Protocolo	Porta	Fonte	Destino	Descrição
TCP	443	Agente de segurança de carga de trabalho	<site_name>.cs01-ap-1.cloudinsights.NetApp.com <site_name>.c01-ap-1.cloudinsights.NetApp.com <site_name>.c02-ap-1.cloudinsights.NetApp.com	Acesso ao Data Infrastructure Insights
TCP	443	Agente de segurança de carga de trabalho	agentlogin.cs01-ap-1.cloudinsights.netapp.com	Acesso aos 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	Ligar ao LDAP
TCP	443	Agente de segurança de carga de trabalho	Endereço IP do gerenciamento do cluster ou SVM (dependendo da configuração do coletor do SVM)	Comunicação de API com o ONTAP

Protocolo	Porta	Fonte	Destino	Descrição
TCP	35000 - 55000	Endereços IP de LIF de dados SVM	Agente de segurança de carga de trabalho	Comunicação do ONTAP para 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). OBSERVE que você não precisa reservar **todos** dessas portas, mas as portas que você reserva para isso devem estar dentro desse intervalo. Recomenda-se começar reservando cerca de 100 portas e aumentando, se necessário.

Protocolo	Porta	Fonte	Destino	Descrição
TCP	35000-55000	IP de gerenciamento de clusters	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 houver). OBSERVE que você não precisa reservar **todos** dessas portas, mas as portas que você reserva para isso devem estar dentro desse intervalo. Recomenda-se começar reservando cerca de 100 portas e aumentando, se necessário.
SSH	22	Agente de segurança de carga de trabalho	Gerenciamento de clusters	Necessário para bloqueio de usuários CIFS/SMB.

Dimensionamento do sistema

Consulte "Verificador de taxa de eventos"a documentação para obter informações sobre dimensionamento.

Instalação do Agente de Segurança de carga de trabalho

A Segurança da carga de trabalho (anteriormente Cloud Secure) coleta dados de atividade do usuário usando um ou mais agentes. Os agentes se conetam a dispositivos no locatário e coletam dados que são enviados para a camada SaaS de segurança do workload para análise. "Requisitos do agente"Consulte para configurar uma VM de agente.

Antes de começar

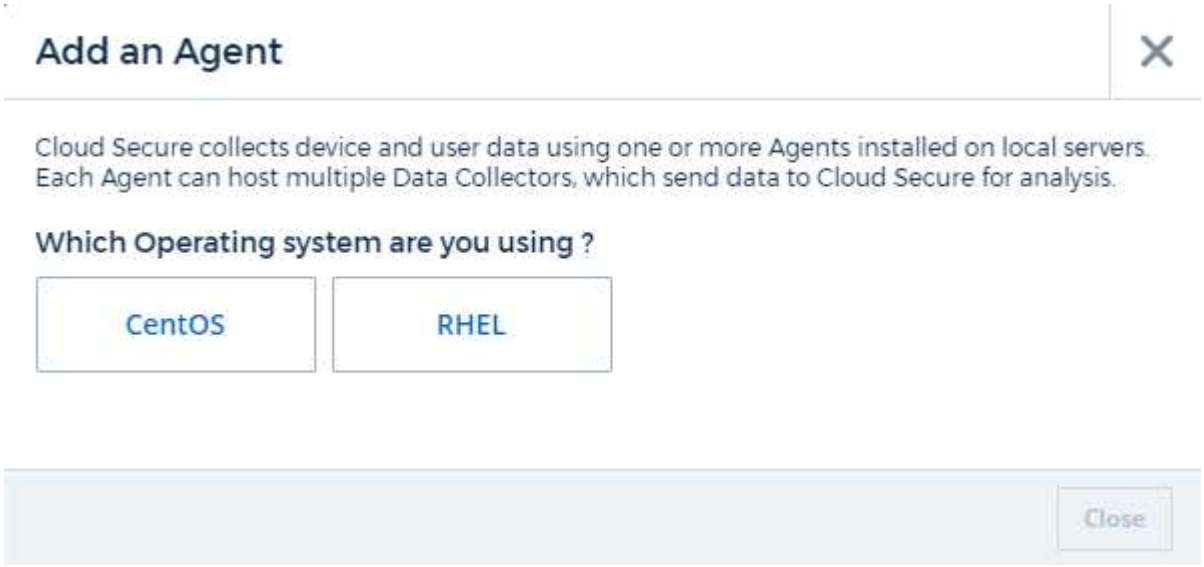
- O privilégio sudo é necessário para instalação, execução de scripts e desinstalação.
- Durante a instalação do agente, um usuário local *cssys* e um grupo local *cssys* são criados na máquina. Se as configurações de permissão não permitirem a criação de um usuário local e, em vez disso, exigirem o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

Mudanças globais podem ter um impacto potencial em seus sistemas ONTAP . É altamente recomendável fazer alterações que afetem um grande número de coletores de dados fora dos horários de pico.

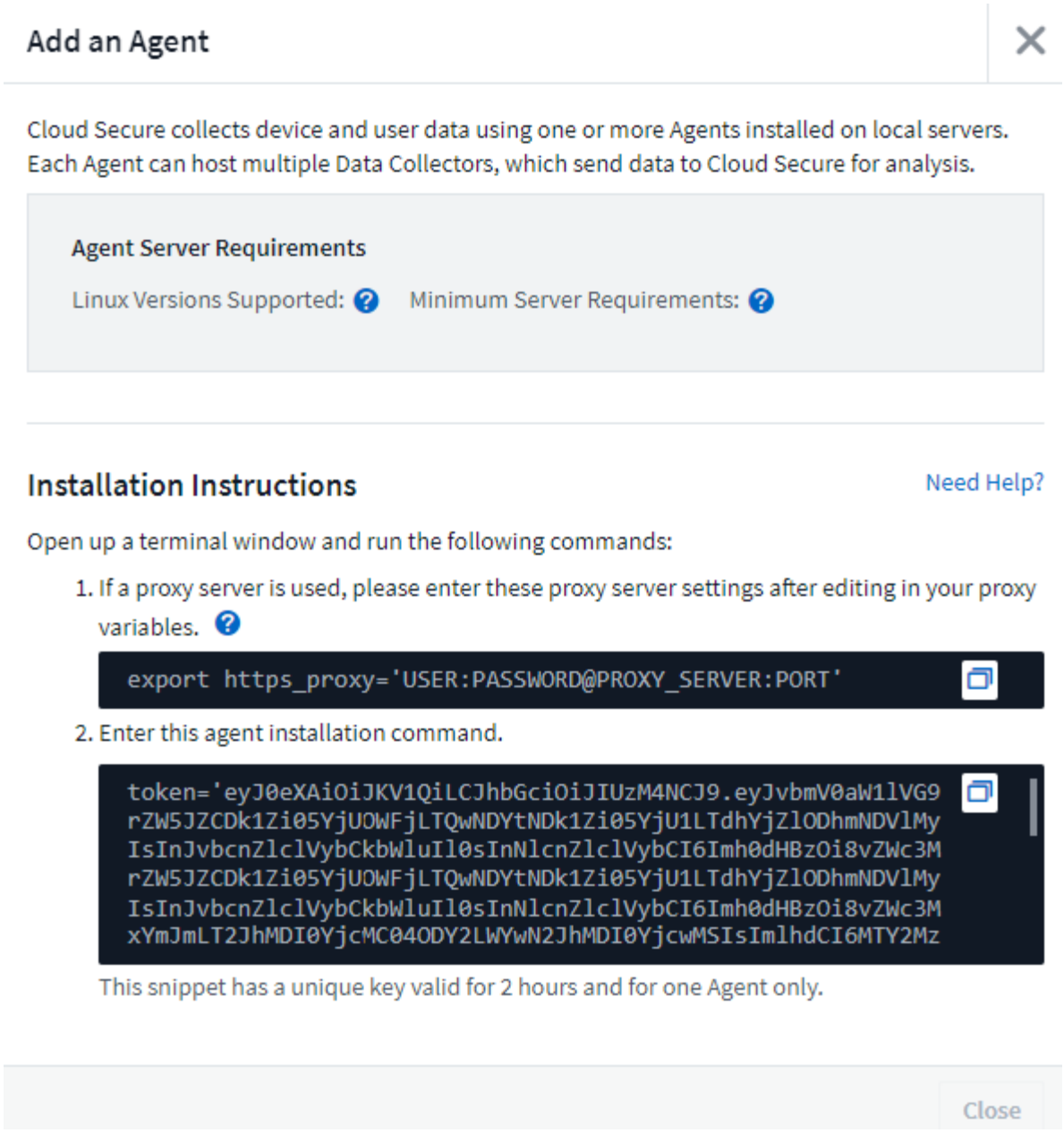
Etapas para instalar o agente

1. Inicie sessão como Administrador ou proprietário de conta no ambiente de Segurança de carga de trabalho.
2. Selecione **Collectors > Agents > Agent**

   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 de agente está executando uma versão suportada do Linux, clique em *versões suportadas (i)*.
5. Se a rede estiver usando o 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 for concluída com êxito:

Depois de concluir

1. É necessário configurar um "Coletor de diretório de usuários".
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 um problema 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 a sua plataforma:

- CentOS 7.x / RHEL 7.x*:
  1. `sudo iptables-save | grep 35000`

Saída da amostra:

```
 -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 da amostra:

```
35000-55000/tcp
```

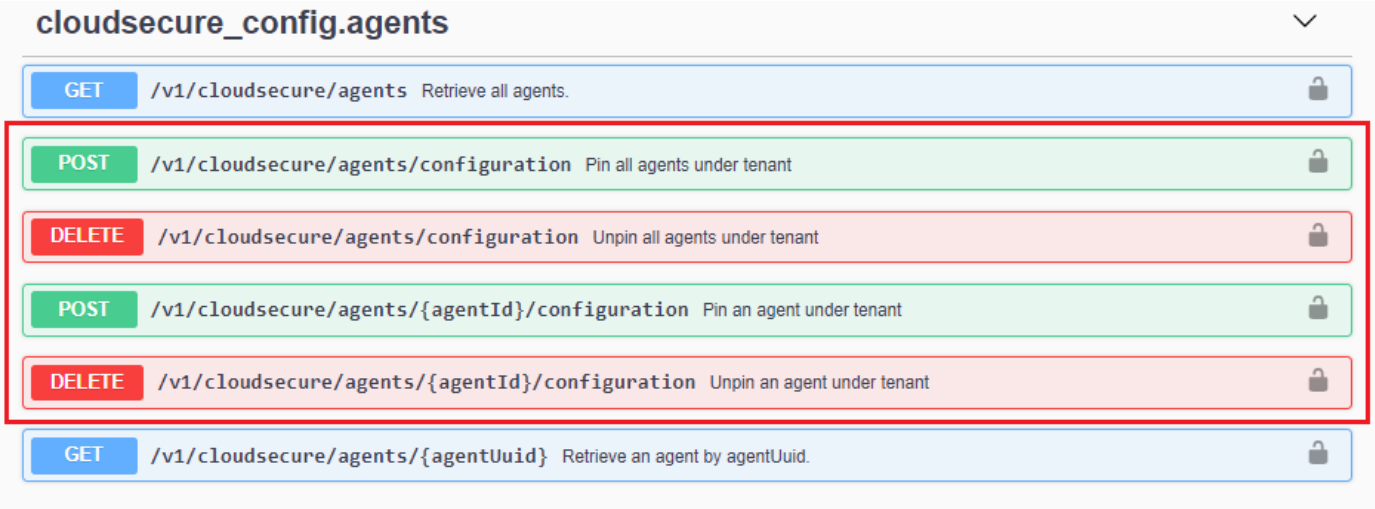
"Fixar" um agente na versão atual

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

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

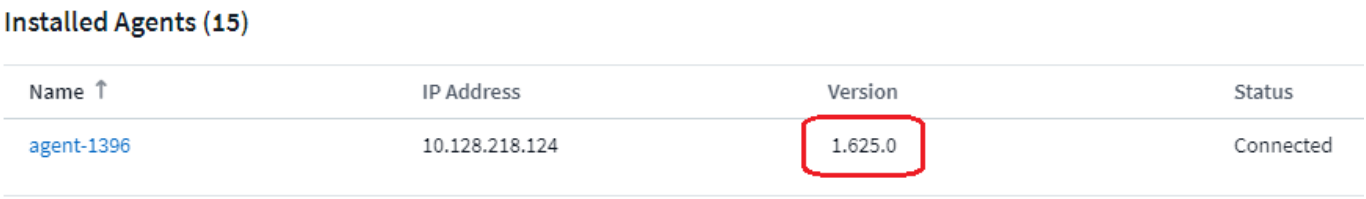
Em cada um desses casos, o agente será atualizado na próxima atualização de Segurança de carga de trabalho.

Para pausar ou retomar atualizações automáticas de agentes, 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 exibir suas versões atuais do Agente na página **Segurança de carga de trabalho > coletores**, na guia **agentes**.



Solução de problemas de erros do agente

Problemas conhecidos e suas resoluções 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.	Esse erro ocorre durante o bootstrapping do agente. O erro não é registrado em arquivos de log porque ocorre antes que o logger seja inicializado. O erro é redirecionado para a saída padrão e é visível no log de serviço usando o `journalctl -u cloudsecure-agent.service` comando. Este comando pode ser usado para solucionar o problema ainda mais. est
A instalação do agente falha com 'esta distribuição linux não é suportada. Sair da instalação'.	Esse erro aparece quando você tenta instalar o Agente em um sistema não suportado. "Requisitos do agente"Consulte .
Falha na instalação do agente com o erro: "-bash: Unzip: Comando not found"	Instale o descompacte e execute o comando de instalação novamente. Se o Yum estiver instalado na máquina, tente "yum install unzip" para instalar o software deszip. Depois disso, copie novamente o comando da IU 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 Agent. Verifique o status do serviço do agente através `sudo systemctl status cloudsecure-agent.service`do . 1. Verifique se os logs mostram uma mensagem "Falha ao iniciar o serviço daemon de Segurança do Workload" . 2. Verifique se o usuário cssys existe ou não na máquina Agente. Execute os seguintes comandos um por um com permissão root e verifique se o usuário e o grupo cssys existem. `sudo id cssys` `sudo groups cssys` 3. Se nenhuma existir, uma política de monitorização centralizada pode ter eliminado o utilizador 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 em execução, verifique as outras opções de resolução 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 coletor, por exemplo, ative Directory, SVM e outros coletores.
A IU mostra que o Agente está no estado NÃO LIGADO.	Etapas para reiniciar o Agente. 1. SSH para a máquina Agent. 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 `sudo systemctl status cloudsecure-agent.service`do . 4. O agente deve ir para o estado CONETADO.
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 à medida que são assinados pela Zscaler CA para que o agente não confie na comunicação.	Desative a inspeção SSL no proxy Zscaler para o url *.cloudinsights.NetApp.com. Se o Zscaler fizer a inspeção SSL e substituir os certificados, o Workload Security não funcionará.

Problema:	Resolução:
Durante a instalação do agente, a instalação trava após o desbloqueio.	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 ao comando chmod com falha, o resto da instalação não é executado. 1. Crie um novo diretório chamado "cloudsecure". 2. Vá para esse diretório. 3. Copie e cole o comando completo de instalação "token……" e pressione ENTER. 4. A instalação deve ser capaz de prosseguir.
Se o agente ainda não conseguir se conetar 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 root e compartilhe o arquivo de saída (cloudsecure-Agent-sympats.zip). A. /opt/NetApp/cloudsecure/Agent/bin/cloudsecure-agent-symptom-collector.sh 2. Execute os seguintes comandos um a um com permissão 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. /Opt/NetApp/cloudsecure/Agent/bin/cloudsecure-agent-symptom-collector.sh coletando log de serviço coletando logs de aplicativos coletando configurações de agentes tomando snapshot de status de serviço tomando snapshot da estrutura de diretórios de agentes…… …… /Opt/NetApp/cloudsecure/Agent/bin/cloudsecure-Agent-sintoma-Collector.sh: Linha 52: Zip: ERRO de comando não encontrado: 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.
Falha na instalação do agente com useradd: Não é possível criar diretório /home/cssys	Esse 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 o usuário cssys e adicionar seu diretório de login manualmente usando o seguinte comando: *Sudo useradd user_name -m -d home_DIR* -m :criar o diretório home do usuário se ele não existir. -D : o novo usuário é criado usando home_DIR como o 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 sob root.

Problema:	Resolução:
O agente não está em execução após a instalação. *Systemctl status cloudsecure-agent.service* NetApp 25889 12:26 126 1 mostra o seguinte: [Root at demo] no. Systemctl status cloudsecure-agent.service agent.service 25889 126 1 03 21 cloudsecure-agent.service – Workload Agente de Segurança Serviço Daemon carregado: Carregado (/usr/lib/systemd/system/cloudsecure-agent.service; 126 03 21 cloudsecure-agent.service: 12:26 ativado; predefinição do fornecedor: Desativado) Ativo: Ativando (auto-restart) (resultado: Exit-code) desde Tue 2s-08-03 21:12:26 PDT; 2021 Aug 03 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 essa 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 *cssys* usuário. Se retornar "permissão negada", a permissão de instalação não está presente. Em vez de uma pasta montada, instale em um diretório local para a máquina.
O agente foi inicialmente conetado através de um servidor proxy e o proxy foi definido durante a instalação do Agente. Agora, o servidor proxy mudou. Como a configuração do 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 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 pretende configurar os coletores de dados com um agente diferente, você deve criar um backup das configurações do Data Collector 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 Workload Security.

   Nota: Ignore esta etapa se todos os coletores associados estiverem no estado PARADO.

Etapas para excluir um agente:

1. 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 **Workload Security > Collectors > Agents**

   O sistema exibe a lista de agentes configurados.

3. Clique no menu de opções para o 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 usuários do ative Directory (AD)

A Segurança da carga de trabalho pode ser configurada para coletar atributos de usuário de servidores do ative Directory.

Antes de começar

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

Passos para configurar um Coletor de diretório de usuários

1. No menu Workload Security, clique em: **Collectors > User Directory Collectors > User Directory Collector** e selecione **ative Directory**

   O sistema exibe a tela Adicionar diretório do usuário.

Configure o Coletor de diretório de usuários 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
Nome de domínio/IP do servidor	Endereço IP ou nome de domínio totalmente qualificado (FQDN) do servidor que hospeda o diretório ativo

Nome da floresta	Nível de floresta da estrutura do diretório. O nome da floresta permite ambos os seguintes formatos: *X.y.z*> nome de domínio direto como você o tem no SVM. [Exemplo: hq.companyname.com]_DC,DC_DC_com] ou você pode especificar como o seguinte: _Ou NetApp <username> <engineering>
Vincular DN	Usuário autorizado a pesquisar o diretório. Por exemplo: *username@companyname.com* ou *username@domainname.com* além disso, a permissão de domínio somente leitura é necessária. O usuário deve ser um membro do grupo Segurança *Controladores de domínio somente leitura*.
Palavra-passe BIND	Senha do servidor de diretório (ou seja, senha para nome de usuário usado no DN de vinculação)
Protocolo	ldap, ldaps, ldap-start-tls
Portas	Selecione a porta

Insira os seguintes atributos necessários do Directory Server se os nomes de atributo padrão tiverem sido modificados no ative Directory. Na maioria das vezes, esses nomes de atributos são *not* modificados no ative Directory, caso em que você pode simplesmente prosseguir com o nome do atributo padrão.

Atributos	Nome do atributo no Directory Server
Nome de exibição	nome
SID	objectsid
Nome de utilizador	SAMAccountName

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

Atributos	Nome do atributo no servidor de diretório
Endereço de e-mail	e-mail
Número de telefone	número de telefone
Função	título
País	co
Estado	estado
Departamento	departamento
Foto	thumbnailphoto
ManagerDN	gerente
Grupos	Membro Of

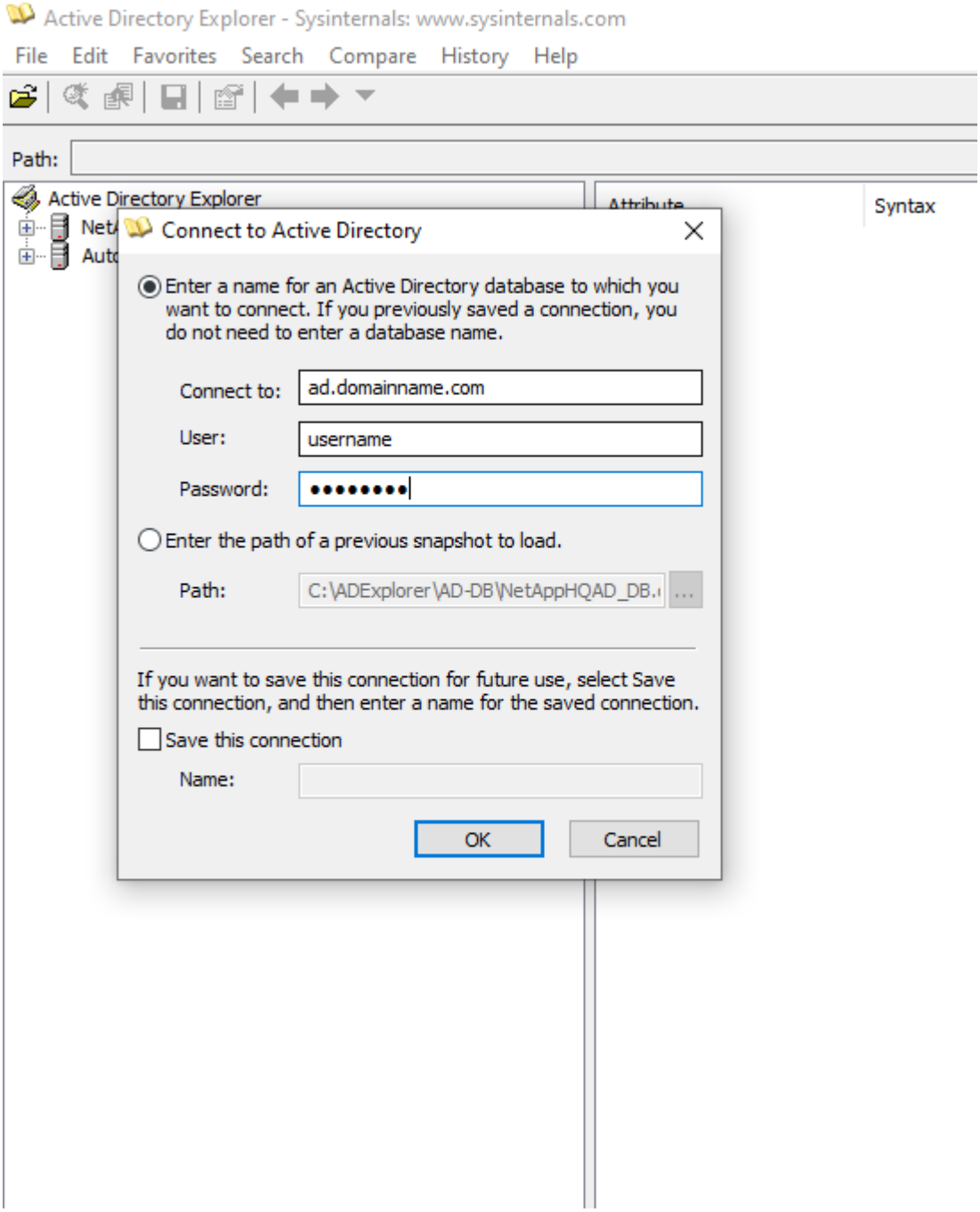
Testando a configuração do coletor do diretório de usuários

Você pode validar permissões de Usuário LDAP e Definições de Atributo usando os seguintes procedimentos:

- Use o seguinte comando para validar a permissão de usuário LDAP de segurança de workload:

```
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, exibir propriedades e atributos de objetos, exibir permissões, exibir o esquema de um objeto, executar pesquisas sofisticadas que você pode salvar e executar novamente.
  - Instale "Explorador de ANÚNCIOS" em qualquer máquina Windows que possa se conetar ao servidor AD.
  - Conete-se ao servidor AD usando o nome de usuário/senha do servidor de diretório AD.



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

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

Problema:	Resolução:
Adicionar um conetor do diretório de usuários resulta no estado "erro". O erro diz: "Credenciais inválidas fornecidas para o servidor LDAP".	Nome de utilizador ou palavra-passe incorretos fornecidos. Edite e forneça o nome de usuário e a senha corretos.
Adicionar um conetor do diretório de usuários resulta no estado "erro". Erro diz: "Falha ao obter o objeto correspondente a DN	Nome da floresta incorreto fornecido. Edite e forneça o nome correto da floresta.
Os atributos opcionais do usuário de domínio não estão aparecendo na página Perfil de usuário de Segurança de carga de trabalho.	Isso provavelmente se deve a uma incompatibilidade entre os nomes de atributos opcionais adicionados no CloudSecure e os nomes de atributos reais no ative Directory. Edite e forneça o(s) nome(s) do atributo opcional correto(s).
Coletor de dados no estado de erro com "Falha ao recuperar usuários LDAP. Motivo da falha: Não é possível conetar no servidor, a conexão é nula"	Reinicie o coletor clicando no botão *Restart*.
Adicionar um conetor do diretório de usuários resulta no estado "erro".	Certifique-se de que forneceu valores válidos para os campos obrigatórios (servidor, nome da floresta, bind-DN, bind-Password). Certifique-se de que a entrada BIND-DN é sempre fornecida como "Administrador <domain_forest_name>" ou como uma conta de usuário com Privileges de administrador de domínio.
Adicionar um conetor do diretório de usuários resulta no estado "TENTAR NOVAMENTE". Mostra o erro "não é possível definir o estado do comando Collector,Reason TCP [Connect(localhost:35012,None,List(),some(,seconds),true)] falhou por causa de java.net.ConnectionException:Connection recusado."	IP ou FQDN incorreto fornecido para o servidor AD. Edite e forneça o endereço IP ou FQDN correto.
Adicionar um conetor do diretório de usuários resulta no estado "erro". O erro diz: "Falha ao estabelecer a conexão LDAP".	IP ou FQDN incorreto fornecido para o servidor AD. Edite e forneça o endereço IP ou FQDN correto.
Adicionar um conetor do diretório de usuários resulta no estado "erro". O erro diz: "Falha ao carregar as configurações. Motivo: A configuração da fonte de dados tem um erro. Razão específica: /Connector/conf/application.conf: 70: LDAP.ldap-port tem STRING de tipo em vez DE NÚMERO"	Valor incorreto para a porta fornecida. Tente usar os valores de porta padrão ou o número de porta correto para o servidor AD.
Comecei com os atributos obrigatórios, e funcionou. Depois de adicionar os opcionais, os dados de atributos opcionais não são obtidos do AD.	Isso provavelmente se deve a uma incompatibilidade entre os atributos opcionais adicionados no CloudSecure e os nomes de atributos reais no ative Directory. Edite e forneça o nome do atributo obrigatório ou opcional correto.

Problema:	Resolução:
Depois de reiniciar o coletor, quando acontecerá a sincronização AD?	A sincronização DE ANÚNCIOS ocorrerá imediatamente após o coletor ser reiniciado. Levará aproximadamente 15 minutos para obter dados do usuário de aproximadamente 300K usuários e é atualizado a cada 12 horas automaticamente.
Os dados do usuário são sincronizados do AD para o CloudSecure. Quando os dados serão excluídos?	Os dados do usuário são mantidos para 13months em caso de não atualização. Se o locatário for excluído, os dados serão excluídos.
O conetor do diretório do usuário resulta no estado "erro". "O conetor está no estado de erro. Nome do serviço: UsersLdap. Motivo da falha: Falha ao recuperar usuários LDAP. Motivo da falha: 80090308: LdapErr: DSID-0C090453, comentário: AcceptSecurityContext error, data 52e, v3839"	Nome da floresta incorreto fornecido. Veja acima como fornecer o nome correto da floresta.
O número de telefone não está a ser preenchido na página de perfil de utilizador.	Isso é provavelmente devido a um problema de mapeamento de atributos com o ative Directory. 1. Edite o coletor específico do ative Directory que está obtendo as informações do usuário do ative Directory. 2. Em atributos opcionais, há um nome de campo "número de telefone" mapeado para o atributo do ative Directory 'número de telefone'. 4. Agora, use a ferramenta Explorador do ative Directory conforme descrito acima para navegar no ative Directory e ver o nome do atributo correto. 3. Certifique-se de que, no ative Directory, existe um atributo chamado "número de telefone" que tem, de fato, o número de telefone do usuário. 5. Digamos que no ative Directory foi modificado para "número de telefone". 6. Em seguida, edite o coletor CloudSecure User Directory. Na seção de atributo opcional, substitua 'número de telefone' por 'número de telefone'. 7. Salve o coletor do ative Directory, o coletor reiniciará e obterá o número de telefone do usuário e exibirá o mesmo na página do perfil do usuário.
Se o certificado de encriptação (SSL) estiver ativado no servidor AD (ative Directory), o Coletor do diretório de utilizadores de Segurança de carga de trabalho não pode ligar-se ao servidor AD.	Desative a criptografia do AD Server antes de configurar um coletor de diretório de usuários. Uma vez que os detalhes do usuário são obtidos, ele estará lá por 13 meses. Se o servidor AD for desconetado após buscar os detalhes do usuário, os usuários recém-adicionados no AD não serão obtidos. Para buscar novamente, o coletor de diretório do usuário precisa ser conetado ao AD.
Os dados do ative Directory estão presentes no CloudInsights Security. Deseja excluir todas as informações do usuário do CloudInsights.	Não é possível excluir APENAS as informações do usuário do ative Directory do CloudInsights Security. Para excluir o usuário, o locatário completo precisa ser excluído.

Configurando um LDAP Directory Server Collector

Você configura o Workload Security para coletar atributos de usuário de servidores LDAP Directory.

Antes de começar

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

Passos para configurar um Coletor de diretório de usuários

1. No menu Workload Security, clique em: **Collectors > User Directory Collectors > User Directory Collector** e selecione **LDAP Directory Server**

   O sistema exibe a tela Adicionar diretório do usuário.

Configure o Coletor de diretório de usuários 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
Nome de domínio/IP do servidor	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 seguintes formatos: *X.y.z*> nome de domínio direto como você o tem no SVM. *DC_DC_DC_DC_NetApp c*<username> c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_<engineering>_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c
Vincular DN	Usuário autorizado a pesquisar o diretório. Por exemplo: uid, uid, uid, uid, uid, uid, uid, ucn, contas, dc, empresa, dc, dc, com para um usuário john@dorp.company.com. dorp.company.com
--contas	--usuários
--john	--anna
Palavra-passe BIND	Senha do servidor de diretório (ou seja, senha para nome de usuário usado no DN de vinculação)
Protocolo	Idap, Idaps, Idap-start-tls
Portas	Selecione a porta

Insira os seguintes atributos necessários do servidor de diretório se os nomes de atributo padrão tiverem sido modificados no servidor de diretório LDAP. Na maioria das vezes, esses nomes de atributos são *not*

modificados no LDAP Directory Server, nesse caso, você pode simplesmente prosseguir com o nome do atributo padrão.

Atributos	Nome do atributo no Directory Server
Nome de exibição	nome
UNIXID	número de identificação
Nome de utilizador	uid

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

Atributos	Nome do atributo no servidor de diretório
Endereço de e-mail	e-mail
Número de telefone	número de telefone
Função	título
País	co
Estado	estado
Departamento	número de peça
Foto	foto
ManagerDN	gerente
Grupos	Membro Of

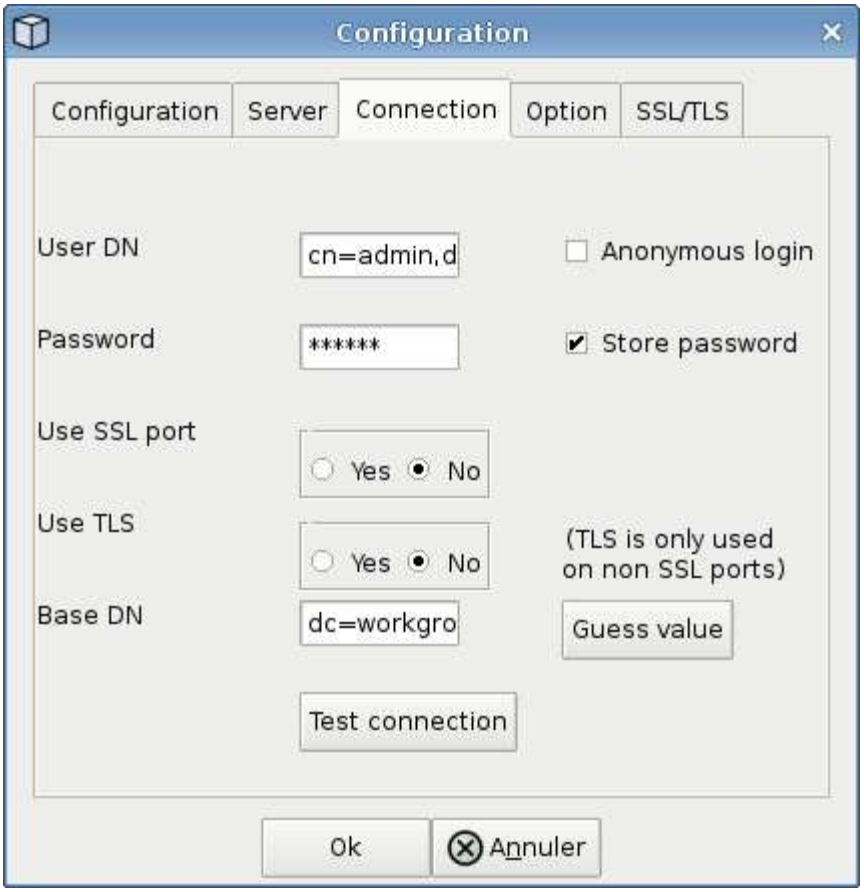
Testando a configuração do coletor do diretório de usuários

Você pode validar permissões de Usuário LDAP e Definições de Atributo usando os seguintes procedimentos:

- Use o seguinte comando para validar a permissão de usuário LDAP de segurança de workload:

```
 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, exibir
propriedades e atributos de objetos, exibir permissões, exibir o esquema
de um objeto, executar pesquisas sofisticadas que você pode salvar e
executar novamente.
```

  - Instale o LDAP Explorer (http://ldaptool.sourceforge.net/) ou o Java LDAP (http://jxplorer.org/Explorer) em qualquer máquina Windows que possa se conetar ao servidor LDAP.
  - Conete-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 resoluções que podem ocorrer durante a configuração do coletor:

Problema:	Resolução:
Adicionar um conetor de diretório LDAP resulta no estado "erro". O erro diz: "Credenciais inválidas fornecidas para o servidor LDAP".	DN de vinculação ou Senha de vinculação incorreta ou base de pesquisa fornecida. Edite e forneça as informações corretas.
Adicionar um conetor de diretório LDAP resulta no estado "erro". Erro diz: "Falha ao obter o objeto correspondente a DN	Base de pesquisa incorreta fornecida. Edite e forneça o nome correto da floresta.
Os atributos opcionais do usuário de domínio não estão aparecendo na página Perfil de usuário de Segurança de carga de trabalho.	Isso provavelmente se deve a uma incompatibilidade entre os nomes de atributos opcionais adicionados no CloudSecure e os nomes de atributos reais no ative Directory. Os campos são sensíveis a maiúsculas e minúsculas. Edite e forneça o(s) nome(s) do atributo opcional correto(s).
Coletor de dados no estado de erro com "Falha ao recuperar usuários LDAP. Motivo da falha: Não é possível conetar no servidor, a conexão é nula"	Reinicie o coletor clicando no botão *Restart*.

Problema:	Resolução:
Adicionar um conetor de diretório LDAP resulta no estado "erro".	Certifique-se de que forneceu valores válidos para os campos obrigatórios (servidor, nome da floresta, bind-DN, bind-Password). Certifique-se de que a entrada bind-DN é sempre fornecida como
Adicionar um conetor de diretório LDAP resulta no estado "TENTAR NOVAMENTE". Mostra o erro "Falha ao determinar a integridade do coletor, portanto, tentar novamente"	Certifique-se de que o IP do servidor e a base de pesquisa estão corretos ///
Ao adicionar o diretório LDAP, o seguinte erro é mostrado: "Falha ao determinar a integridade do coletor dentro de 2 tentativas, tente reiniciar o coletor novamente (Código de erro: AGENT008)"	Certifique-se de que o IP do servidor e a base de pesquisa estão corretos
Adicionar um conetor de diretório LDAP resulta no estado "TENTAR NOVAMENTE". Mostra o erro "não é possível definir o estado do comando Collector,Reason TCP [Connect(localhost:35012,None,List(),some(,seconds),true)] falhou por causa de java.net.ConnectionException:Connection recusado."	IP ou FQDN incorreto fornecido para o servidor AD. Edite e forneça o endereço IP ou FQDN correto. ///
Adicionar um conetor de diretório LDAP resulta no estado "erro". O erro diz: "Falha ao estabelecer a 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 conetor 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. Razão específica: /Connector/conf/application.conf: 70: LDAP.ldap-port tem STRING de tipo em vez DE NÚMERO"	Valor incorreto para a porta fornecida. Tente usar os valores de porta padrão ou o número de porta correto para o servidor AD.
Comecei com os atributos obrigatórios, e funcionou. Depois de adicionar os opcionais, os dados de atributos opcionais não são obtidos do AD.	Isso provavelmente se deve a uma incompatibilidade entre os atributos opcionais adicionados no CloudSecure e os nomes de atributos reais no ative Directory. Edite e forneça o nome do atributo obrigatório ou opcional correto.
Depois de reiniciar o coletor, quando acontecerá a sincronização LDAP?	A sincronização LDAP ocorrerá imediatamente após o coletor ser reiniciado. Levará aproximadamente 15 minutos para obter dados do usuário de aproximadamente 300K usuários e é atualizado a cada 12 horas automaticamente.
Os dados do usuário são sincronizados do LDAP para o CloudSecure. Quando os dados serão excluídos?	Os dados do usuário são mantidos para 13months em caso de não atualização. Se o locatário for excluído, os dados serão excluídos.

Problema:	Resolução:
O conetor de diretório LDAP resulta no estado "erro". "O conetor está no estado de erro. Nome do serviço: UsersLdap. Motivo da falha: Falha ao recuperar usuários LDAP. Motivo da falha: 80090308: LdapErr: DSID-0C090453, comentário: AcceptSecurityContext error, data 52e, v3839"	Nome da floresta incorreto fornecido. Veja acima como fornecer o nome correto da floresta.
O número de telefone não está a ser preenchido na página de perfil de utilizador.	Isso é provavelmente devido a um problema de mapeamento de atributos com o ative Directory. 1. Edite o coletor específico do ative Directory que está obtendo as informações do usuário do ative Directory. 2. Em atributos opcionais, há um nome de campo "número de telefone" mapeado para o atributo do ative Directory 'número de telefone'. 4. Agora, utilize a ferramenta Explorador do ative Directory conforme descrito acima para navegar no servidor LDAP Directory e ver o nome do atributo correto. 3. Certifique-se de que no diretório LDAP existe um atributo chamado "número de telefone" que tem realmente 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 CloudSecure User Directory. Na seção de atributo opcional, substitua 'número de telefone' por 'número de telefone'. 7. Salve o coletor do ative Directory, o coletor reiniciará e obterá o número de telefone do usuário e exibirá o mesmo na página do perfil do usuário.
Se o certificado de encriptação (SSL) estiver ativado no servidor AD (ative Directory), o Coletor do diretório de utilizadores de Segurança de carga de trabalho não pode ligar-se ao servidor AD.	Desative a criptografia do AD Server antes de configurar um coletor de diretório de usuários. Uma vez que os detalhes do usuário são obtidos, ele estará lá por 13 meses. Se o servidor AD for desconetado após buscar os detalhes do usuário, os usuários recém-adicionados no AD não serão obtidos. Para buscar novamente, o coletor de diretório do usuário precisa ser conetado ao AD.

Configurando o coletor de dados SVM do ONTAP

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 .

Mudanças globais podem ter um impacto potencial em seus sistemas ONTAP . É altamente recomendável fazer alterações que afetem um grande número de coletores de dados fora dos horários de pico.

Antes de começar

- Este coletor de dados é suportado com o seguinte:
  - Data ONTAP 9,2 e versões posteriores. Para obter o melhor desempenho, use uma versão do Data ONTAP superior a 9.13.1.
  - Protocolo SMB versão 3,1 e anterior.
  - Versões de NFS até NFS 4,1 (observe que o NFS 4,1 é compatível com ONTAP 9,15 ou posterior).
  - O FlexGroup é suportado a partir do 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.
  - O ONTAP Select é suportado
- Somente SVMs do tipo de dados são compatíveis. SVMs com volumes infinitos não são compatíveis.
- O SVM tem vários subtipos. Destes, apenas *default*, *Sync_source* e *Sync_destination* são suportados.
- Um agente "tem de ser configurado" antes de poder configurar coletores de dados.
- Certifique-se de ter um conetor do diretório de usuário configurado corretamente, caso contrário, os eventos mostrarão nomes de usuário codificados e não o nome real do usuário (como armazenado no ative Directory) na página "Activity Forensics".
- • O ONTAP Persistent Store é suportado a partir de 9.14.1.
- Para um desempenho ideal, você deve configurar o servidor FPolicy para estar na mesma sub-rede que o sistema de armazenamento.
- É necessário 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 do gerenciamento de cluster. ***este é o método recomendado.***
    - O nome da SVM deve ser exatamente como mostrado no ONTAP e diferencia maiúsculas de minúsculas.
  - Usando o SVM Management IP, Nome de usuário e Senha
  - Se você não puder ou não estiver disposto a usar o nome de usuário e senha completos do gerenciamento do cluster do administrador/SVM, você poderá criar um usuário personalizado com Privileges menor, conforme mencionado na "Uma nota sobre permissões"seção abaixo. É possível criar esse usuário personalizado para SVM ou acesso a cluster.
    - O você também pode usar um usuário do AD com uma função que tenha pelo menos as permissões de csrole como mencionado na seção "Uma nota sobre permissões" abaixo. Consulte também a "Documentação do ONTAP".
- Verifique se os aplicativos corretos estão 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 SVM, o nome do servidor CIFS e os campos adicionais.

- Defina uma senha para o usuário SVM vsadmin. Se estiver usando usuário personalizado ou usuário de administrador de cluster, pule esta etapa. Clustershell:> `security login password -username vsadmin -vserver svmname`
- Desbloqueie o usuário do SVM vsadmin para acesso externo. Se estiver usando usuário personalizado ou usuário de 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 está definida como 'gmt' (não 'data'). Ignore esta etapa se estiver usando um lif de gerenciamento dedicado para adicionar o SVM. Clustershell:> `network interface modify -lif <SVM_data_LIF_name> -firewall-policy mgmt`
- Quando um firewall está ativado, você deve ter uma exceção definida para permitir tráfego TCP para a porta usando o coletor de dados Data ONTAP.

  "Requisitos do agente"Consulte 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 storage devem estar na mesma VPC. Se estiverem em VPCs separados, deve haver uma rota válida entre as VPC.

Test Connectivity for Data Collectors

The test connectivity feature (introduced March 2025) aims to help end users identify the specific causes of failures when setting up data collectors in Data Infrastructure Insights (DII) Workload Security. This allows the users to self-correct issues related to network communication or missing roles.

This feature will help users determine if all network-related checks are in place before setting up a data collector. Additionally, it will inform users about the features they can access based on the ONTAP version, roles, and permissions assigned to them in ONTAP.

Test connectivity is not supported for User Directory collectors

Prerequisites for Connection Testing

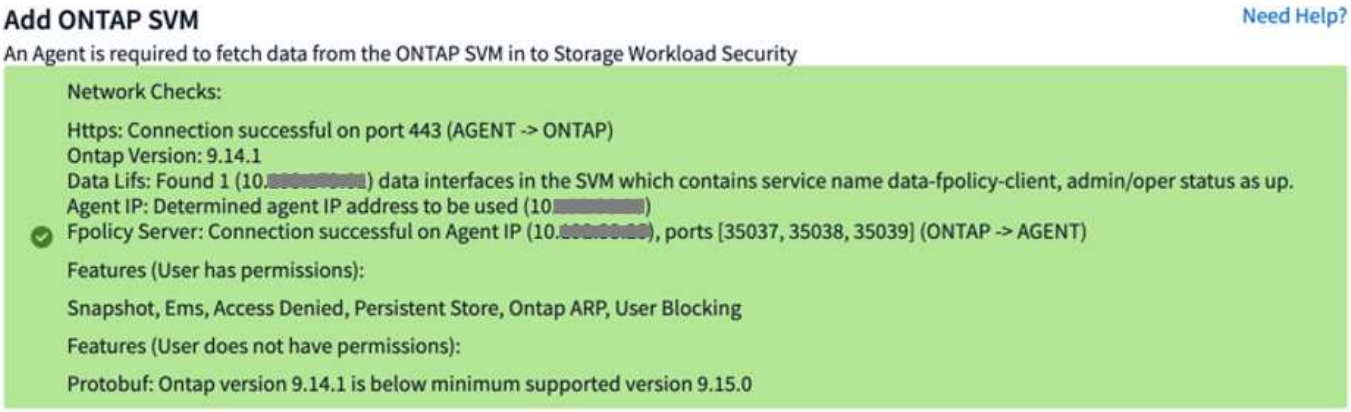
- Cluster level credentials are needed for this feature to work in full.
- Feature access check is not supported in SVM mode.
- Se você estiver usando credenciais de administração de cluster, não serão necessárias novas permissões.

- If you are using a custom user (e.g., *csuser*), provide the mandatory permissions and feature specific permissions for the features you want to use.

Be sure to review the Permissões section below as well.

Test the Connection

The user can go to the add/edit collector page, enter the cluster level details (in Cluster Mode) or SVM level details (in SVM Mode), and click on the **Test Connection** button. Workload Security will then process the request and display an appropriate success or failure message.



Pré-requisitos para bloqueio de acesso do usuário

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

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

Se você estiver usando credenciais de administração de cluster, não serão necessárias novas permissões.

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 conceder permissões ao Workload Security para bloquear o usuário.

Uma Nota sobre permissões

Permissões ao adicionar via Cluster Management IP:

Se você não puder usar o usuário administrador de gerenciamento de cluster para permitir que a Segurança de carga de trabalho acesse o coletor de dados ONTAP SVM, você poderá criar um novo usuário chamado "csuser" com as funções como mostrado nos comandos abaixo. Use o nome de usuário "csuser" e a senha para "csuser" ao configurar o coletor de dados do Workload Security para usar o Cluster Management IP.

Observação: Você pode criar uma única função para usar para todas as permissões de recursos para um usuário personalizado. Se houver um usuário existente, exclua primeiro o usuário existente e a função 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, faça 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 SVM Management IP:

Se você não puder usar o usuário administrador de gerenciamento de cluster para permitir que a Segurança de carga de trabalho acesse o coletor de dados ONTAP SVM, você poderá criar um novo usuário chamado "csuser" com as funções como mostrado nos comandos abaixo. Use o nome de usuário "csuser" e a senha para "csuser" ao configurar o coletor de dados do Workload Security para usar o SVM Management IP.

Observação: Você pode criar uma única função para usar para todas as permissões de recursos para um usuário personalizado. Se houver um usuário existente, exclua primeiro o usuário existente e a função 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, faça 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 o <vservername> pelo nome do SVM antes e execute 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

A Segurança da carga de trabalho configurará o mecanismo FPolicy no modo protobuf quando esta opção estiver ativada nas configurações *Advanced Configuration* do coletor. O modo Protobuf é suportado no ONTAP versão 9,15 e posterior.

Mais detalhes sobre esse recurso podem ser encontrados no "Documentação do ONTAP".

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

Modo de cluster:

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

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

Permissões para proteção autônoma contra ransomware do ONTAP e acesso à ONTAP negadas

Se você estiver usando credenciais de administração de cluster, não serão necessárias novas permissões.

Se você estiver usando um usuário personalizado (por exemplo, *csuser*) com permissões dadas ao usuário, siga as etapas abaixo para conceder permissões à Segurança de carga de trabalho para coletar informações relacionadas ao ARP do ONTAP.

Para obter mais informações, leia sobre "Integração com o ONTAP Access negada"

e "Integração com a proteção autônoma contra ransomware do ONTAP"

Configurar o coletor de dados

Passos para a configuração

1. Faça login como Administrador ou proprietário de conta no seu ambiente Data Infrastructure Insights.
2. Clique em **Workload Security > Collectors > 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. Introduza os dados necessários para cada campo.

Campo	Descrição
Nome	Nome exclusivo para o Data Collector
Agente	Selecione um agente configurado na lista.
Ligar através de IP de gestão para:	Selecione Cluster IP ou SVM Management IP
Endereço IP do 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 se conetar via IP de cluster)

Nome de utilizador	Nome de usuário para acessar o SVM/cluster ao adicionar via IP de cluster as opções são: 1. Cluster-admin 2. 'csuser' 3. AD-user com papel semelhante ao csuser. Ao adicionar via SVM IP, as opções são: 4. Vsadmin 5. 'csuser' 6. AD-username com função semelhante ao csuser.
Palavra-passe	Senha para o nome de usuário acima
Filtre compartilhamentos/volumes	Escolha se deseja incluir ou excluir compartilhamentos / volumes da coleção de eventos
Introduza nomes de partilha completos para excluir/incluir	Lista de compartilhamentos separados por vírgulas para excluir ou incluir (conforme apropriado) da coleção de eventos
Introduza nomes de volume completos para excluir/incluir	Lista de volumes separados por vírgulas para excluir ou incluir (conforme apropriado) da coleção de eventos
Monitorar o acesso à pasta	Quando marcada, ativa eventos para monitoramento de acesso a pastas. Observe que a pasta criar/renomear e excluir será monitorada mesmo sem essa opção selecionada. Ativar isto aumentará o número de eventos monitorizados.
Definir o tamanho do buffer de envio do ONTAP	Define o tamanho do buffer de envio do Fpolicy do ONTAP. Se uma versão do ONTAP anterior a 9.8p7 for usada e um problema de desempenho for visto, o tamanho do buffer de envio do ONTAP pode ser alterado para obter um desempenho aprimorado do ONTAP. Entre em Contato com o suporte da NetApp se você não vir essa opção e deseja explorá-la.

Depois de 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 atributos de configuração do coletor de dados.

Configuração recomendada para MetroCluster

O seguinte é recomendado para o 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 conetados 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**, a fim de se conetar ao coletor de origem 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 a 9,9.1, *data-fpolicy-client* não precisam ser definidas.

Play-Pause Data Collector

Se o Coletor de dados estiver no estado *Running*, você pode pausar a coleta. Abra o menu "três pontos" para o coletor e SELECIONE PAUSE. Enquanto o coletor está em pausa, nenhum dado é coletado do ONTAP e nenhum dado é enviado do coletor para o ONTAP. Isso significa que nenhum evento do Fpolicy fluirá do ONTAP para o coletor de dados e dali para Insights de infraestrutura de dados.

Observe que se novos volumes, etc. forem criados no ONTAP enquanto o coletor estiver em pausa, a Segurança de carga de trabalho não coletará os dados e esses volumes, etc., não serão refletidos em 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 purga de instantâneos não acontecerá de acordo com as configurações configuradas em um coletor pausado.
- Os eventos EMS (como ONTAP ARP) não serão processados em um coletor pausado. Isso significa que, se o ONTAP identificar um ataque de ransomware, a segurança de workloads da infraestrutura de dados não poderá adquirir esse evento.
- Os e-mails de notificações de saúde NÃO serão enviados para um coletor em pausa.
- Ações manuais ou automáticas (como captura Instantânea ou bloqueio do usuário) não serão suportadas em um coletor pausado.
- Nas atualizações do agente ou coletor, a VM do agente reinicia/reinicia ou a reinicialização do serviço do agente, um coletor pausado permanecerá no estado *Pausado*.
- Se o coletor de dados estiver no estado *Error*, o coletor não poderá ser alterado para o estado *Paused*. O botão Pausa será ativado somente se o estado do coletor for *Running*.
- Se o agente estiver desconetado, o coletor não poderá ser alterado para o estado *Pausado*. O coletor entrará no estado *stopped* e o botão Pausa será desativado.

Armazenamento persistente

O armazenamento persistente é suportado com o ONTAP 9.14,1 e posterior. Observe que as instruções de nome de volume variam de ONTAP 9.14 a 9,15.

O armazenamento persistente pode ser ativado selecionando a caixa de seleção na página de edição/adição do coletor. Depois de selecionar a caixa de verificação, é apresentado um campo de texto para aceitar o nome do volume. O nome do volume é um campo obrigatório para ativar o armazenamento persistente.

- Para ONTAP 9.14,1, você deve criar o volume antes de ativar o recurso e fornecer o mesmo nome no campo *Nome do volume*. O tamanho de volume recomendado é 16GB.
- Para ONTAP 9.15,1, o volume será criado automaticamente com tamanho 16GB pelo coletor, usando o nome fornecido no campo *Nome do volume*.

Permissões específicas são necessárias para o armazenamento persistente (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 SVM:

```
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 Workload Security de um agente para outro, permitindo o balanceamento de carga eficiente de coletores entre agentes.

Pré-requisitos

- O agente de origem deve estar no estado *Connected*.
- O coletor a ser migrado deve estar no estado *running*.

Nota:

- Migrar é suportado para coletores de dados e diretório de usuários.
- A migração de um coletor não é suportada para locatários gerenciados manualmente.

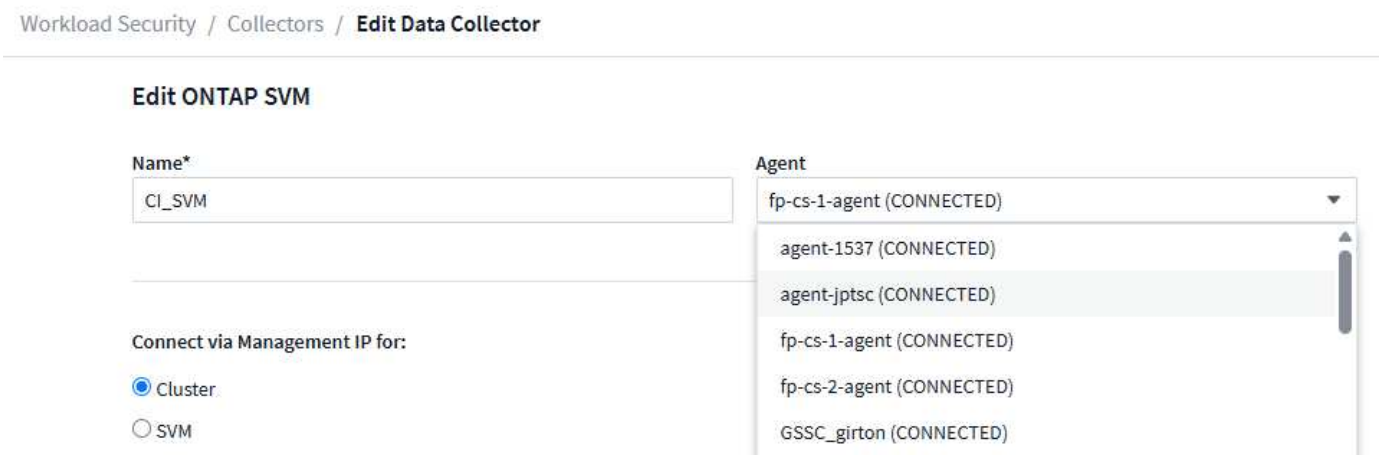
Migrar coletor

Para migrar um coletor, siga estas etapas:

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

A Segurança da carga de trabalho processará a solicitação. Na migração bem-sucedida, o usuário será redirecionado para a página de 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 êxito para o agente de destino.



Solução de problemas

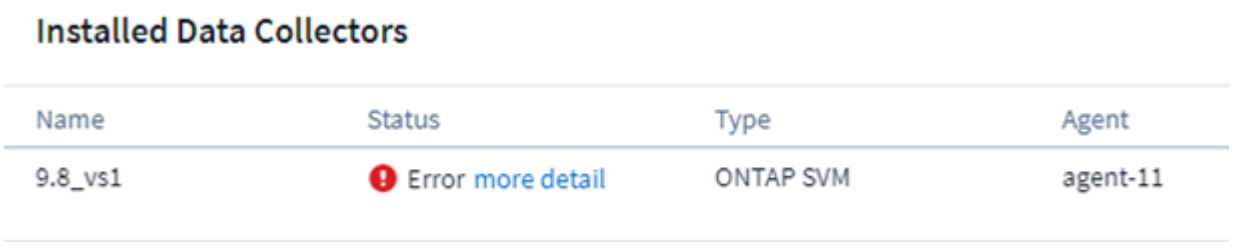
Consulte "Solução de problemas do SVM Collector"a página para obter dicas de solução de problemas.

Solução de problemas do coletor de dados SVM do ONTAP

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.

Consulte "Configurando o SVM Collector"a página para obter instruções sobre como configurar este coletor.

No caso de um 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 resoluções são descritos abaixo.

- Problema:* Data Collector é executado por algum tempo e pára após um tempo aleatório, falhando com: "Mensagem de erro: O conetor está em estado de erro. Nome do serviço: Auditoria. Motivo da falha: Servidor fpolicy externo sobrecarregado."

Experimente: a taxa de eventos do ONTAP foi muito maior do que a caixa Agente pode lidar. Daí a conexão foi terminada.

Verifique o tráfego de pico no CloudSecure quando a desconexão aconteceu. Isso pode ser verificado na página **CloudSecure > Activity Forensics > All Activity**.

Se o tráfego agregado de pico for maior do que o que a caixa de agente pode lidar, consulte a página Verificador de taxa de eventos sobre como dimensionar a implantação do coletor em uma caixa de agente.

Se o Agente tiver sido instalado na caixa Agente antes de 4 de março de 2021, execute os seguintes comandos na caixa 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 a partir da IU após o redimensionamento.

Problema: Collector relata mensagem de erro: "Nenhum endereço IP local encontrado no conetor que pode alcançar as interfaces de dados do SVM". **Tente isto:** isto é provavelmente devido a um problema de rede no lado do ONTAP. Siga estes passos:

1. Certifique-se de que não haja firewalls na biblioteca de dados do SVM ou na biblioteca 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 as informações de dados e de gerenciamento do SVM sejam pingáveis na VM do agente. Em caso de problemas, verifique o gateway, a máscara de rede e as rotas para o lif.

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

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

   Se não for possível fazer o ping, verifique se as configurações de rede no ONTAP estão corretas, para que a máquina do agente possa ser digitalizada.
3. Se você tentou se conetar via IP de cluster e não estiver funcionando, tente se conetar diretamente via SVM IP. Consulte acima as etapas para se conetar via SVM IP.
4. Ao adicionar o coletor por meio de credenciais SVM IP e vsadmin, verifique se a função SVM LIF tem Data plus Mgmt ativada. Nesse caso, o ping para o SVM LIF funcionará, no entanto o SSH para o SVM LIF não funcionará. Em caso afirmativo, crie um LIF somente do SVM Mgmt e tente se conetar por meio desse LIF somente de gerenciamento da SVM.
5. Se ainda não estiver funcionando, crie um novo SVM LIF e tente se conetar por meio desse LIF. Certifique-se de que a máscara de sub-rede está corretamente definida.
6. Depuração avançada:
   a. Inicie um rastreamento de pacote no ONTAP.
   b. Tente conetar um coletor de dados à SVM a partir da IU do CloudSecure.
   c. Aguarde até que o erro seja exibido. 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_trac
      es/
      .. Certifique-se de que existe um SYN de ONTAP para a caixa
      Agente.
      .. Se não houver SYN do ONTAP, então é um problema com firewall
      no ONTAP.
      .. Abra o firewall no ONTAP, para que o ONTAP possa conetar a
      caixa de agente.
      ```
7. Se ainda não estiver funcionando, consulte a equipe de rede para garantir que nenhum firewall externo esteja bloqueando a conexão do ONTAP à caixa Agente.

8. Se nenhuma das opções acima resolver o problema, abra um caso com "Suporte à NetApp" para obter mais assistência.

Problema: mensagem: "Falha ao determinar o tipo de ONTAP para [hostname: <IP Address>. Motivo: Erro de conexão com o sistema de armazenamento <IP Address>: O host está inacessível (o host não pode ser acessado)" **Tente isto:**

1. Verifique se o endereço de gerenciamento de IP do SVM correto ou o IP de gerenciamento de cluster foram fornecidos.
2. SSH para o SVM ou cluster ao qual você pretende se conetar. Depois de conectar, verifique se o SVM ou o nome do cluster estão corretos.

Problema: mensagem de erro: "O conetor está no estado de erro. service.name: Auditoria. Motivo da falha: Servidor fpolicy externo encerrado." **Tente 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 conete a partir do SVM. Certifique-se também de que não há firewalls ativados a partir da comunicação de bloqueio do lado do ONTAP para a máquina do agente.
2. Digite o seguinte comando na caixa Agente e verifique se o intervalo de portas está aberto.

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

   A saída da amostra deve parecer:

   ```
    -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack
   -ctstate NEW -j ACCEPT
   . Faça 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. Faça ping na caixa Agente a partir do SVM data lif (com suporte a protocolos CIFS, NFS) e certifique-se de que o ping esteja funcionando:

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

   Se não for possível fazer o ping, verifique se as configurações de rede no ONTAP estão corretas, para que a máquina do agente possa ser digitalizada.

4. Se um único SVM for adicionado duas vezes a um locatário por meio de coletores de dados 2, esse erro será mostrado. Exclua um dos coletores de dados através da IU. Em seguida, reinicie o outro coletor de dados através da IU. Em seguida, o coletor de dados mostrará o status "EM EXECUÇÃO" e começará a receber eventos da SVM.

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

5. Nos casos em que o mesmo SVM foi adicionado em dois ambientes de segurança de workload (locatários) diferentes, o último sempre será bem-sucedido. O segundo coletor irá configurar o fpolicy com seu próprio endereço IP e expulsar o primeiro. Assim, 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. Este erro também pode ocorrer se as políticas de serviço não estiverem configuradas corretamente. Com o ONTAP 9.8 ou posterior, para se conetar ao coletor de origem de dados, o serviço de cliente data-fpolicy é necessário junto com o serviço de dados data-nfs e/ou data-cifs. Além disso, o serviço cliente data-fpolicy deve estar associado às lif(s) de dados do SVM monitorado.

Problema: nenhum evento visto na página de atividades. **Tente isto:**

1. Verifique se o coletor ONTAP está no estado "EM FUNCIONAMENTO". Se sim, certifique-se de que alguns eventos cifs estão sendo gerados nas VMs 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
   ```

   Por favor, certifique-se de que não existem erros relacionados ao fpolicy.

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

   ```
   <SVM>fpolicy show
   ```

   Verifique se a política fpolicy nomeada com o prefixo "cloudsecure_" foi definida e o status está "ligado". Se não estiver definido, é provável que o Agente não consiga executar os comandos na SVM. Certifique-se de que todos os pré-requisitos, conforme descrito no início da página, foram seguidos.

Problema: o SVM Data Collector está no estado de erro e a mensagem de erro é "o agente falhou ao conetar-se ao coletor" **Tente isto:**

1. Muito provavelmente, o Agente está sobrecarregado e não consegue se conetar aos coletores de origem de dados.
2. Verifique quantos coletores de fonte de dados estão conetados ao Agente.
3. Verifique também a taxa de fluxo de dados na página "todas as atividades" na IU.
4. Se o número de atividades por segundo for significativamente alto, instale outro Agente e mova alguns dos coletores de origem de dados para o novo Agente.

Problema: o SVM Data Collector mostra uma mensagem de erro como "Falha no nó fpolicy.server.connectError: ao estabelecer uma conexão com o servidor FPolicy "12.195.15.146" (motivo: "Selecionar limite de tempo")" **Experimente:** o firewall está habilitado no SVM/Cluster. Portanto, o mecanismo fpolicy não consegue se conetar 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.

Problema: mensagem de erro: "O conetor está no 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: Up) encontrada no SVM." **Tente isto:** Certifique-se de que existe uma interface operacional (tendo papel como protocolo de dados e dados como CIFS/NFS.

Problema: o coletor de dados entra em estado de erro e, em seguida, entra em ESTADO DE EXECUÇÃO após algum tempo, em seguida, volta para erro novamente. Este ciclo repete-se. **Tente isto:** isso normalmente acontece no seguinte cenário:

1. Há vários coletores de dados adicionados.
2. Os coletores de dados que mostram esse tipo de comportamento terão 1 SVM adicionados a esses coletores de dados. Ou seja, 2 ou mais coletores de dados estão conetados ao 1 SVM.
3. Garantir que o coletor de dados do 1 se conecte apenas ao 1 SVM.
4. Exclua os outros coletores de dados que estão conetados ao mesmo SVM.

Problema: o conetor está no estado de erro. Nome do serviço: Auditoria. Motivo da falha: Falha ao configurar (política no SVM svmname. Motivo: Valor inválido especificado para o elemento 'hares-to-include' dentro de 'fpolicy.policy.scope-moDIMY: "Federal" **Tente isto:** *os nomes de compartilhamento precisam ser dados 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 compartilhamento. Use a filtragem por volume se você tiver um grande número de compartilhamentos para incluir ou excluir.

Problema: existem fpolíticas existentes no cluster que não são usadas. O que deve ser feito com eles antes da instalação do Workload Security? **Tente isto:** recomenda-se excluir todas as configurações de fpolicy não utilizadas existentes, mesmo que estejam no estado desconetado. A segurança da carga de trabalho criará fpolicy com o prefixo "cloudsecure_". Todas as outras configurações de 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>
```

|depois de ativar a segurança de carga de trabalho, o desempenho do ONTAP é afetado: A latência se torna esporadicamente alta, os IOPs se tornam esporadicamente baixos. |ao usar o ONTAP com segurança de workload, às vezes, problemas de latência podem ser vistos no ONTAP. Há uma série de razões possíveis para isso, como observado no seguinte: "1372994" "1415152", , "1438207", "1479704", "1354659". Todos esses problemas são corrigidos no ONTAP 9.13,1 e posterior; é altamente recomendável usar uma dessas versões posteriores.

Problema: Data Collector está em erro, mostra esta mensagem de erro. "Erro: O conetor está no estado de erro. Nome do serviço: Auditoria. Motivo da falha: Falha ao configurar a política no SVM.svm_test. Motivo: Valor ausente para o campo zapi: Eventos. * Experimente isto:*

1. Comece com um novo SVM com apenas o serviço NFS configurado.
2. Adicione um coletor de dados do ONTAP SVM na segurança de workload. O CIFS é configurado como um protocolo permitido para o SVM, ao mesmo tempo em que adiciona o coletor de dados ONTAP SVM na segurança de workload.
3. Aguarde até que o coletor de dados no Workload Security mostre um erro.
4. Como o servidor CIFS NÃO está configurado na SVM, esse erro, como mostrado à esquerda, é mostrado pela Segurança de workload.
5. Edite o coletor de dados ONTAP SVM e desmarque o protocolo CIFS conforme permitido. Salve o coletor de dados. Ele começará a ser executado somente com o protocolo NFS ativado.

Problema: Data Collector mostra a mensagem de erro: "Erro: Falha ao determinar a integridade do coletor dentro de 2 tentativas, tente reiniciar o coletor novamente (Código de erro: AGENT008)". **Tente isto:**

1. Na página coletores de dados, role para a direita do coletor de dados dando o erro e clique no menu 3 pontos. Selecione *Edit*. Introduza novamente a palavra-passe do coletor de dados. Salve o coletor de dados pressionando o botão *Save*. O Data Collector será reiniciado e o erro deve ser resolvido.
2. A máquina Agent pode não ter espaço suficiente para CPU ou RAM, é por isso que os DSCs estão falhando. Verifique o número de coletores de dados que são adicionados ao Agente na máquina. Se for superior a 20 GB, aumente a capacidade de CPU e RAM da máquina Agent. Uma vez que a CPU e a RAM forem aumentadas, os DSCs entrarão em Initializing (Inicializar) e, em seguida, no estado Running (execução) automaticamente. Veja o guia de dimensionamento em "esta página".

Problema: o Data Collector está errando quando o modo SVM está selecionado. **Tente isto:** ao se conetar no modo SVM, se o IP de gerenciamento de cluster for usado para se conetar em vez do IP de gerenciamento SVM, a conexão falhará. Certifique-se de que o SVM IP correto seja usado.

Problema: Data Collector mostra uma mensagem de erro quando o recurso Acesso negado está ativado: "O conetor está no estado de erro. Nome do serviço: Auditoria. Motivo da falha: Falha ao configurar o fpolicy no SVM test_svm. Motivo: O usuário não está autorizado." **Tente:** o usuário pode estar perdendo as PERMISSÕES DE DESCANSO necessárias para o recurso Acesso negado. Siga as instruções em "esta página" para definir as permissões.

Reinicie o coletor assim que as permissões estiverem definidas.

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

Configurando o Cloud Volumes ONTAP e o Amazon FSX para NetApp ONTAP Collector

O Workload Security usa coletores de dados para coletar dados de acesso de arquivos e usuários de dispositivos.

Configuração de armazenamento Cloud Volumes ONTAP

Consulte a documentação do OnCommand Cloud Volumes ONTAP para configurar uma instância do AWS de nó único/HA para hospedar o agente de segurança de carga de trabalho: https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html

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

Plataformas compatíveis

- Cloud Volumes ONTAP, compatível com todos os fornecedores de serviços de nuvem disponíveis, onde disponível. Por exemplo: Amazon, Azure, Google Cloud.

- ONTAP no FSX

Configuração da Máquina do Agente

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

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

Na AWS, siga as etapas a seguir para configurar a máquina a ser usada como agente de segurança de carga de trabalho:

Siga as etapas a seguir para configurar a máquina a ser usada como agente de segurança de carga de trabalho:

Passos

1. Faça login no console da AWS e navegue até a página de instâncias EC2 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 EC2.
5. Instale os pacotes Linux necessários usando o gerenciador de pacotes YUM:
   a. Instale os pacotes Linux nativos *wget* e *unzip*.

Instale o agente de segurança de carga de trabalho

1. Faça login como Administrador ou proprietário de conta no seu ambiente Data Infrastructure Insights.
2. Navegue até Workload Security **Collectors** e clique na guia **Agents**.
3. Clique em * Agente* e especifique RHEL como a plataforma de destino.
4. Copie o comando Instalação do agente.
5. Cole o comando Agent Installation na instância RHEL EC2 na qual você está conetado. Isso instala o agente Workload Security, desde que todos os "Pré-requisitos do agente" sejam atendidos.

Para obter as etapas detalhadas, consulte este xref:./ https://docs.NetApp.com/US-en/cloudinsights/task_cs_add_Agent.html

Solução de problemas

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

Problema	Resolução

"Segurança de carga de trabalho: Falha ao determinar o tipo de ONTAP para o coletor de dados do Amazon FxSN" é mostrado pelo coletor de dados. O cliente não consegue adicionar um novo coletor de dados Amazon FSxN ao Workload Security. A conexão com o cluster FSxN na porta 443 do agente está esgotando. 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. Esse mesmo agente é usado para conetar e monitorar os dispositivos NetApp restantes (e todos eles estão funcionando).	Resolva esse problema adicionando o segmento de rede fsxadmin LIF à regra de segurança do agente. Permitido todas as portas se você não tiver certeza sobre as portas.

Gerenciamento de usuários

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

O Data Infrastructure Insights oferece quatro níveis de conta de usuário: Proprietário da conta, Administrador, Usuário e convidado. Cada conta recebe níveis de permissão específicos. Uma conta de usuário que tenha Privileges de administrador pode criar ou modificar usuários e atribuir a cada usuário uma das seguintes funções de segurança de carga de trabalho:

Função	Acesso à segurança do workload
Administrador	Pode executar todas as funções de Segurança de carga de trabalho, incluindo as de Alertas, Forensics, 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.
Utilizador	Pode visualizar e gerir Alertas e visualizar Forensics. A função de usuário pode alterar o status de alerta, adicionar uma nota, tirar snapshots manualmente e restringir o acesso do usuário.
Convidado	Pode visualizar Alertas e Forensics. A função convidado não pode alterar o status de alerta, adicionar uma nota, tirar snapshots manualmente ou restringir o acesso do usuário.

Passos

1. Faça login no Workload Security
2. No menu, clique em **Admin > User Management**

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

3. Selecione a função pretendida para cada utilizador.

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

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

Verificador de taxa de eventos SVM (Guia de dimensionamento de agentes)

O Verificador de taxa de eventos é usado para verificar a taxa de eventos combinados NFS/SMB no SVM antes de instalar um coletor de dados ONTAP SVM, para ver quantos SVMs uma máquina pode monitorar. Use o Event Rate Checker como um guia de dimensionamento para ajudar a Planejar seu ambiente de segurança.

Um agente pode suportar até um máximo de 50 coletores de dados.

Requisitos:

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

Ao executar esse script, nenhum coletor de dados SVM do ONTAP 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 _sshpass_ para ser instalado na máquina linux. Há
duas maneiras de instalá-lo:
```

   a. Execute o seguinte comando:

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

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

3. Forneça os valores corretos quando solicitado. Veja abaixo um exemplo.
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 do ONTAP SVM pode ser associado a um único SVM, ou seja, cada coletor de dados poderá receber o número de eventos gerados por um único SVM.

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 lidar
4 núcleo, 16GB	10 coletores de dados	20k eventos/seg
4 núcleo, 32GB	20 coletores de dados	20k eventos/seg

B) para calcular o total de eventos, adicione os Eventos gerados para todos os SVMs para esse agente.

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

B o C deve ser inferior A A, caso contrário, a máquina do Agente falhará em monitorar.

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

```
 Sum of all Event rate of all Data Source Collectors + Buffer Event rate
of 30% < 20000 events/second
Consulte
xref:{relative_path}concept_cs_agent_requirements.html["Requisitos do
agente"]a página para obter pré-requisitos e requisitos adicionais.
```

Exemplo

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

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 Agente no nome do arquivo *fpolicy_stat_<SVM Name>.log* no diretório de trabalho atual.

O script pode dar resultados errôneos nos seguintes casos:

- Credenciais, IP ou nome do SVM incorretos são fornecidos.
- Um fpolicy já existente com o mesmo nome, número de sequência, etc. irá dar 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	Resposta
Se eu executar esse script em um SVM que já esteja configurado para o Workload Security, ele só usará a configuração fpolicy existente no SVM ou configurará uma configuração 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 impactos.
Posso aumentar o número de SVMs em que o script pode ser executado?	Sim. Basta editar o script e alterar o número máximo de SVMs de 5 para qualquer número desejável.
Se eu aumentar o número de SVMs, isso aumentará o tempo de execução do script?	Não. O script será executado por um máximo de 5 minutos, mesmo que o número de SVMs seja aumentado.
Posso aumentar o número de SVMs em que o script pode ser executado?	Sim. Você precisa editar o script e alterar o número máximo de SVMs de 5 para qualquer número desejável.
Se eu aumentar o número de SVMs, isso aumentará o tempo de execução do script?	Não. O script será executado por um máximo de 5mins, mesmo que o número de SVMs seja aumentado.

O que acontece se eu executar o Event Rate Checker com um agente existente?	A execução do Event Rate Checker em relação a um agente já existente pode causar um aumento na latência do SVM. Este aumento será temporário por natureza enquanto o verificador de taxa de eventos estiver em execução.

Informações sobre direitos autorais

Informações sobre marcas comerciais