Segurança da Carga de Trabalho

Data Infrastructure Insights

NetApp
February 11, 2026

Índice

Segurança da Carga de Trabalho

Sobre a segurança da carga de trabalho de armazenamento

O Data Infrastructure Insights Storage Workload Security (antigo Cloud Secure) ajuda a proteger seus dados com inteligência acionável sobre ameaças internas. Ele fornece visibilidade e controle centralizados de todo o acesso a dados corporativos em ambientes de nuvem híbrida para garantir que as metas de segurança e conformidade sejam atendidas.

Visibilidade

Obtenha visibilidade e controle centralizados do acesso do usuário aos seus dados corporativos críticos armazenados no local ou na nuvem.

Substitua ferramentas e processos manuais que não fornecem visibilidade precisa e oportuna do acesso e controle de dados. O Workload Security opera exclusivamente em sistemas de armazenamento na nuvem e no local para fornecer alertas em tempo real sobre comportamento malicioso de usuários.

Proteção

Proteja os dados organizacionais contra uso indevido por usuários mal-intencionados ou comprometidos por meio de aprendizado de máquina avançado e detecção de anomalias.

Alerta você sobre qualquer acesso anormal a dados por meio de aprendizado de máquina avançado e detecção de anomalias no comportamento do usuário.

Conformidade

Garanta a conformidade corporativa auditando o acesso dos dados do usuário aos seus dados corporativos críticos armazenados no local ou na nuvem.

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

Componente	Requisitos do Linux
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

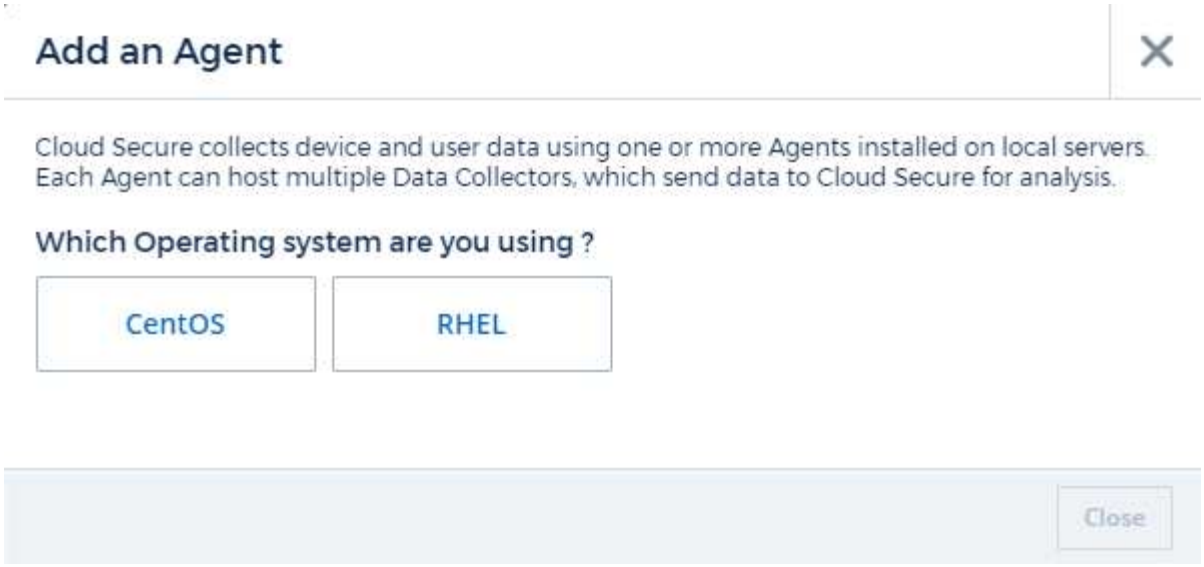
Antes de configurar seu agente do Workload Security, leve em consideração o seguinte.

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.

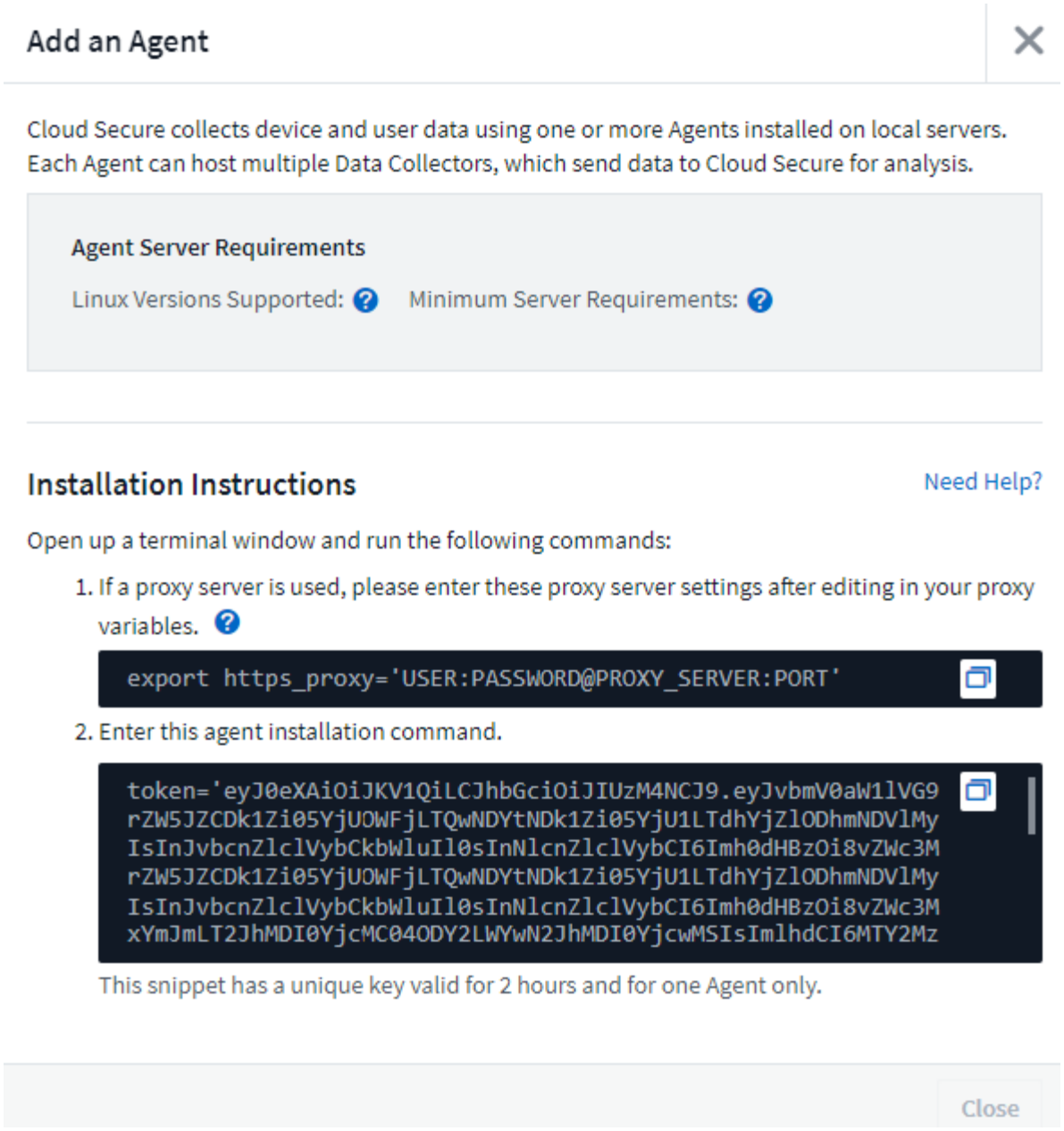
Etapas para instalar o agente

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
```

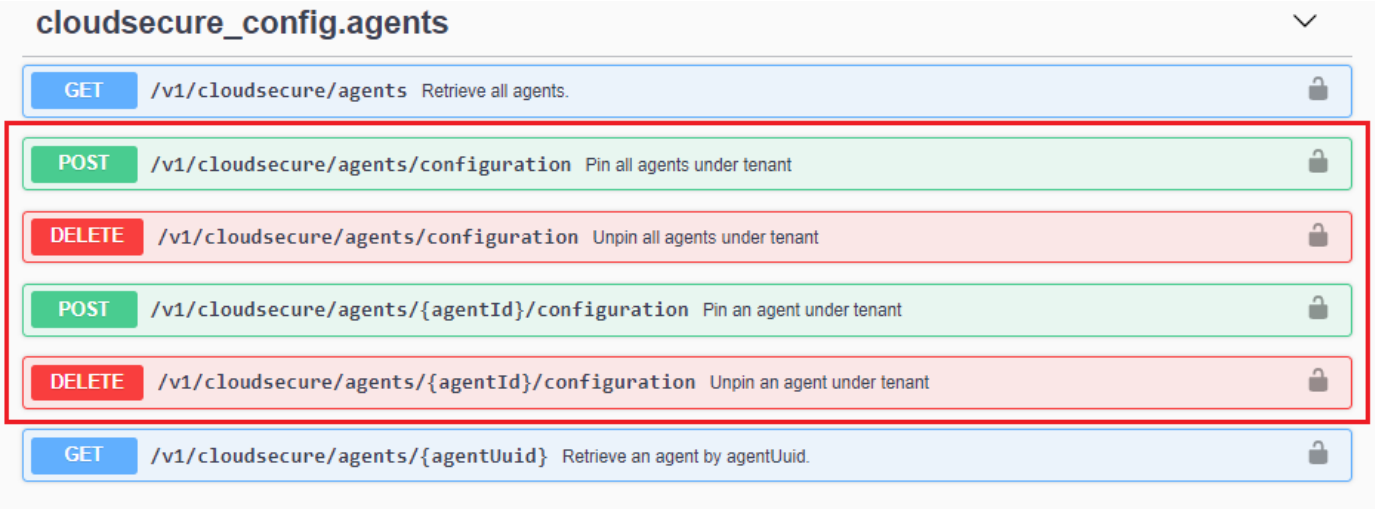
"Fixando" um Agente na versão atual

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.

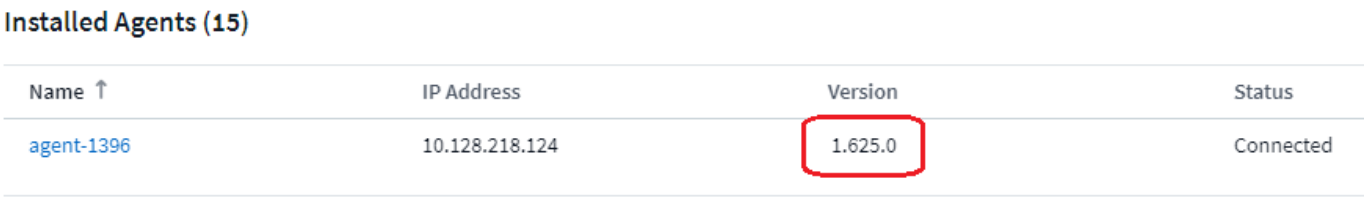
Em cada um desses casos, o agente será atualizado na próxima atualização do Workload Security.

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

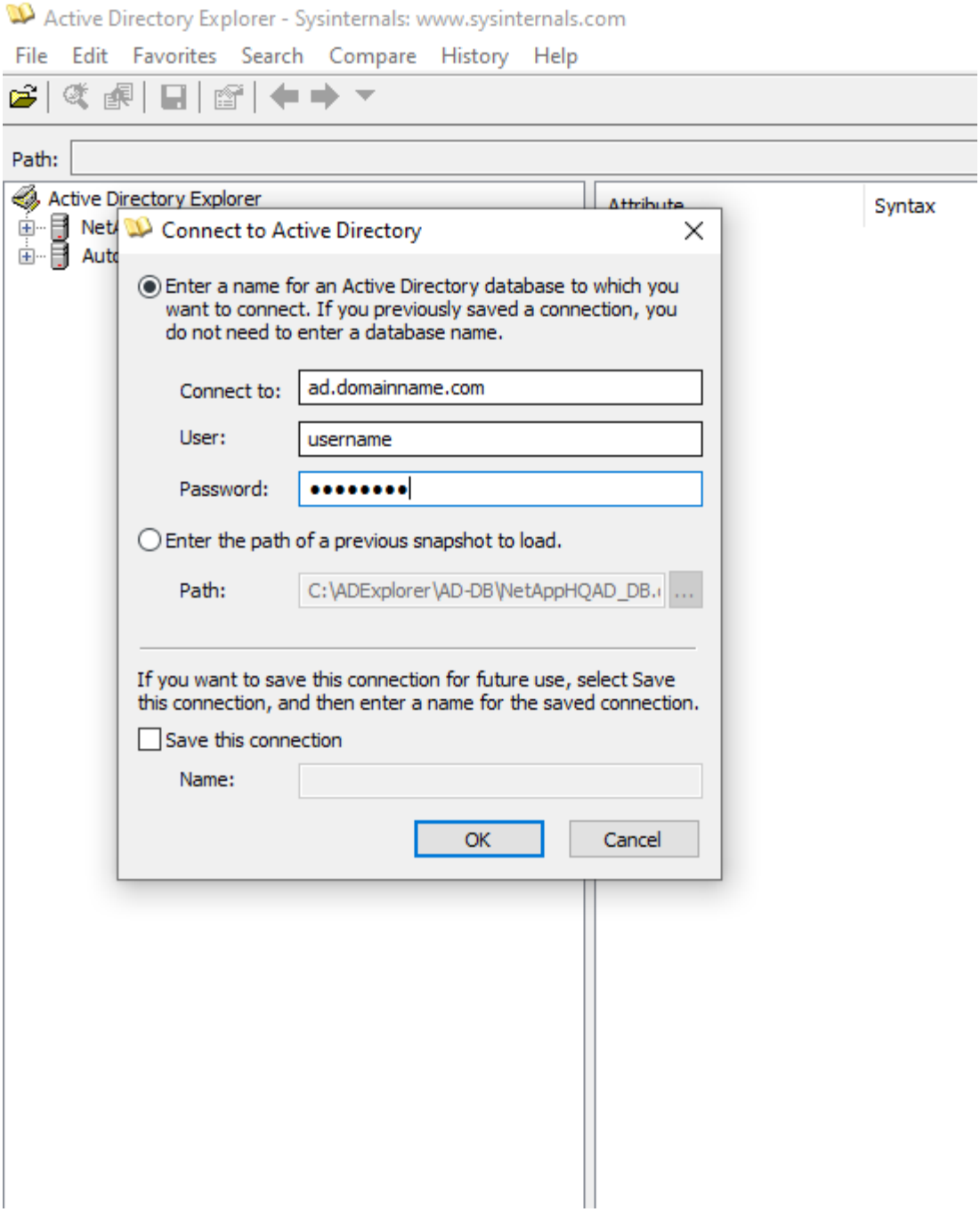
Testando a configuração do coletor de diretório do usuário

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:

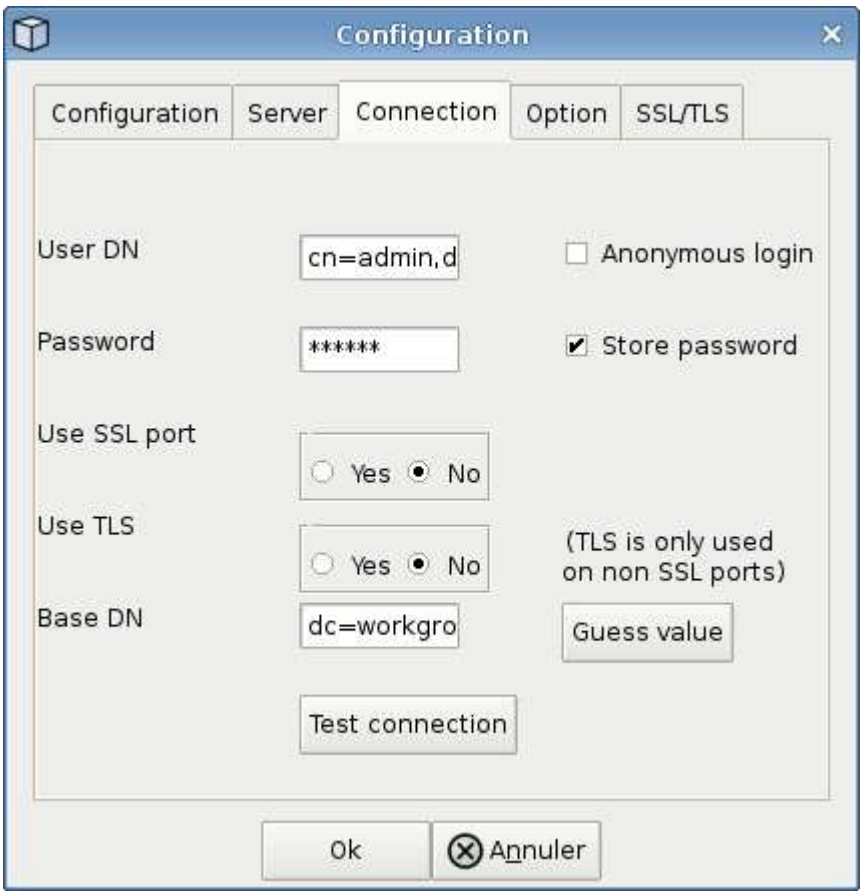
- Use o seguinte comando para validar a permissão do usuário LDAP do Workload Security:

```
 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

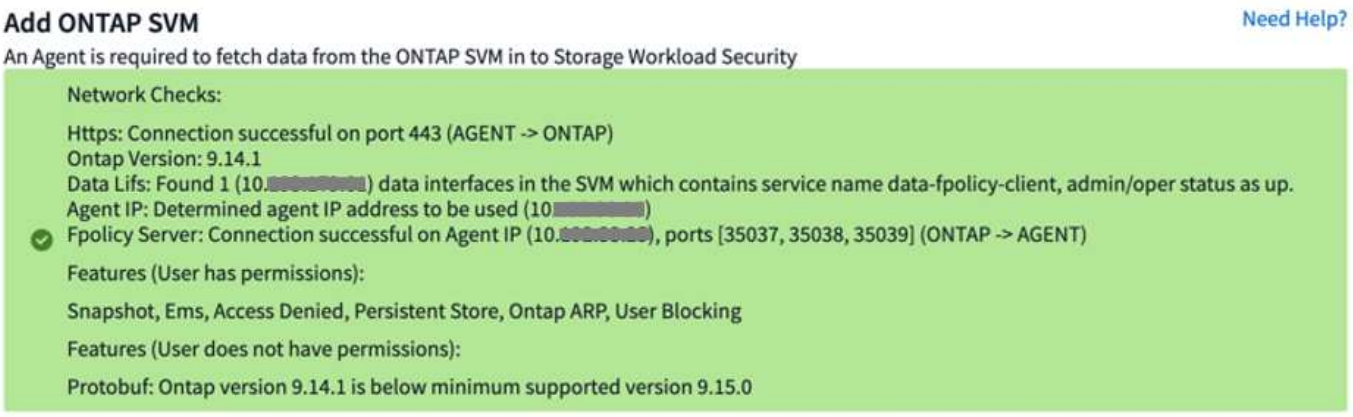
- Credenciais em nível de cluster são necessárias para que esse recurso funcione completamente.
- A verificação de acesso a recursos não é suportada no modo SVM.

- 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.

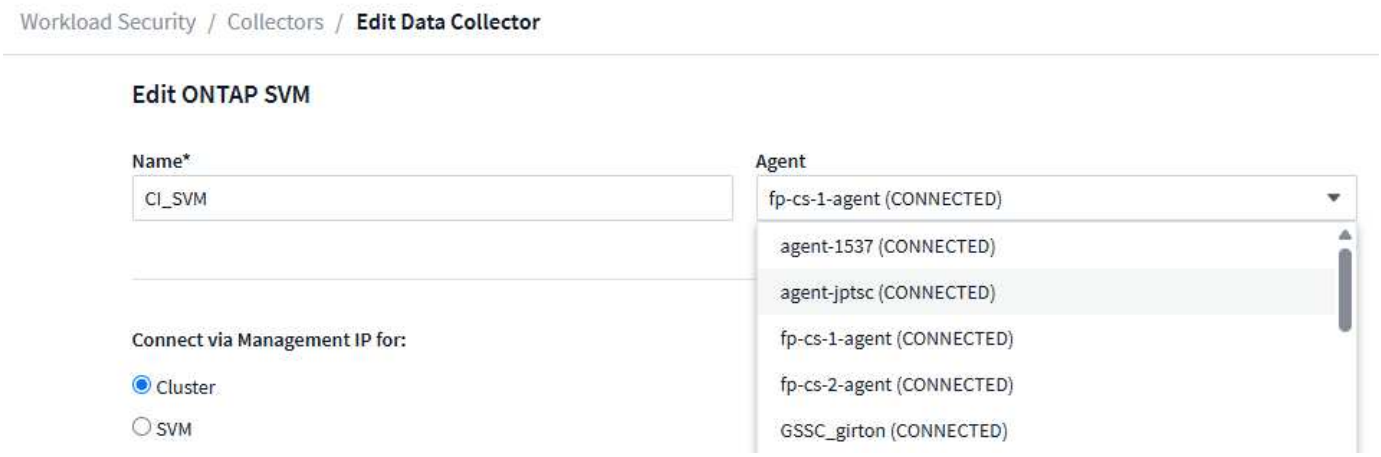
Migrar coletor

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

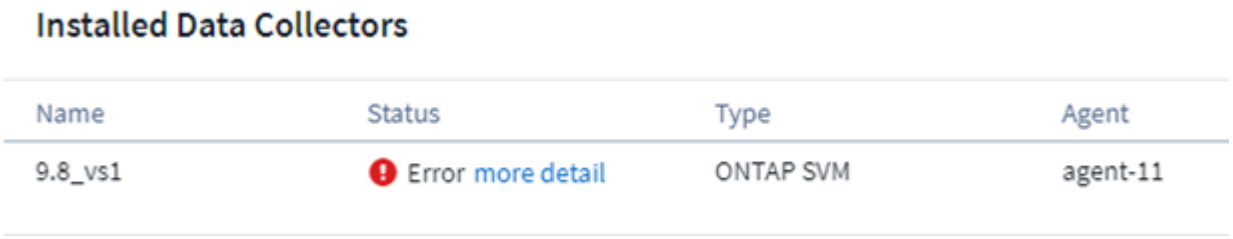
Veja o"Solução de problemas do coletor SVM" página para dicas de solução de problemas.

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]#
```

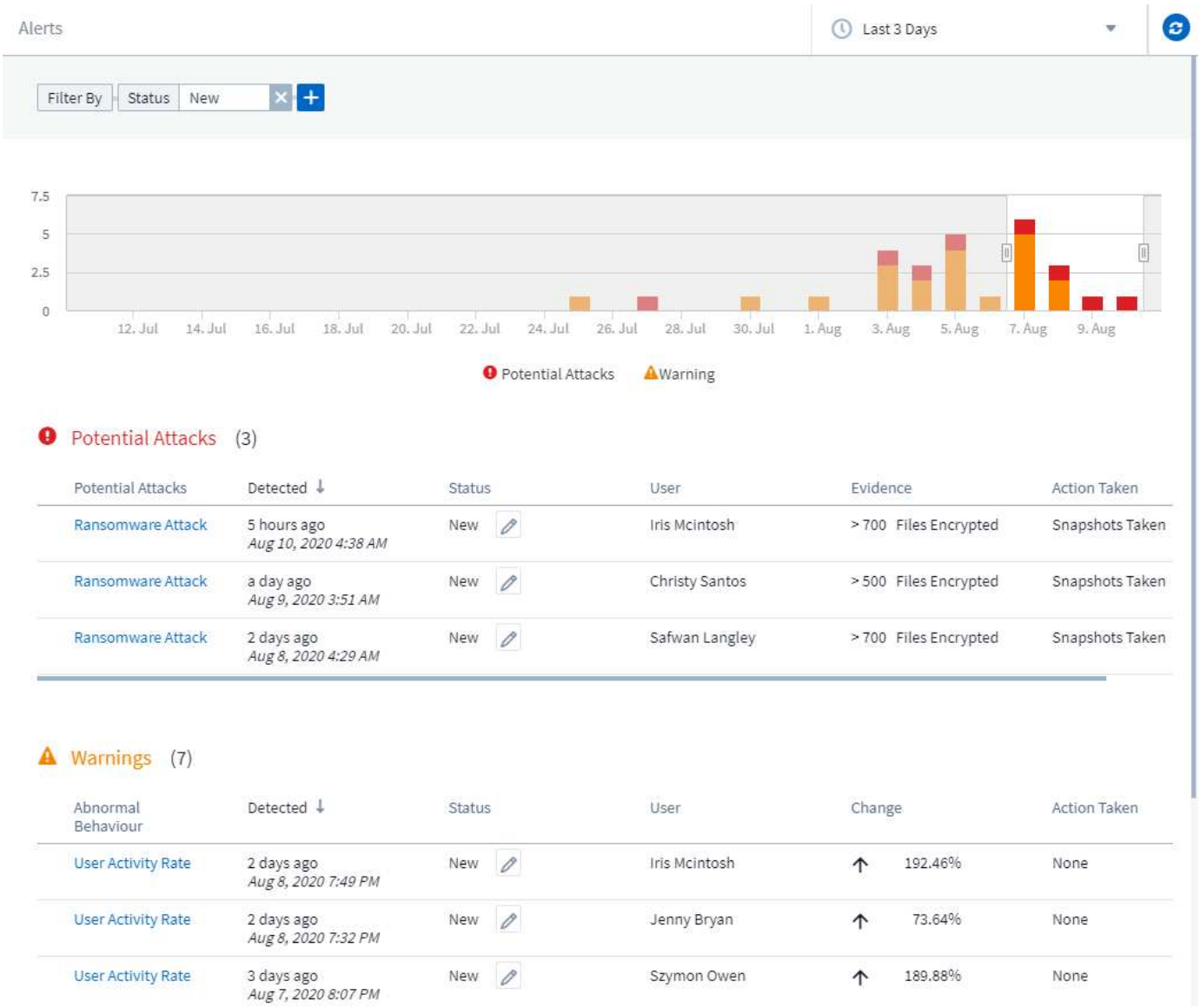
Solução de problemas

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.

Compreendendo e investigando alertas

A página de Alertas de Segurança de Carga de Trabalho fornece uma linha do tempo abrangente de ameaças e avisos detectados, com ferramentas de investigação detalhadas. Visualize detalhes de alertas, gerencie atualizações de status, filtre por critérios e acompanhe as atividades do usuário para investigar e responder a incidentes de segurança com eficiência.



Alerta

A lista de alertas exibe um gráfico mostrando o número total de ataques e/ou avisos potenciais que foram gerados no intervalo de tempo selecionado, seguido por uma lista dos ataques e/ou avisos que ocorreram nesse intervalo de tempo. Você pode alterar o intervalo de tempo ajustando os controles deslizantes de hora de início e hora de término no gráfico.

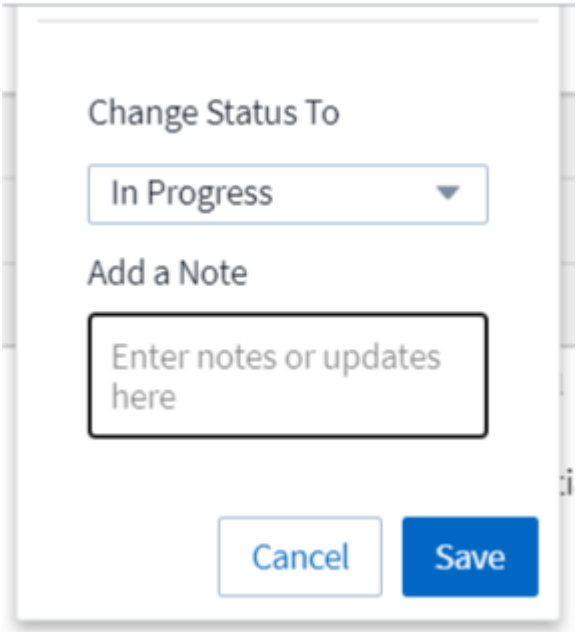
O seguinte é exibido para cada alerta:

Ataques potenciais:

- O tipo de ataque potencial (por exemplo, adulteração de arquivos ou sabotagem).
- A data e a hora em que o ataque potencial foi *Detectado*
- O *Status* do alerta:
  - **Novo**: Este é o padrão para novos alertas.
  - **Em andamento**: O alerta está sendo investigado por um ou mais membros da equipe.
  - **Resolvido**: O alerta foi marcado como resolvido por um membro da equipe.

◦ **Dispensado**: O alerta foi descartado como falso positivo ou comportamento esperado.

Um administrador pode alterar o status do alerta e adicionar uma nota para auxiliar na investigação.



- O *Usuário* cujo comportamento disparou o alerta
- *Evidência* do ataque (por exemplo, um grande número de arquivos foi criptografado)
- A *Ação tomada* (por exemplo, um instantâneo foi tirado)

Avisos:

- O *Comportamento Anormal* que desencadeou o aviso
- A data e a hora em que o comportamento foi *Detectado*
- O *Status* do alerta (Novo, Em andamento, etc.)
- O *Usuário* cujo comportamento disparou o alerta
- Uma descrição da *Mudança* (por exemplo, um aumento anormal no acesso a arquivos)
- A *Ação Tomada*

Opções de filtro

Você pode filtrar alertas pelo seguinte:

- O *Status* do alerta
- Texto específico na *Nota*
- O tipo de *Ataques/Avisos*
- O *Usuário* cujas ações acionaram o alerta/aviso

A página Detalhes do Alerta

Você pode clicar no link de um alerta na página da lista de alertas para abrir a página de detalhes do alerta. Os detalhes do alerta podem variar de acordo com o tipo de ataque ou alerta. Por exemplo, uma página de

detalhes de um ataque de adulteração de arquivos pode exibir as seguintes informações:

Seção de resumo:

- Tipo de ataque (adulteração de arquivos, sabotagem) e ID de alerta (atribuído pela segurança da carga de trabalho)
- Data e hora em que o ataque foi detectado
- Ação tomada (por exemplo, um instantâneo automático foi tirado. O horário do instantâneo é mostrado imediatamente abaixo da seção de resumo))
- Status (Novo, Em andamento, etc.)

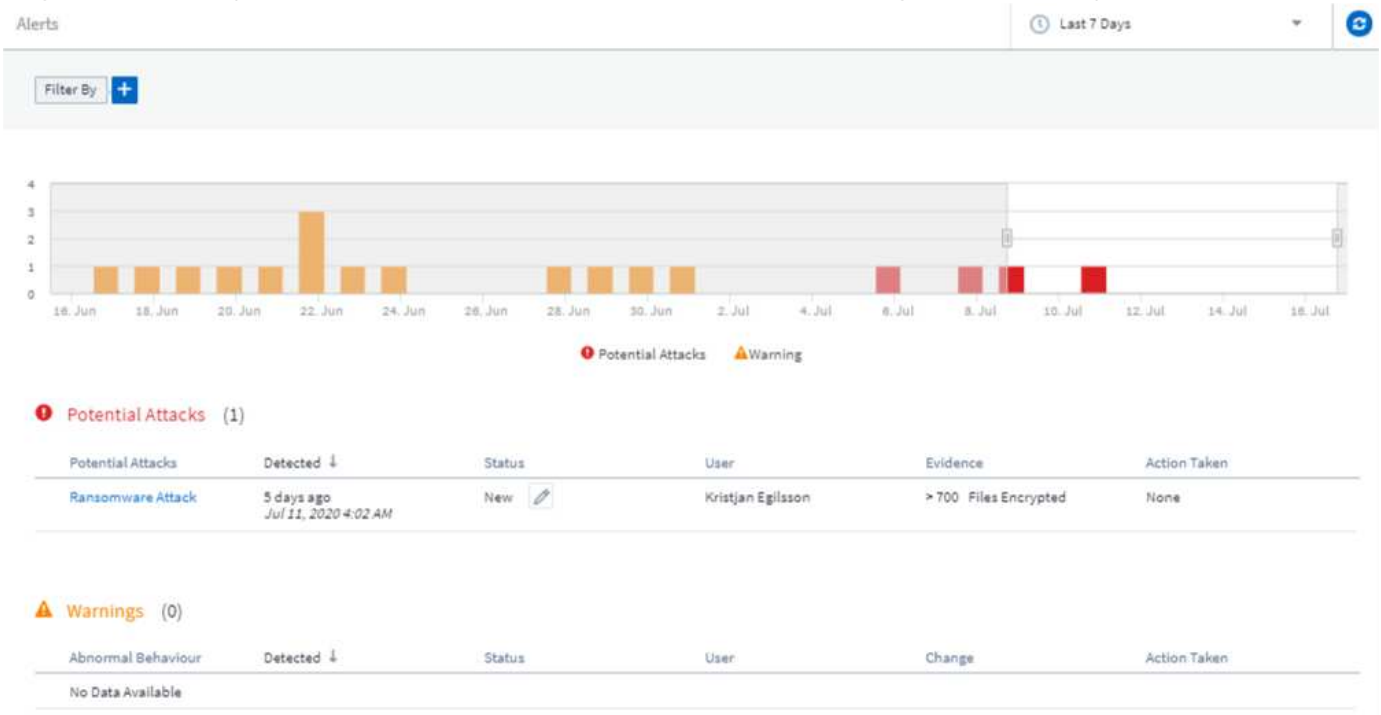
Seção Resultados do Ataque:

- Contagens de volumes e arquivos afetados
- Um resumo anexo da detecção
- Um gráfico mostrando a atividade do arquivo durante o ataque

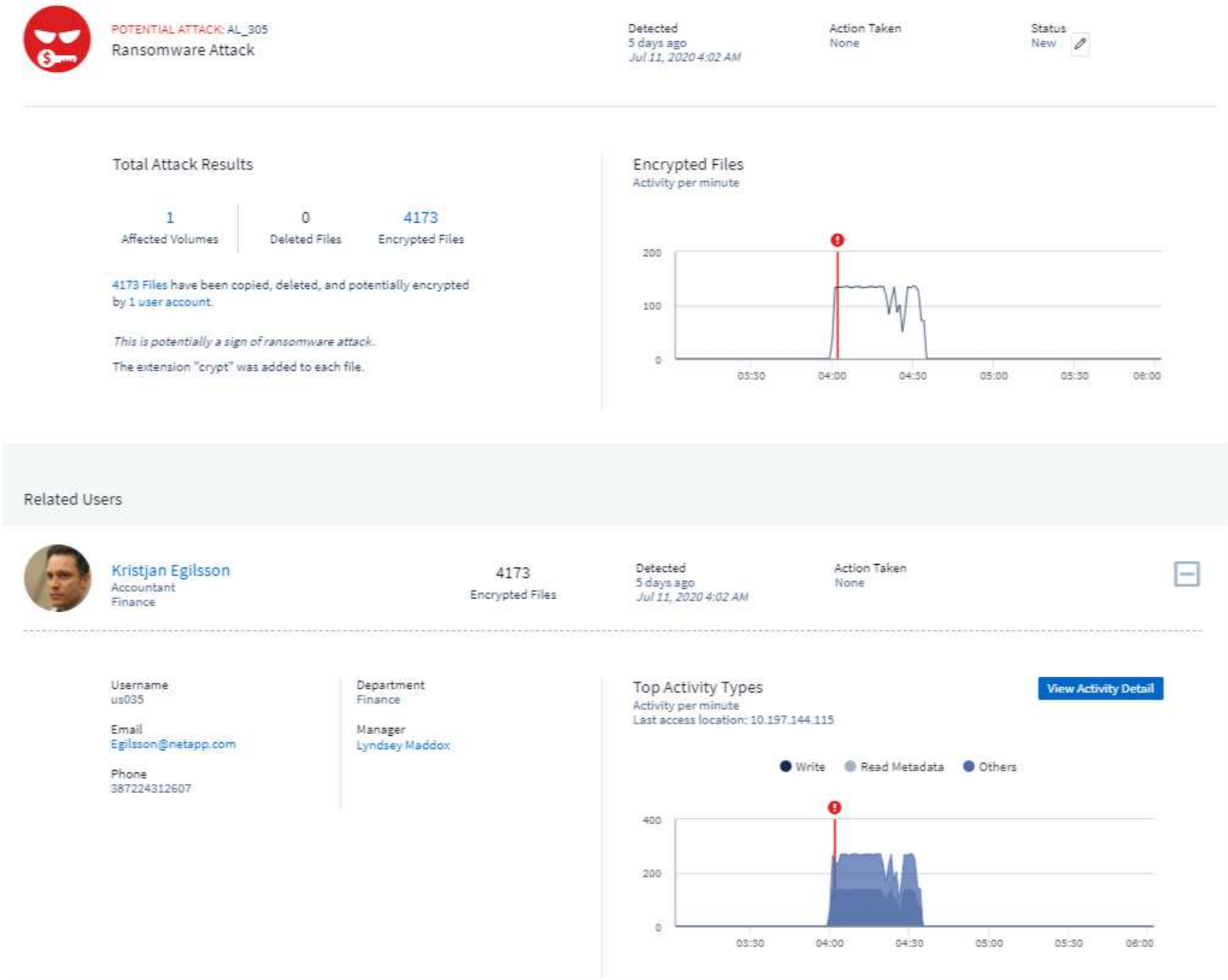
Seção Usuários relacionados:

Esta seção mostra detalhes sobre o usuário envolvido no possível ataque, incluindo um gráfico de atividade principal do usuário.

Página de alertas (este exemplo mostra um possível ataque de adulteração de arquivos):



Página de detalhes (este exemplo mostra um possível ataque de adulteração de arquivos):

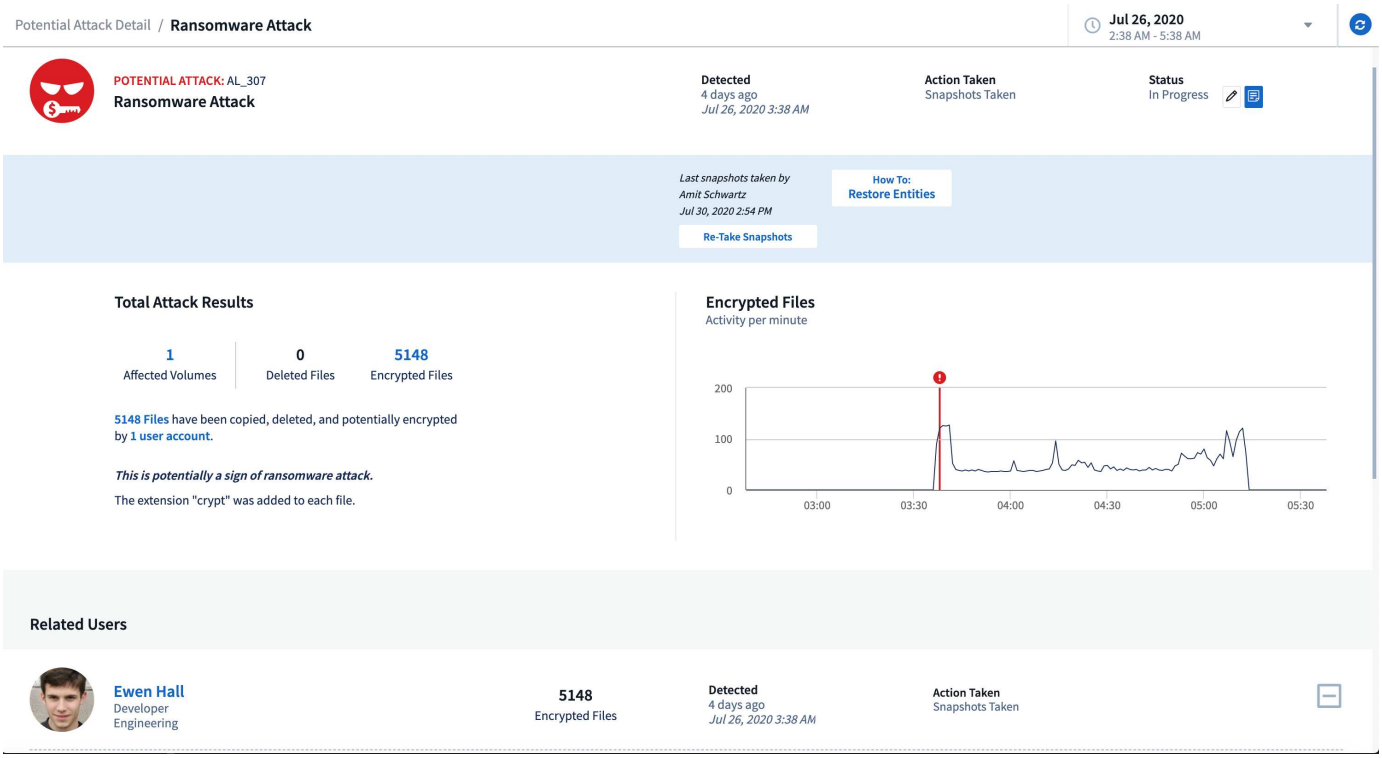


Ação *Tirar um instantâneo*

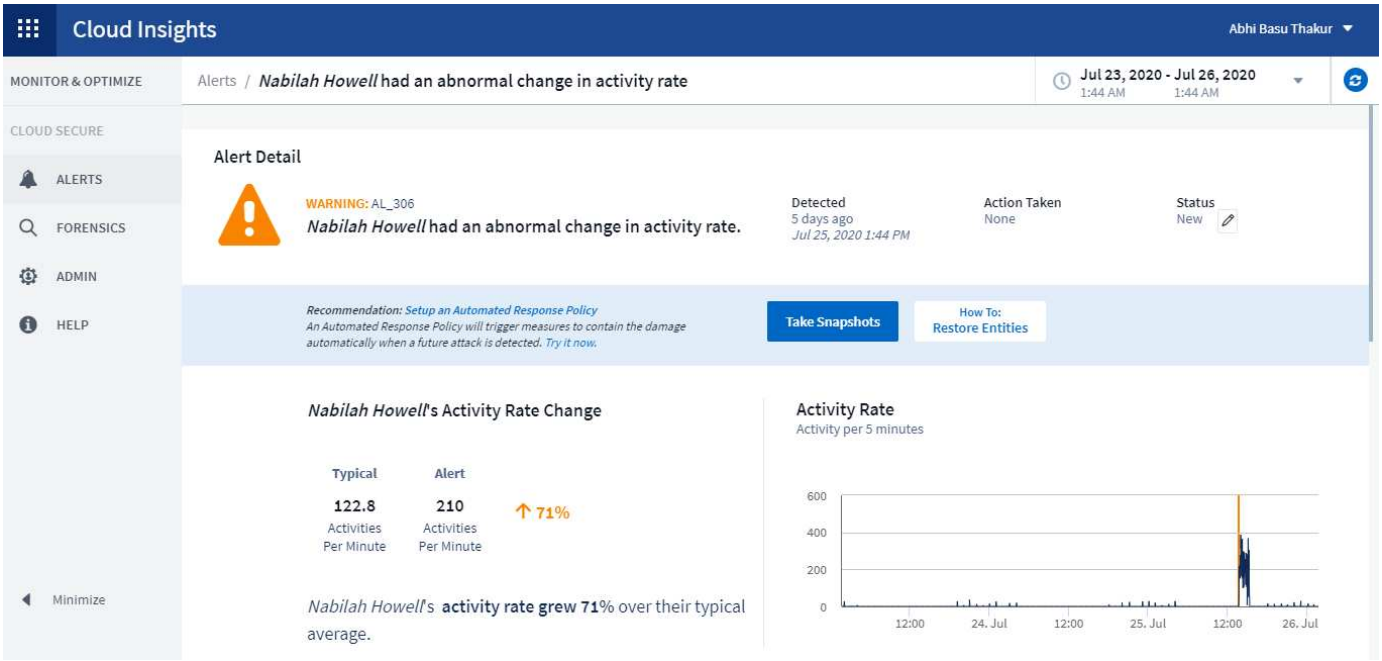
O Workload Security protege seus dados tirando um instantâneo automaticamente quando uma atividade maliciosa é detectada, garantindo que seus dados sejam armazenados em backup com segurança.

Você pode definir "políticas de resposta automatizadas" que tiram uma captura de tela quando um ataque de adulteração de arquivos ou outra atividade anormal do usuário é detectada. Você também pode tirar uma captura de tela manualmente a partir da página de alertas.

Snapshot automático
tirado:



Instantâneo manual:



Notificações de alerta

Notificações por e-mail de alertas são enviadas para uma lista de destinatários de alertas para cada ação no alerta. Para configurar destinatários de alertas, clique em **Admin > Notificações** e insira um endereço de e-mail para cada destinatário.

Política de retenção

Alertas e avisos são mantidos por 13 meses. Alertas e avisos com mais de 13 meses serão excluídos. Se o

ambiente de segurança de carga de trabalho for excluído, todos os dados associados ao ambiente também serão excluídos.

Solução de problemas

Problema:	Experimente isto:
Há uma situação em que o ONTAP tira instantâneos a cada hora por dia. Os snapshots do Workload Security (WS) afetarão isso? O snapshot do WS substituirá o snapshot por hora? O snapshot horário padrão será interrompido?	Os snapshots de segurança de carga de trabalho não afetarão os snapshots por hora. Os snapshots do WS não ocuparão o espaço de snapshots por hora e isso deve continuar como antes. O instantâneo horário padrão não será interrompido.
O que acontecerá se a contagem máxima de snapshots for atingida no ONTAP?	Se a contagem máxima de Snapshots for atingida, a captura de Snapshots subsequentes falhará e o Workload Security mostrará uma mensagem de erro informando que o Snapshot está cheio. O usuário precisa definir políticas de Snapshot para excluir os snapshots mais antigos, caso contrário, os snapshots não serão tirados. No ONTAP 9.3 e versões anteriores, um volume pode conter até 255 cópias de Snapshot. No ONTAP 9.4 e posteriores, um volume pode conter até 1023 cópias de Snapshot. Consulte a documentação do ONTAP para obter informações sobre"definindo política de exclusão de instantâneo" .
O Workload Security não consegue tirar instantâneos.	Certifique-se de que a função usada para criar snapshots tenha o direitos apropriados atribuídos. Certifique-se de que csrole foi criado com direitos de acesso adequados para tirar instantâneos: security login role create -vserver <vservername> -role csrole -cmddirname "volume snapshot" -access all
Os snapshots estão falhando para alertas mais antigos em SVMs que foram removidos do Workload Security e posteriormente adicionados novamente. Para novos alertas que ocorrem após o SVM ser adicionado novamente, são tirados instantâneos.	Este é um cenário raro. Caso isso aconteça, faça login no ONTAP e tire os instantâneos manualmente dos alertas mais antigos.
Na página *Detalhes do alerta*, a mensagem de erro “Última tentativa falhou” é vista abaixo do botão *Tirar instantâneo*. Passar o mouse sobre o erro exibe “O comando Invoke API expirou para o coletor de dados com id”.	Isso pode acontecer quando um coletor de dados é adicionado ao Workload Security por meio do IP de gerenciamento do SVM, se o LIF do SVM estiver no estado *desativado* no ONTAP. Habilite o LIF específico no ONTAP e acione *Obter Snapshot manualmente* no Workload Security. A ação Snapshot será então bem-sucedida.

Forense

Forense - Todas as atividades

A página Todas as atividades ajuda você a entender as ações executadas em entidades no ambiente de segurança de carga de trabalho.

Examinando todos os dados de atividade

Clique em **Forense > Forense de atividades** e clique na aba **Todas as atividades** para acessar a página Todas as atividades. Esta página fornece uma visão geral das atividades do seu locatário, destacando as seguintes informações:

- Um gráfico mostrando o *Histórico de atividades* (com base no intervalo de tempo global selecionado)

  Você pode ampliar o gráfico arrastando um retângulo no gráfico. A página inteira será carregada para exibir o intervalo de tempo ampliado. Quando ampliado, um botão é exibido permitindo que o usuário diminua o zoom.

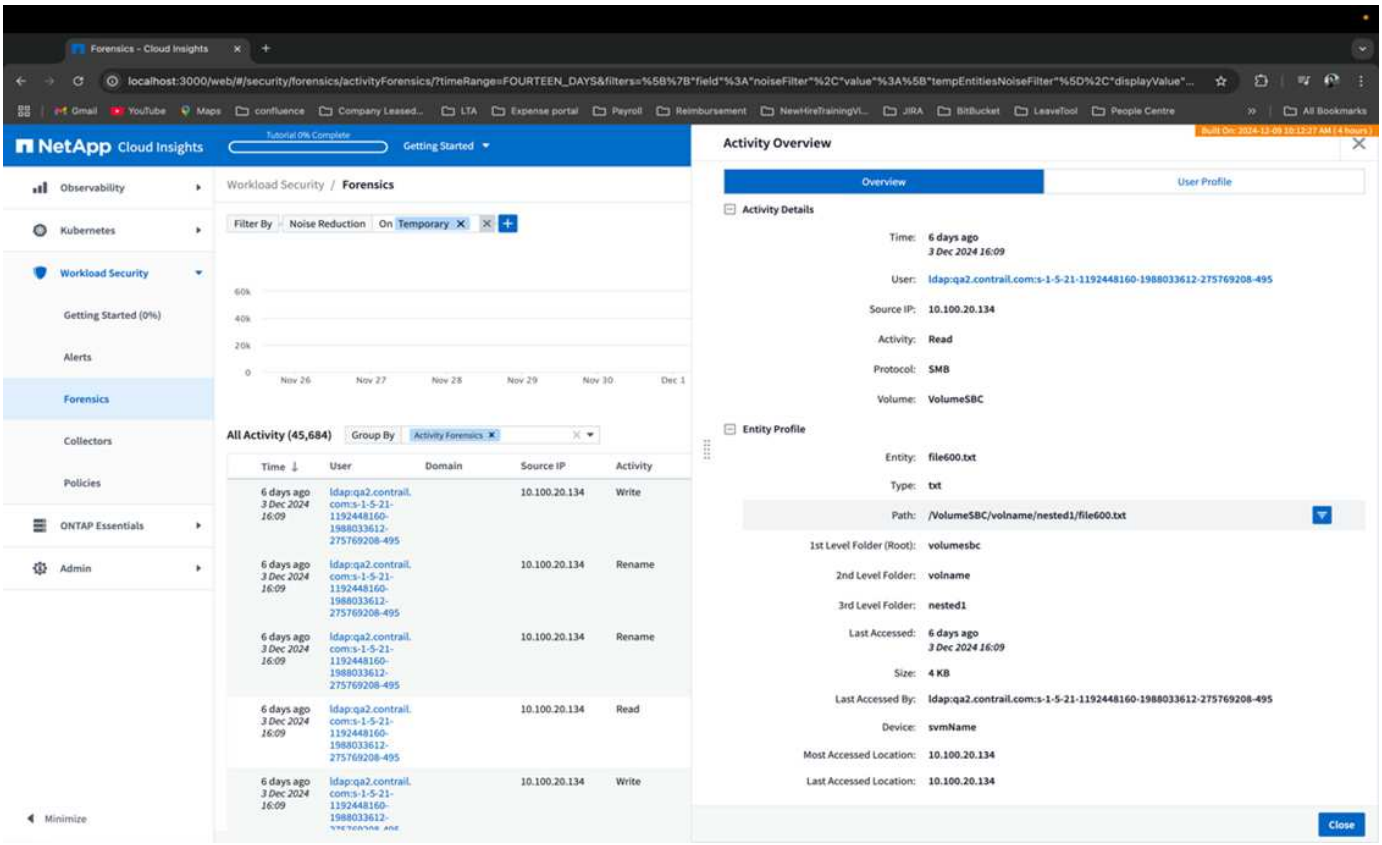
- Uma lista de dados de *Todas as atividades*.
- Um grupo suspenso fornecerá a opção de agrupar a atividade por usuários, pastas, tipo de entidade, etc.
- Um botão de caminho comum estará disponível acima da tabela. Ao clicar nele, podemos obter um painel deslizante com detalhes do caminho da entidade.

A tabela **Todas as atividades** mostra as seguintes informações. Observe que nem todas essas colunas são exibidas por padrão. Você pode selecionar colunas a serem exibidas clicando no ícone de "engrenagem".

- O **horário** em que uma entidade foi acessada, incluindo o ano, mês, dia e hora do último acesso.
- O **usuário** que acessou a entidade com um link para o"Informações do usuário" como um painel deslizante.
- A **atividade** realizada pelo usuário. Os tipos suportados são:
  - **Alterar propriedade do grupo** - A propriedade do grupo do arquivo ou pasta foi alterada. Para mais detalhes sobre a propriedade do grupo, consulte"este link."
  - **Alterar proprietário** - A propriedade do arquivo ou pasta é alterada para outro usuário.
  - **Alterar permissão** - A permissão do arquivo ou pasta é alterada.
  - **Criar** - Cria arquivo ou pasta.
  - **Excluir** - Excluir arquivo ou pasta. Se uma pasta for excluída, eventos *delete* serão obtidos para todos os arquivos nessa pasta e subpastas.
  - **Ler** - O arquivo foi lido.
  - **Ler metadados** - Somente ao habilitar a opção de monitoramento de pastas. Será gerado ao abrir uma pasta no Windows ou executar "ls" dentro de uma pasta no Linux.
  - **Renomear** - Renomear arquivo ou pasta.
  - **Gravar** - Os dados são gravados em um arquivo.
  - **Gravar metadados** - Os metadados do arquivo são gravados, por exemplo, a permissão é alterada.
  - **Outras alterações** - Qualquer outro evento que não esteja descrito acima. Todos os eventos não mapeados são mapeados para o tipo de atividade "Outra alteração". Aplicável a arquivos e pastas.

- O **Caminho** é o caminho da *entidade*. Este deve ser o caminho exato da entidade (por exemplo, "*/home/userX/nested1/nested2/abc.txt*") OU parte do diretório do caminho para pesquisa recursiva (por exemplo, "*/home/userX/nested1/nested2/*"). OBSERVAÇÃO: padrões de caminho regex (por exemplo, *nested*) NÃO são permitidos aqui. Como alternativa, filtros individuais de nível de pasta de caminho, conforme mencionado abaixo, também podem ser especificados para filtragem de caminho.
- A **Pasta de 1º Nível (Raiz)** é o diretório raiz do caminho da entidade em letras minúsculas.
- A **Pasta de 2º Nível** é o diretório de segundo nível do caminho da entidade em letras minúsculas.
- A **Pasta de 3º Nível** é o diretório de terceiro nível do caminho da entidade em letras minúsculas.
- A **Pasta de 4º Nível** é o diretório de quarto nível do caminho da entidade em letras minúsculas.
- O **Tipo de Entidade**, incluindo a extensão da entidade (ou seja, arquivo) (.doc, .docx, .tmp, etc.).
- O **Dispositivo** onde as entidades residem.
- O **Protocolo** usado para buscar eventos.
- O **Caminho original** usado para eventos de renomeação quando o arquivo original foi renomeado. Esta coluna não é visível na tabela por padrão. Use o seletor de colunas para adicionar esta coluna à tabela.
- O **Volume** onde as entidades residem. Esta coluna não é visível na tabela por padrão. Use o seletor de colunas para adicionar esta coluna à tabela.
- O **Nome da Entidade** é o último componente do caminho da entidade; Para o Tipo de Entidade como arquivo, é o nome do arquivo.

Selecionar uma linha da tabela abre um painel deslizante com o perfil do usuário em uma guia e a visão geral da atividade e da entidade em outra guia.



O método padrão *Agrupar por* é *Forense de atividades*. Se você selecionar um método *Agrupar por* diferente — por exemplo, Tipo de Entidade — a tabela de entidades *Agrupar por* será exibida. Se nenhuma seleção for

feita, *Agrupar por* **todos** será exibido.

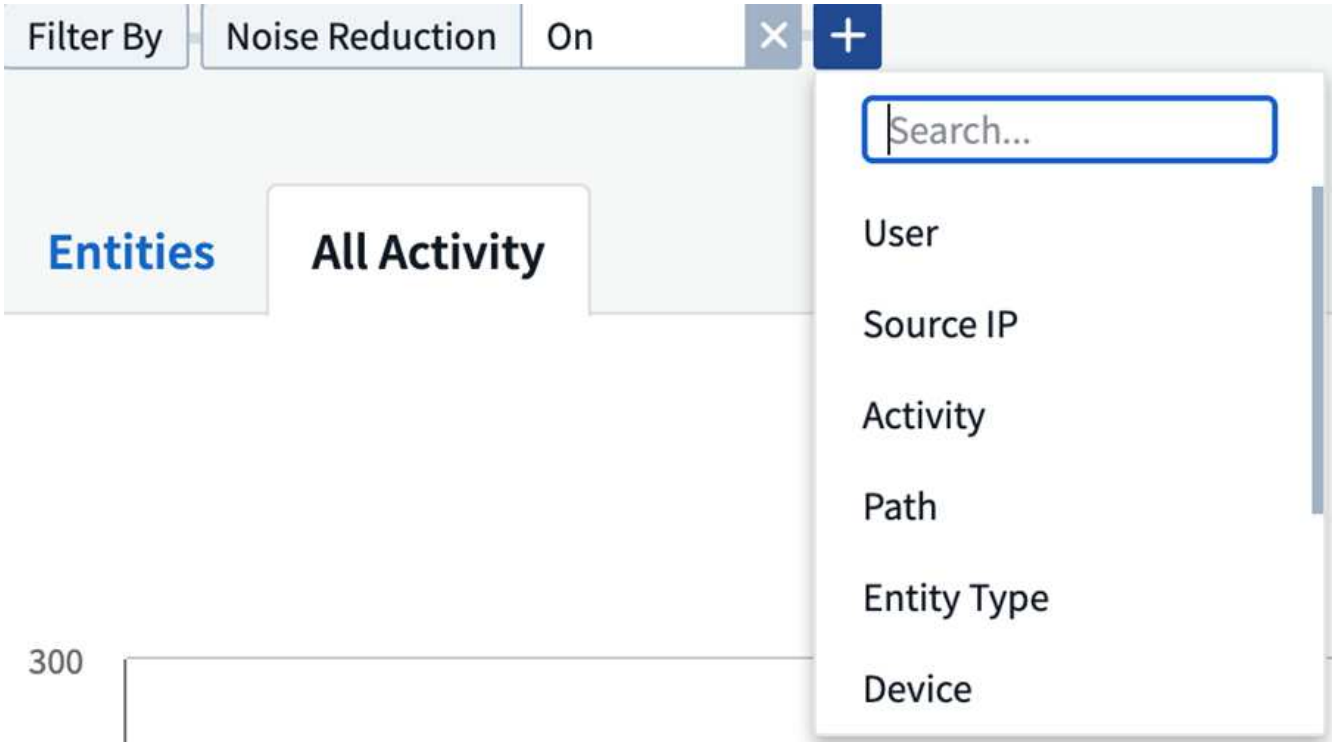
- A contagem de atividades é exibida como um hiperlink; selecionar isso adicionará o agrupamento selecionado como um filtro. A tabela de atividades será atualizada com base nesse filtro.
- Observe que se você alterar o filtro, alterar o intervalo de tempo ou atualizar a tela, não poderá retornar aos resultados filtrados sem definir o filtro novamente.
- Observe que quando o Nome da Entidade for selecionado como filtro, o menu suspenso Agrupar por será desabilitado. Além disso, quando o usuário já estiver na tela Agrupar por, o Nome da Entidade como filtro será desabilitado.

Filtrando dados do histórico de atividades forenses

Há dois métodos que você pode usar para filtrar dados.

- O filtro pode ser adicionado a partir do painel deslizante. O valor é adicionado aos filtros apropriados na lista superior *Filtrar por*.
- Filtre os dados digitando no campo *Filtrar por*:

  Selecione o filtro apropriado no widget superior 'Filtrar por' clicando no botão **[+]**:



  Digite o texto de pesquisa

  Pressione Enter ou clique fora da caixa de filtro para aplicá-lo.

Você pode filtrar dados de atividade forense pelos seguintes campos:

- O tipo **Atividade**.
- **Protocolo** para buscar atividades específicas do protocolo.
- **Nome de usuário** do usuário que está realizando a atividade. Você precisa fornecer o nome de usuário exato para filtrar. Pesquisar com nome de usuário parcial ou nome de usuário parcial prefixado ou

sufixado com '*' não funcionará.

- **Redução de ruído** para filtrar arquivos criados nas últimas 2 horas pelo usuário. Ele também é usado para filtrar arquivos temporários (por exemplo, arquivos .tmp) acessados pelo usuário.
- **Domínio** do usuário que executa a atividade. Você precisa fornecer o **domínio exato** para filtrar. A busca por domínio parcial ou domínio parcial prefixado ou sufixado com curinga ('*') não funcionará. *Nenhum* pode ser especificado para pesquisar domínios ausentes.

Os seguintes campos estão sujeitos a regras especiais de filtragem:

- **Tipo de entidade**, usando extensão de entidade (arquivo) - é preferível especificar o tipo exato de entidade entre aspas. Por exemplo *"txt"*.
- **Caminho** da entidade - Deve ser o caminho exato da entidade (por exemplo, "*/home/userX/nested1/nested2/abc.txt*") OU parte do diretório do caminho para pesquisa recursiva (por exemplo, "*/home/userX/nested1/nested2/*"). OBSERVAÇÃO: padrões de caminho regex (por exemplo, *nested*) NÃO são permitidos aqui. Filtros de caminho de diretório (string de caminho terminando com /) com até 4 diretórios de profundidade são recomendados para resultados mais rápidos. Por exemplo, "*/home/userX/nested1/nested2/*". Veja a tabela abaixo para mais detalhes.
- Pasta de 1º nível (raiz) - diretório raiz do caminho da entidade como filtros. Por exemplo, se o caminho da entidade for /home/userX/nested1/nested2/, então home OU "home" podem ser usados.
- Pasta de 2º nível - diretório de 2º nível de filtros de caminho de entidade. Por exemplo, se o caminho da entidade for /home/userX/nested1/nested2/, então userX OU "userX" podem ser usados.
- Pasta de 3º nível – diretório de 3º nível de filtros de caminho de entidade.
- Por exemplo, se o caminho da entidade for /home/userX/nested1/nested2/, então nested1 OU "nested1" podem ser usados.
- Pasta de 4º nível - Diretório Diretório de 4º nível de filtros de caminho de entidade. Por exemplo, se o caminho da entidade for /home/userX/nested1/nested2/, então nested2 OU "nested2" podem ser usados.
- **Usuário** executando a atividade - é preferível especificar o usuário exato entre aspas. Por exemplo, *"Administrador"*.
- **Dispositivo** (SVM) onde as entidades residem
- **Volume** onde as entidades residem
- O **Caminho original** usado para eventos de renomeação quando o arquivo original foi renomeado.
- **IP de origem** de onde a entidade foi acessada.
  - Você pode usar curingas * e ?. Por exemplo: 10.0.0.**, 10.0?.0.10, 10.10**
  - Se for necessária uma correspondência exata, você deverá fornecer um endereço IP de origem válido entre aspas duplas, por exemplo, "10.1.1.1.". IPs incompletos com aspas duplas, como "10.1.1.", "10.1..*", etc., não funcionarão.
- **Nome da Entidade** - o nome do arquivo do Caminho da Entidade como filtros. Por exemplo, se o caminho da entidade for /home/userX/nested1/testfile.txt, o nome da entidade será testfile.txt. Observe que é recomendável especificar o nome exato do arquivo entre aspas; tente evitar pesquisas com curingas. Por exemplo, "testfile.txt". Observe também que esse filtro de nome de entidade é recomendado para intervalos de tempo mais curtos (até 3 dias).

Os campos anteriores estão sujeitos ao seguinte ao filtrar:

- O valor exato deve estar entre aspas: Exemplo: "searchtext"
- As strings curinga não devem conter aspas: Exemplo: searchtext, *searchtext*, filtrará qualquer string que contenha 'searchtext'.

- String com um prefixo, Exemplo: searchtext* , pesquisará qualquer string que comece com 'searchtext'.

Observe que todos os campos de filtro diferenciam maiúsculas de minúsculas. Por exemplo: se o filtro aplicado for Tipo de Entidade com valor como 'searchtext', ele retornará resultados com Tipo de Entidade como 'searchtext', 'SearchText', 'SEARCHTEXT'

Exemplos de filtros de atividade forense:

Expressão de filtro aplicada pelo usuário	Resultado esperado	Avaliação de desempenho	Comentário
Caminho = "/home/usuárioX/aninhado1/aninhado2/"	Pesquisa recursiva de todos os arquivos e pastas no diretório fornecido	Rápido	Pesquisas em diretórios de até 4 diretórios serão rápidas.
Caminho = "/home/userX/nested1/"	Pesquisa recursiva de todos os arquivos e pastas no diretório fornecido	Rápido	Pesquisas em diretórios de até 4 diretórios serão rápidas.
Caminho = "/home/userX/nested1/test"	Correspondência exata onde o valor do caminho corresponde a /home/userX/nested1/test	Mais devagar	A pesquisa exata será mais lenta em comparação às pesquisas de diretório.
Caminho = "/home/usuárioX/aninhado1/aninhado2/aninhado3/"	Pesquisa recursiva de todos os arquivos e pastas no diretório fornecido	Mais devagar	Pesquisas em mais de 4 diretórios são mais lentas.
Quaisquer outros filtros não baseados em caminho. Recomenda-se que os filtros de usuário e tipo de entidade estejam entre aspas, por exemplo, Usuário="Administrador" Tipo de entidade="txt"		Rápido	
Nome da entidade = "test.log"	Correspondência exata onde o nome do arquivo é test.log	Rápido	Como é uma correspondência exata
Nome da entidade = *test.log	Nomes de arquivos terminados em test.log	Lento	Devido ao curinga, pode ser lento.
Nome da entidade = test*.log	Nomes de arquivos que começam com test e terminam com .log	Lento	Devido ao curinga, pode ser lento.
Nome da entidade = test.lo	Nomes de arquivos começando com test.lo Por exemplo: corresponderá a test.log, test.log.1, test.log1	Mais devagar	Devido ao curinga no final, pode ser lento.

Expressão de filtro aplicada pelo usuário	Resultado esperado	Avaliação de desempenho	Comentário
Nome da Entidade = teste	Nomes de arquivos começando com teste	Mais lento	Devido ao curinga no final e ao valor mais genérico usado, ele pode ser mais lento.

OBSERVAÇÃO:

1. A contagem de atividades exibida ao lado do ícone Todas as atividades é arredondada para 30 minutos quando o intervalo de tempo selecionado abrange mais de 3 dias. Por exemplo, um intervalo de tempo de *1º de setembro, 10h15 a 7 de setembro, 10h15* mostrará contagens de atividades de 1º de setembro, 10h00 a 7 de setembro, 10h30.
2. Da mesma forma, as métricas de contagem mostradas no gráfico Histórico de atividades são arredondadas para 30 minutos quando o intervalo de tempo selecionado abrange mais de 3 dias.

Classificando dados do histórico de atividades forenses

Você pode classificar os dados do histórico de atividades por *Hora, Usuário, IP de origem, Atividade,*, *Tipo de entidade*, Pasta de 1º nível (raiz), Pasta de 2º nível, Pasta de 3º nível e Pasta de 4º nível. Por padrão, a tabela é classificada em ordem decrescente de *Tempo*, o que significa que os dados mais recentes serão exibidos primeiro. A classificação está desabilitada para os campos *Dispositivo* e *Protocolo*.

Guia do usuário para exportações assíncronas

Visão geral

O recurso Exportações Assíncronas no Storage Workload Security foi projetado para lidar com grandes exportações de dados.

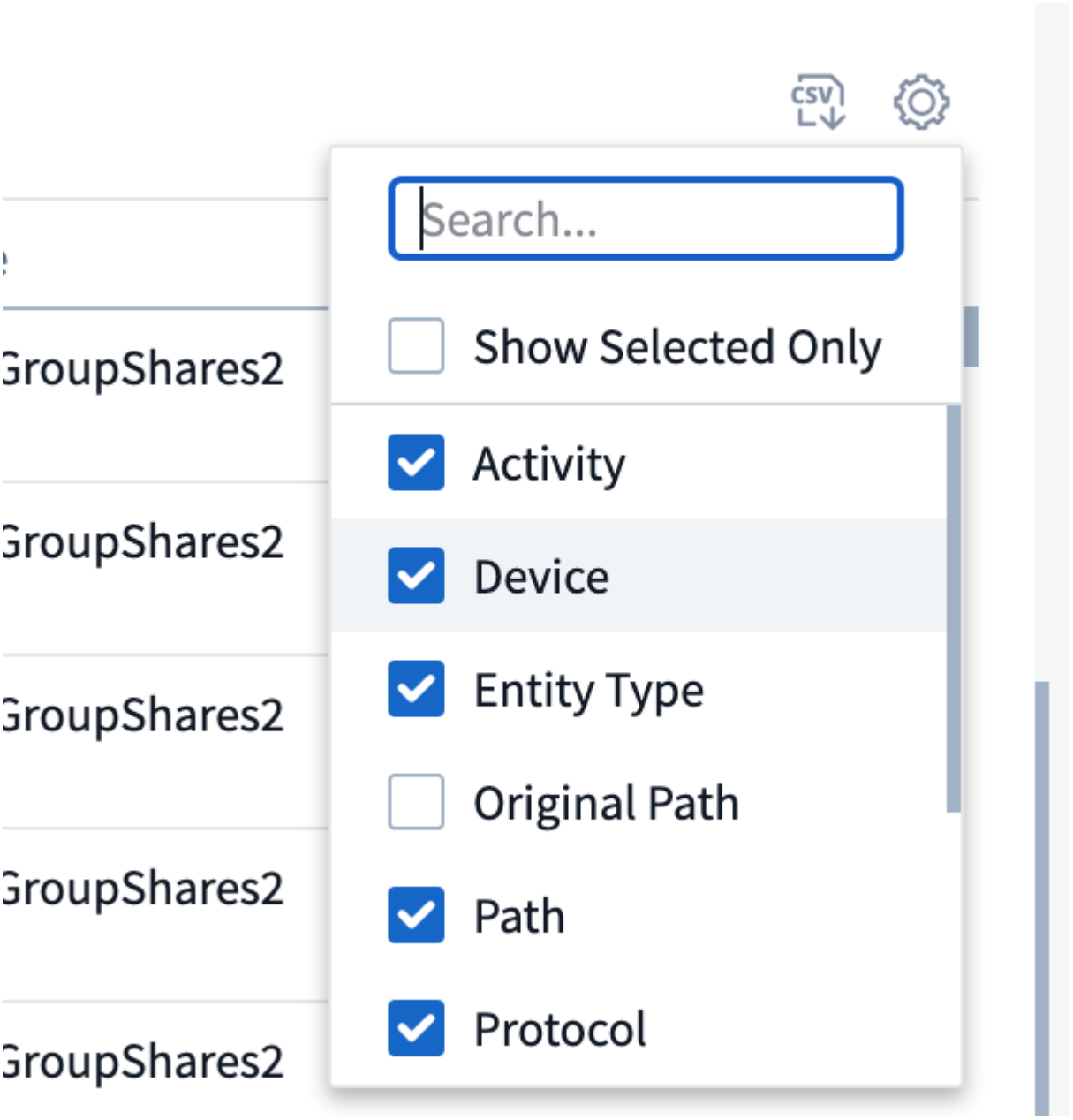
Guia passo a passo: Exportando dados com exportações assíncronas

1. **Iniciar exportação**: Selecione a duração e os filtros desejados para a exportação e clique no botão exportar.
2. **Aguarde a conclusão da exportação**: O tempo de processamento pode variar de alguns minutos a algumas horas. Pode ser necessário atualizar a página forense algumas vezes. Quando o trabalho de exportação estiver concluído, o botão "Baixar último arquivo CSV de exportação" será habilitado.
3. **Download**: Clique no botão "Baixar último arquivo de exportação criado" para obter os dados exportados em formato .zip. Esses dados estarão disponíveis para download até que o usuário inicie outra Exportação Assíncrona ou até que 3 dias tenham decorrido, o que ocorrer primeiro. O botão permanecerá habilitado até que outra Exportação Assíncrona seja iniciada.
4. **Limitações**:
   - O número de downloads assíncronos está atualmente limitado a 1 por usuário para cada atividade e tabela de análise de atividades e 3 por locatário.
   - Os dados exportados são limitados a um máximo de 1 milhão de registros para a Tabela de Atividades; enquanto para Agrupar por, o limite é de meio milhão de registros.

Um script de exemplo para extrair dados forenses via API está presente em */opt/netapp/cloudsecure/agent/export-script/* no agente. Veja o arquivo leia-me neste local para mais detalhes sobre o script.

Seleção de colunas para todas as atividades

A tabela *Todas as atividades* mostra colunas selecionadas por padrão. Para adicionar, remover ou alterar as colunas, clique no ícone de engrenagem à direita da tabela e selecione na lista de colunas disponíveis.



Retenção do histórico de atividades

O histórico de atividades é mantido por 13 meses para ambientes ativos de segurança de carga de trabalho.

Aplicabilidade de Filtros em Perícia Forense

Filtro	O que ele faz	Exemplo	Aplicável para estes filtros	Não aplicável para esses filtros	Resultado
* (Asterisco)	permite que você pesquise tudo	Auto*03172022 Se o texto da pesquisa contiver hífen ou sublinhado, informe a expressão entre colchetes. Por exemplo, (svm*) para pesquisar svm-123	Usuário, Tipo de Entidade, Dispositivo, Volume, Caminho Original, Pasta de 1º Nível, Pasta de 2º Nível, Pasta de 3º Nível, Pasta de 4º Nível, Nome da Entidade, IP de Origem		Retorna todos os recursos que começam com "Auto" e terminam com "03172022"
? (ponto de interrogação)	permite que você pesquise um número específico de caracteres	UsuárioAutoSabotage1_03172022?	Usuário, Tipo de Entidade, Dispositivo, Volume, Pasta de 1º Nível, Pasta de 2º Nível, Pasta de 3º Nível, Pasta de 4º Nível, Nome da Entidade, IP de Origem		retorna AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022B, AutoSabotageUser1_031720225 e assim por diante
OU	permite que você especifique múltiplas entidades	AutoSabotageUser1_03172022 OU AutoRansomUser4_03162022	Usuário, Domínio, Tipo de Entidade, Caminho Original, Nome da Entidade, IP de Origem		retorna qualquer um dos AutoSabotageUser1_03172022 OU AutoRansomUser4_03162022
NÃO	permite que você exclua texto dos resultados da pesquisa	NOT AutoRansomUser4_03162022	Usuário, Domínio, Tipo de Entidade, Caminho Original, Pasta de 1º Nível, Pasta de 2º Nível, Pasta de 3º Nível, Pasta de 4º Nível, Nome da Entidade, IP de Origem	Dispositivo	retorna tudo que não começa com "AutoRansomUser4_03162022"

Filtro	O que ele faz	Exemplo	Aplicável para estes filtros	Não aplicável para esses filtros	Resultado
Nenhum	procura por valores NULL em todos os campos	Nenhum	Domínio		retorna resultados onde o campo de destino está vazio

Busca de Caminho

Os resultados da pesquisa com e sem / serão diferentes

"/AutoDir1/AutoFile03242022"	Somente a pesquisa exata funciona; retorna todas as atividades com caminho exato como /AutoDir1/AutoFile03242022 (sem distinção de maiúsculas e minúsculas)
"/AutoDir1/ "	Funciona; retorna todas as atividades com diretório de 1º nível correspondente a AutoDir1 (sem distinção de maiúsculas e minúsculas)
"/AutoDir1/AutoFile03242022/"	Funciona; retorna todas as atividades com diretório de 1º nível correspondente a AutoDir1 e diretório de 2º nível correspondente a AutoFile03242022 (sem distinção de maiúsculas e minúsculas)
/AutoDir1/AutoFile03242022 OU /AutoDir1/AutoFile03242022	Não funciona
NÃO /AutoDir1/AutoFile03242022	Não funciona
NÃO /AutoDir1	Não funciona
NÃO /AutoFile03242022	Não funciona
*	Não funciona

Alterações na atividade do usuário raiz SVM local

Se um usuário SVM raiz local estiver executando qualquer atividade, o IP do cliente no qual o compartilhamento NFS está montado agora será considerado no nome de usuário, que será mostrado como root@<endereço-ip-do-cliente> nas páginas de atividade forense e de atividade do usuário.

Por exemplo:

- Se o SVM-1 for monitorado pelo Workload Security e o usuário root desse SVM montar o compartilhamento em um cliente com endereço IP 10.197.12.40, o nome de usuário mostrado na página de atividade forense será *root@10.197.12.40*.
- Se o mesmo SVM-1 for montado em outro cliente com endereço IP 10.197.12.41, o nome de usuário mostrado na página de atividade forense será *root@10.197.12.41*.

*• Isso é feito para segregar a atividade do usuário root do NFS por endereço IP. Anteriormente, toda a atividade era considerada feita apenas pelo usuário *root*, sem distinção de IP.

Solução de problemas

Problema	Experimente isto
Na tabela "Todas as atividades", na coluna "Usuário", o nome do usuário é exibido como: "ldap:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817" ou "ldap:default:80038003"	Possíveis razões podem ser: 1. Nenhum coletor de diretório de usuário foi configurado ainda. Para adicionar um, vá para **Segurança de carga de trabalho > Coletores > Coletores de diretório de usuário** e clique em **+Coletor de diretório de usuário**. Escolha *Active Directory* ou *LDAP Directory Server*. 2. Um coletor de diretório de usuário foi configurado, mas ele parou ou está em estado de erro. Acesse **Coletores > Coletores do Diretório de Usuários** e verifique o status. Consulte o"Solução de problemas do coletor de diretório do usuário" seção da documentação para dicas de solução de problemas. Após a configuração correta, o nome será resolvido automaticamente em 24 horas. Se ainda assim não for resolvido, verifique se você adicionou o Coletor de Dados do Usuário correto. Certifique-se de que o usuário realmente faça parte do servidor de diretório Active Directory/LDAP adicionado.
Alguns eventos NFS não são vistos na interface do usuário.	Verifique o seguinte: 1. Um coletor de diretório de usuário para servidor AD com atributos POSIX definidos deve estar em execução com o atributo unixid habilitado na interface do usuário. 2. Qualquer usuário que fizer acesso NFS deverá ser visto quando pesquisado na página do usuário na UI 3. Eventos brutos (eventos para os quais o usuário ainda não foi descoberto) não são suportados pelo NFS 4. O acesso anônimo à exportação NFS não será monitorado. 5. Certifique-se de que a versão do NFS usada seja 4.1 ou inferior. (Observe que o NFS 4.1 é compatível com o ONTAP 9.15 ou posterior.)
Depois de digitar algumas letras contendo um caractere curinga como asterisco (*) nos filtros nas páginas Forensics *Todas as atividades* ou *Entidades*, as páginas carregam muito lentamente.	Um asterisco (*) na sequência de pesquisa pesquisa tudo. Entretanto, strings curinga iniciais como *<searchTerm> ou *<searchTerm>* resultarão em uma consulta lenta. Para obter melhor desempenho, use strings de prefixo, no formato <searchTerm>* (em outras palavras, acrescente o asterisco (*) *após* um termo de pesquisa). Exemplo: use a string *testvolume**, em vez de *testvolume ou *test*volume*. Use uma pesquisa de diretório para ver todas as atividades em uma determinada pasta recursivamente (pesquisa hierárquica). Por exemplo, "/path1/path2/path3/" listará todas as atividades recursivamente em /path1/path2/path3. Como alternativa, use a opção "Adicionar ao filtro" na aba Todas as atividades.
Estou encontrando um erro "Falha na solicitação com código de status 500/503" ao usar um filtro de caminho.	Tente usar um intervalo de datas menor para filtrar registros.

A interface do usuário forense está carregando dados lentamente ao usar o filtro *path*.	Filtros de caminho de diretório (string de caminho terminando com /) com até 4 diretórios de profundidade são recomendados para resultados mais rápidos. Por exemplo, se o caminho do diretório for /Aaa/Bbb/Ccc/Ddd, tente pesquisar por "/Aaa/Bbb/Ccc/Ddd/" para carregar os dados mais rapidamente.
A interface do usuário forense está carregando dados lentamente e enfrentando falhas ao usar o filtro de nome da entidade.	Tente com intervalos de tempo menores e com pesquisa de valor exato com aspas duplas. Por exemplo, se entityPath for "/home/userX/nested1/nested2/nested3/testfile.txt", tente com "testfile.txt" como filtro de nome de entidade.

Visão geral do usuário forense

Informações para cada usuário são fornecidas na Visão Geral do Usuário. Use essas visualizações para entender as características do usuário, entidades associadas e atividades recentes.

Perfil do usuário

As informações do perfil do usuário incluem informações de contato e localização do usuário. O perfil fornece as seguintes informações:

- Nome do usuário
- Endereço de e-mail do usuário
- Gerenciador de usuários
- Contato telefônico do usuário
- Localização do usuário

Comportamento do usuário

As informações de comportamento do usuário identificam atividades e operações recentes realizadas pelo usuário. Essas informações incluem:

- Atividade recente
  - Último local de acesso
  - Gráfico de atividade
  - Alertas
- Operações dos últimos sete dias
  - Número de operações

Intervalo de atualização

A lista de usuários é atualizada a cada 12 horas.

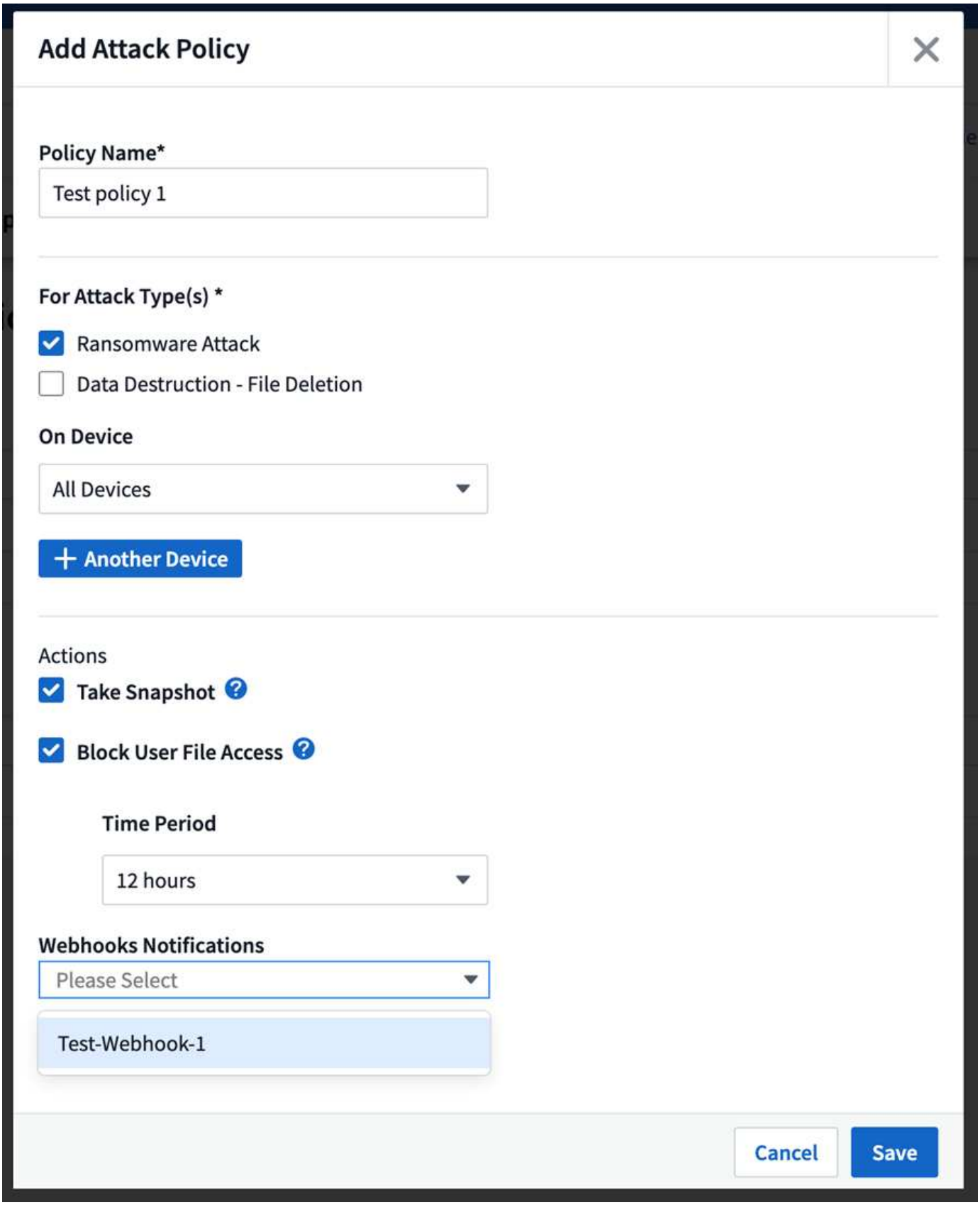
Política de retenção

Se não for atualizada novamente, a lista de usuários será mantida por 13 meses. Após 13 meses, os dados serão excluídos. Se o seu ambiente de segurança de carga de trabalho for excluído, todos os dados associados ao ambiente serão excluídos.

Políticas de Resposta Automatizada

As Políticas de Resposta acionam ações como tirar um instantâneo ou restringir o acesso do usuário em caso de ataque ou comportamento anormal do usuário.

Você pode definir políticas em dispositivos específicos ou em todos os dispositivos. Para definir uma política de resposta, selecione **Admin > Políticas de resposta automatizadas** e clique no botão **+Política** apropriado. Você pode criar políticas para Ataques ou para Avisos.



Você deve salvar a política com um nome exclusivo.

Para desabilitar uma ação de resposta automatizada (por exemplo, Tirar instantâneo), basta desmarcar a ação e salvar a política.

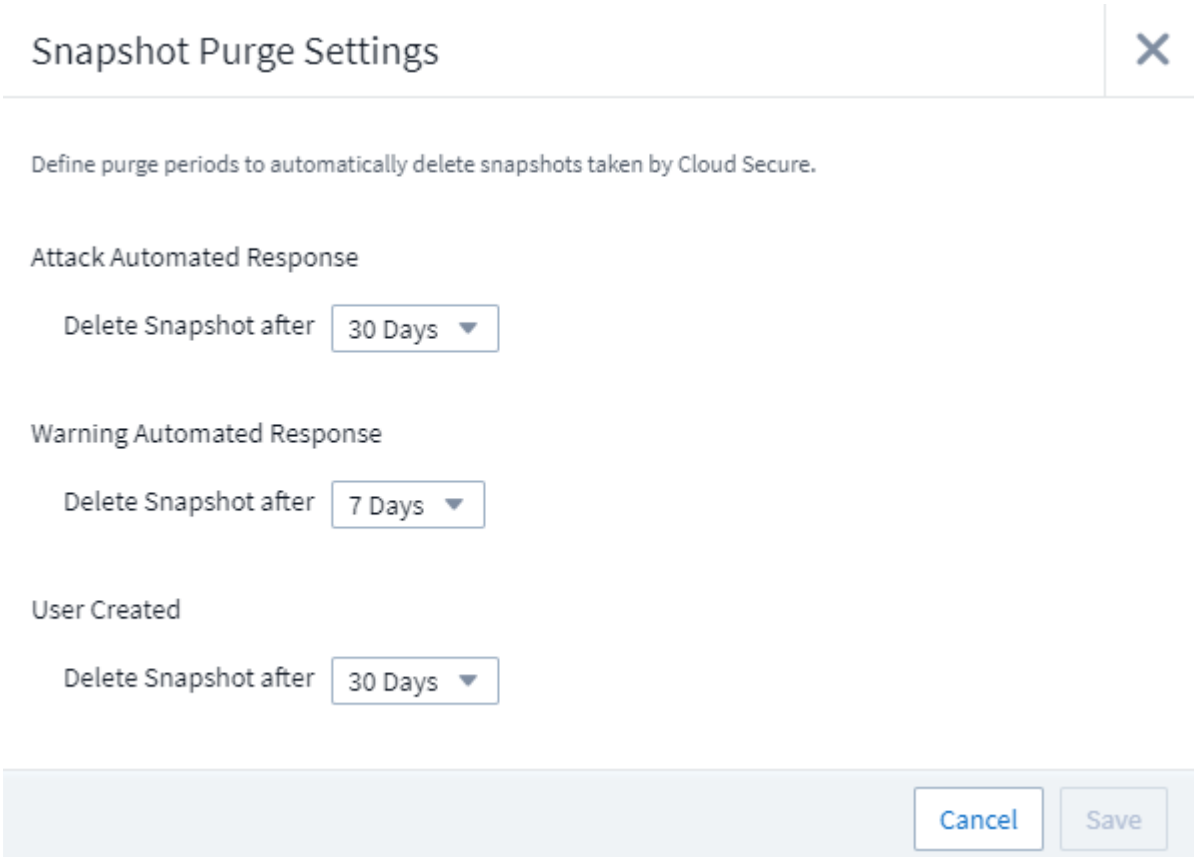
Quando um alerta é disparado para os dispositivos especificados (ou todos os dispositivos, se selecionados), a política de resposta automatizada tira um instantâneo dos seus dados. Você pode ver o status do instantâneo no"Página de detalhes do alerta" .

Veja o"Restringir acesso do usuário" página para mais detalhes sobre como restringir o acesso do usuário por IP.

Você pode anexar um ou mais webhooks a uma política para ser notificado quando um alerta for criado e uma ação for tomada. É recomendável adicionar no máximo 10 webhooks a uma política. Lembre-se de que, se uma política for pausada, as notificações de webhooks não serão acionadas.

Você pode modificar ou pausar uma Política de Resposta Automatizada escolhendo a opção no menu suspenso da política.

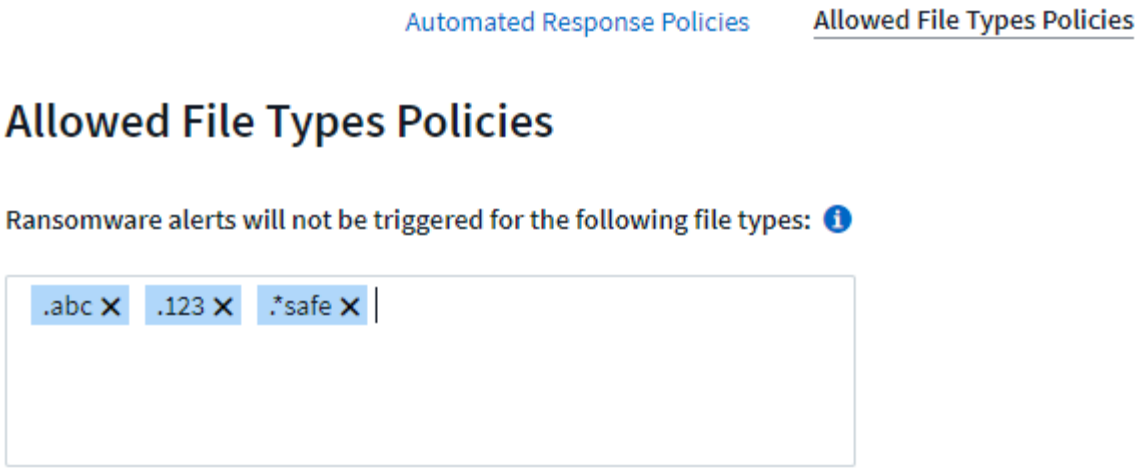
O Workload Security excluirá automaticamente os snapshots uma vez por dia com base nas configurações de limpeza de snapshots.



Políticas de tipos de arquivo permitidos

Se for detectado um ataque de adulteração de arquivos para uma extensão de arquivo conhecida e alertas estiverem sendo gerados na tela de Alertas, essa extensão de arquivo poderá ser adicionada a uma lista de *tipos de arquivo permitidos* para evitar alertas desnecessários.

Navegue até **Segurança de carga de trabalho > Políticas** e vá para a guia *Políticas de tipo de arquivo permitidas*.



Uma vez adicionado à lista de *tipos de arquivo permitidos*, nenhum alerta de ataque de adulteração de arquivo será gerado para esse tipo de arquivo permitido. Note que a política de *Tipos de Arquivo Permitidos* só se aplica à detecção de adulteração de arquivos.

Por exemplo, se um arquivo chamado *test.txt* for renomeado para *test.txt.abc* e o Workload Security detectar um ataque de adulteração de arquivo devido à extensão *.abc*, a extensão *.abc* poderá ser adicionada à lista de *tipos de arquivo permitidos*. Após serem adicionados à lista, os ataques de adulteração de arquivos não serão mais gerados contra arquivos com a extensão *.abc*.

Os tipos de arquivo permitidos podem ser correspondências exatas (por exemplo, ".abc") ou expressões (por exemplo, ".**type", ".type**" ou "**type**"). Expressões dos tipos “.a*c”, “.p*f” não são suportadas.

Integração com a Proteção Autônoma contra Ransomware ONTAP

O recurso de Proteção Autônoma do ONTAP utiliza a análise de carga de trabalho em ambientes NAS (NFS e SMB) para detectar proativamente e alertar sobre atividades anormais em arquivos que possam indicar ataques maliciosos ou modificações de dados não autorizadas.

Detalhes adicionais e requisitos de licença sobre ARP podem ser encontrados"aqui" .

O Workload Security integra-se ao ONTAP para receber eventos ARP e fornecer uma camada adicional de análise e respostas automáticas.

O Workload Security recebe os eventos ARP do ONTAP e executa as seguintes ações:

1. Correlaciona eventos de criptografia de volume com a atividade do usuário para identificar quem está causando o dano.
2. Implementa políticas de resposta automática (se definidas)
3. Fornece recursos forenses:
    - Permitir que os clientes conduzam investigações de violação de dados.
    - Identifique quais arquivos foram afetados, ajudando a recuperar mais rapidamente e conduzir investigações de violação de dados.

Pré-requisitos

1. Versão mínima do ONTAP : 9.11.1
2. Volumes habilitados para ARP. Detalhes sobre como habilitar o ARP podem ser encontrados"aqui" . O ARP deve ser habilitado via OnCommand System Manager. O Workload Security não pode habilitar o ARP.
3. O coletor de segurança de carga de trabalho deve ser adicionado via IP do cluster.
4. Credenciais em nível de cluster são necessárias para que esse recurso funcione. Em outras palavras, as credenciais em nível de cluster devem ser usadas ao adicionar o SVM.

Permissões de usuário necessárias

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.

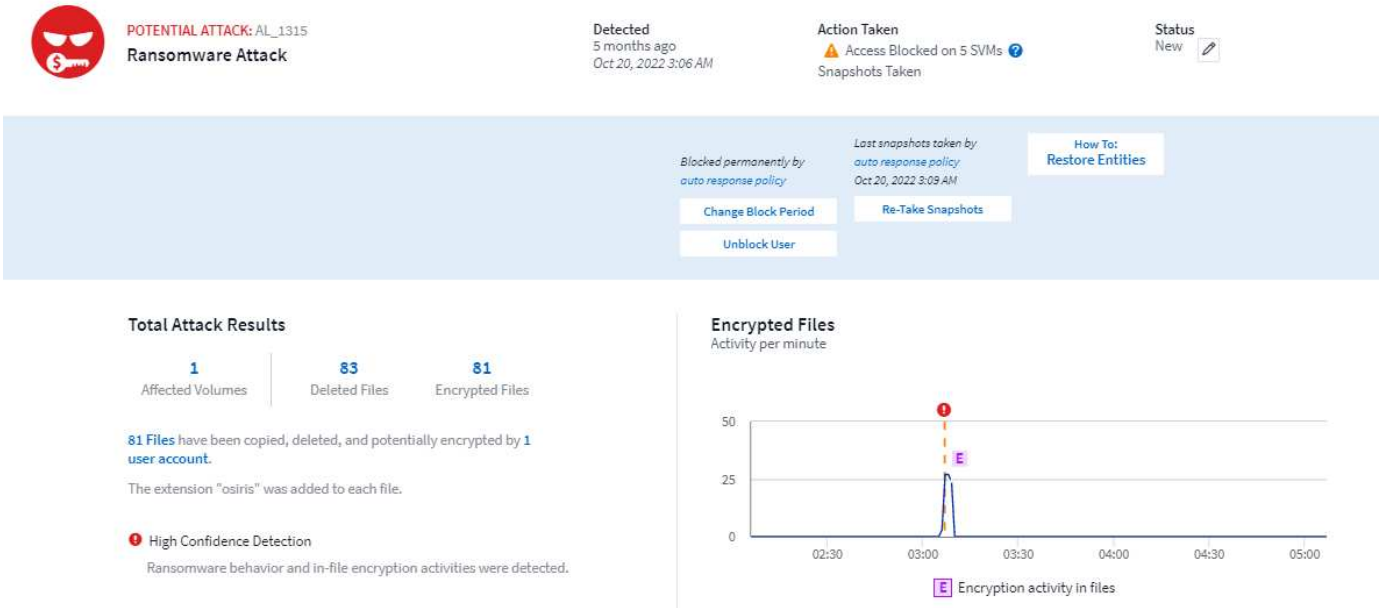
Para *csuser* com credenciais de cluster, faça o seguinte na linha de comando do ONTAP :

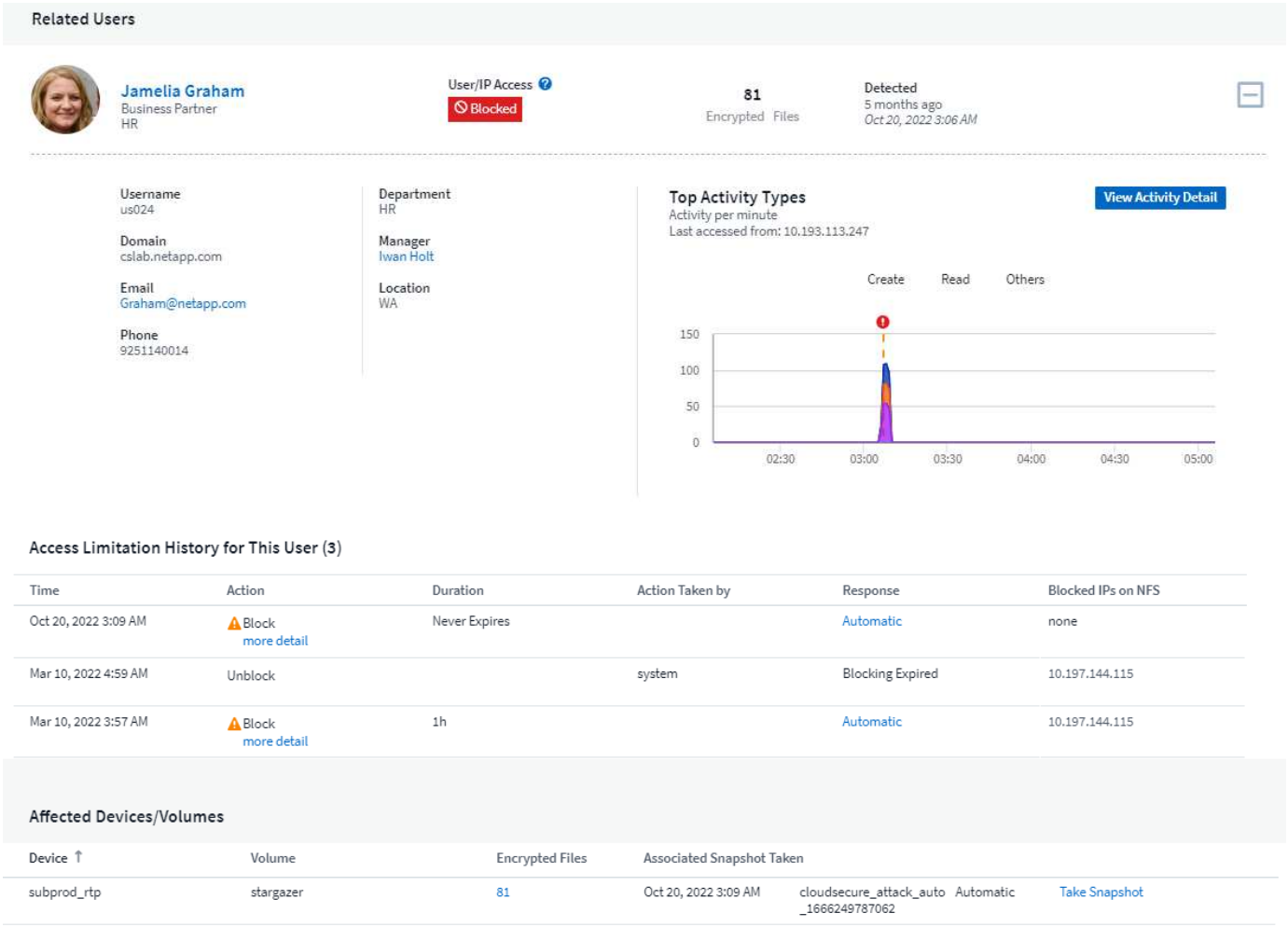
```
security login role create -role csrole -cmddirname "volume" -access
readonly
security login role create -role csrole -cmddirname "security anti-
ransomware volume" -access readonly
```

Leia mais sobre como configurar outros"Permissões da ONTAP" .

Alerta de amostra

Um exemplo de alerta gerado devido ao evento ARP é mostrado abaixo:





Um indicador de alta confiança mostra que o ataque apresentou comportamento de adulteração de arquivos, juntamente com atividades de criptografia de arquivos. O gráfico de arquivos criptografados indica o registro de data e hora em que a atividade de criptografia do volume foi detectada pela solução ARP.

Limitações

No caso em que um SVM não é monitorado pelo Workload Security, mas há eventos ARP gerados pelo ONTAP, os eventos ainda serão recebidos e exibidos pelo Workload Security. No entanto, informações forenses relacionadas ao alerta, bem como o mapeamento do usuário, não serão capturadas ou exibidas.

Solução de problemas

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

Problema:	Resolução:
Os alertas por e-mail são recebidos 24 horas após um ataque ser detectado. Na interface do usuário, os alertas são exibidos 24 horas antes, quando os e-mails são recebidos pelo Data Infrastructure Insights Workload Security.	Quando o ONTAP envia o evento *Ransomware detectado* para o Data Infrastructure Insights Workload Security (ou seja, Workload Security), o e-mail é enviado. O evento contém uma lista de ataques e seus registros de data e hora. A interface do usuário do Workload Security exibe o registro de data e hora do alerta do primeiro arquivo atacado. O ONTAP envia o evento *Ransomware detectado* para o Data Infrastructure Insights quando um determinado número de arquivos é codificado. Portanto, pode haver uma diferença entre o momento em que o alerta é exibido na interface do usuário e o momento em que o e-mail é enviado.

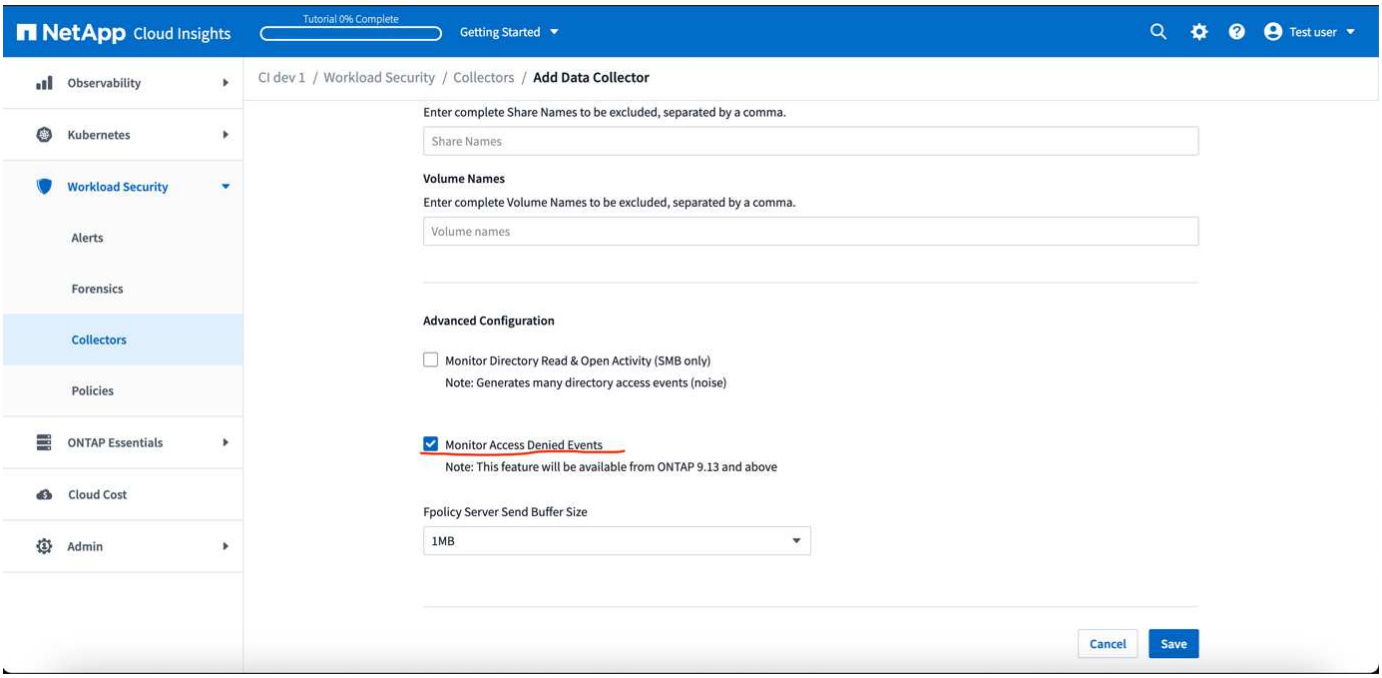
Integração com ONTAP Acesso negado

O recurso ONTAP Access Denied usa análise de carga de trabalho em ambientes NAS (NFS e SMB) para detectar e alertar proativamente sobre operações de arquivo com falha (ou seja, um usuário tentando executar uma operação para a qual não tem permissão). Essas notificações de falha na operação de arquivos — especialmente em casos de falhas relacionadas à segurança — ajudarão ainda mais a bloquear ataques internos nos estágios iniciais.

O Data Infrastructure Insights Workload Security integra-se ao ONTAP para receber eventos de acesso negado e fornecer uma camada adicional de resposta analítica e automática.

Pré-requisitos

- Versão mínima do ONTAP : 9.13.0.
- Um administrador de segurança de carga de trabalho deve habilitar o recurso Acesso negado ao adicionar um novo coletor ou editar um coletor existente, marcando a caixa de seleção *Monitorar eventos de acesso negado* em Configuração avançada.



Permissões de usuário necessárias

Se o Coletor de Dados for adicionado usando credenciais de administração de cluster, nenhuma nova permissão será necessária.

Se o Collector for adicionado usando um usuário personalizado (por exemplo, *csuser*) com permissões dadas ao usuário, siga as etapas abaixo para dar ao Workload Security a permissão necessária para registrar eventos de Acesso Negado com o ONTAP.

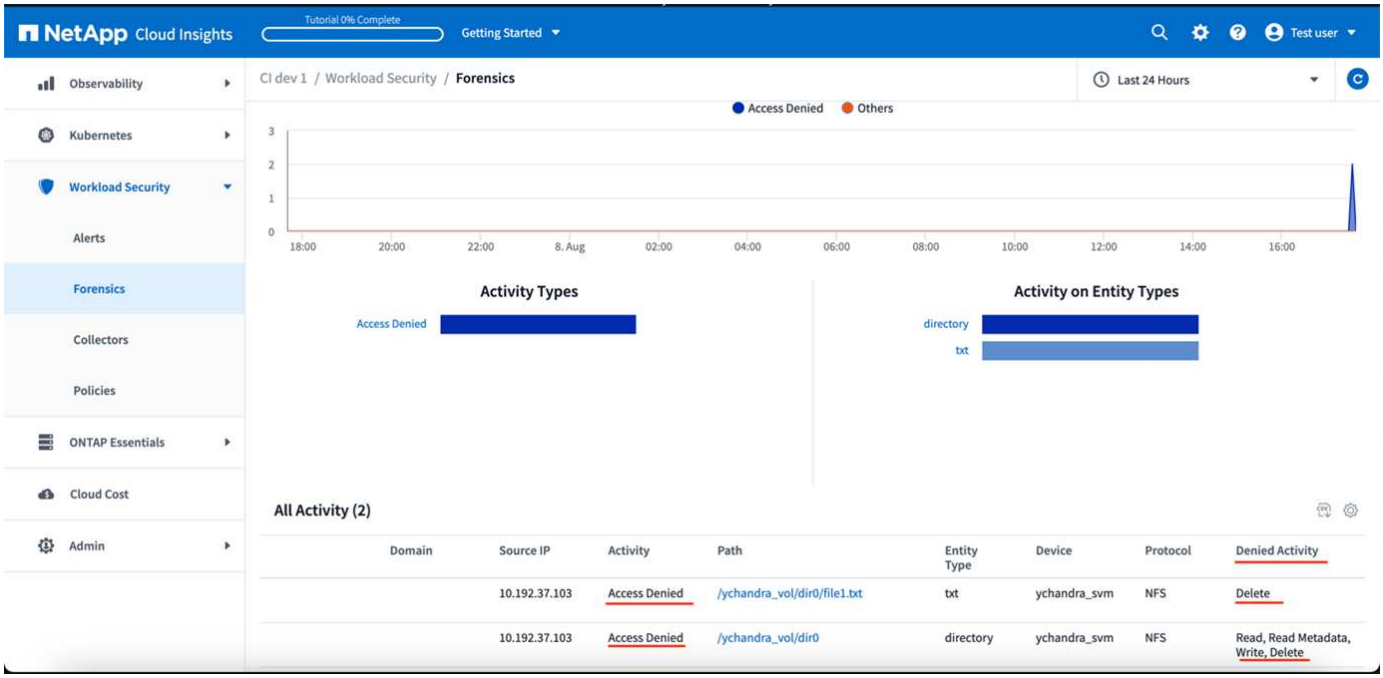
Para csuser com credenciais *cluster*, execute os seguintes comandos na linha de comando do ONTAP . Observe que essa permissão pode já existir.

```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
Para csuser com credenciais _SVM_, execute os seguintes comandos na linha
de comando do ONTAP .  Observe que essa permissão pode já existir.
```

```
 security login role create -vserver <vservername> -role csrole
-cmddirname "vserver fpolicy" -access all
Leia mais sobre como configurar
outroslink:task_add_collector_svm.html["Permissões da ONTAP"] .
```

Eventos de acesso negado

Depois que os eventos forem adquiridos do sistema ONTAP , a página Análise Forense de Segurança de Carga de Trabalho mostrará eventos de Acesso Negado. Além das informações exibidas, você pode visualizar as permissões de usuário ausentes para uma operação específica adicionando a coluna *Atividade desejada* à tabela no ícone de engrenagem.



Bloquear o acesso do usuário para impedir ataques

Interrompa imediatamente os ataques detectados bloqueando o acesso do usuário comprometido para evitar maiores danos ou exfiltração de dados. A Segurança de Carga de Trabalho permite tanto o bloqueio automático por meio de Políticas de Resposta Automatizadas quanto a intervenção manual a partir de alertas ou páginas de detalhes do usuário, oferecendo controle flexível sobre sua resposta de segurança. As restrições de acesso são aplicadas automaticamente a todos os volumes de armazenamento monitorados e têm um prazo de validade para restauração automática.

O usuário é bloqueado diretamente para SMB e o endereço IP das máquinas host que causam o ataque será bloqueado para NFS. Esses endereços IP de máquina serão bloqueados para acessar qualquer uma das Máquinas Virtuais de Armazenamento (SVMs) monitoradas pelo Workload Security.

Por exemplo, digamos que o Workload Security gerencia 10 SVMs e a Política de Resposta Automática está configurada para quatro dessas SVMs. Se o ataque tiver origem em uma das quatro SVMs, o acesso do usuário será bloqueado em todas as 10 SVMs. Um Snapshot ainda é tirado no SVM de origem.

Se houver quatro SVMs com uma SVM configurada para SMB, uma configurada para NFS e as duas restantes configuradas para NFS e SMB, todas as SVMs serão bloqueadas se o ataque tiver origem em qualquer uma das quatro SVMs.

Pré-requisitos 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 abaixo para dar permissões ao Workload Security para bloquear o usuário.

Para csuser com credenciais de cluster, faça o seguinte na linha de comando do ONTAP :

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

Não deixe de revisar a seção Permissões do"Configurando o coletor de dados ONTAP SVM" página também.

Como habilitar o recurso?

- Em Segurança de Carga de Trabalho, navegue até **Segurança de Carga de Trabalho > Políticas > Políticas de Resposta Automatizada**. Escolha **+Política de Ataque**.
- Selecione (marque) *Bloquear acesso de usuário a arquivos*.

Como configurar o bloqueio automático de acesso de usuários?

- Crie uma nova Política de Ataque ou edite uma política de Ataque existente.
- Selecione as SVMs nas quais a política de ataque deve ser monitorada.
- Clique na caixa de seleção “Bloquear acesso do usuário ao arquivo”. O recurso será habilitado quando esta opção for selecionada.
- Em “Período de tempo”, selecione o tempo até o qual o bloqueio deve ser aplicado.
- Para testar o bloqueio automático de usuários, você pode simular um ataque por meio de um"roteiro simulado" .

Como saber se há usuários bloqueados no sistema?

- Na página de listas de alertas, um banner na parte superior da tela será exibido caso algum usuário seja bloqueado.
- Clicar no banner levará você para a página “Usuários”, onde a lista de usuários bloqueados pode ser vista.
- Na página “Usuários”, há uma coluna chamada “Acesso de Usuário/IP”. Nessa coluna, será exibido o estado atual do bloqueio do usuário.

Restringir e gerenciar o acesso do usuário manualmente

- Você pode ir para a tela de detalhes do alerta ou detalhes do usuário e então bloquear ou restaurar manualmente um usuário a partir dessas telas.

Histórico de Limitação de Acesso do Usuário

Na página de detalhes do alerta e do usuário, no painel do usuário, você pode visualizar uma auditoria do histórico de limitação de acesso do usuário: Hora, Ação (Bloquear, Desbloquear), duração, ação tomada por, manual/automático e IPs afetados para NFS.

Como desabilitar o recurso?

Você pode desativar o recurso a qualquer momento. Se houver usuários restritos no sistema, você deverá restaurar o acesso deles primeiro.

- Em Segurança de Carga de Trabalho, navegue até **Segurança de Carga de Trabalho > Políticas > Políticas de Resposta Automatizada**. Escolha **+Política de Ataque**.
- Desmarque a opção *Bloquear acesso do usuário ao arquivo*.

O recurso ficará oculto em todas as páginas.

Restaurar IPs manualmente para NFS

Use as etapas a seguir para restaurar manualmente quaisquer IPs do ONTAP se o seu teste do Workload Security expirar ou se o agente/coletor estiver inativo.

1. Listar todas as políticas de exportação em um SVM.

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

2. Exclua as regras em todas as políticas no SVM que têm “cloudsecure_rule” como Client Match especificando seu respectivo RuleIndex. A regra de segurança da carga de trabalho geralmente será 1.

```
 contrail-qa-fas8020:*> export-policy rule delete -vserver <svm name>
-policyname * -ruleindex 1
. Garanta que a regra de segurança da carga de trabalho seja excluída
(etapa opcional para confirmação).
```

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

Restaurar usuários manualmente para SMB

Use as etapas a seguir para restaurar manualmente qualquer usuário do ONTAP se o teste do Workload Security expirar ou se o agente/coletor estiver inativo.

Você pode obter a lista de usuários bloqueados no Workload Security na página da lista de usuários.

1. Efetue login no cluster ONTAP (onde você deseja desbloquear usuários) com as credenciais de administrador do cluster. (Para Amazon FSx, faça login com credenciais do FSx).
2. Execute o seguinte comando para listar todos os usuários bloqueados pelo Workload Security para SMB em todas as SVMs:

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

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

Na saída acima, 2 usuários foram bloqueados (US030, US040) com domínio CSLAB.

1. Depois de identificar a posição na saída acima, execute o seguinte comando para desbloquear o usuário:

```
 vserver name-mapping delete -direction win-unix -position <position>
. Confirme se os usuários estão desbloqueados executando o comando:
```

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

Nenhuma entrada deve ser exibida para os usuários bloqueados anteriormente.

Solução de problemas

Problema	Experimente isto
Alguns usuários não estão sendo restringidos, embora haja um ataque.	1. Certifique-se de que o Coletor de Dados e o Agente para as SVMs estejam no estado *Em execução*. O Workload Security não poderá enviar comandos se o Data Collector e o Agent estiverem parados. 2. Isso ocorre porque o usuário pode ter acessado o armazenamento de uma máquina com um novo IP que não foi usado antes. A restrição ocorre por meio do endereço IP do host por meio do qual o usuário está acessando o armazenamento. Verifique na IU (Detalhes do alerta > Histórico de limitação de acesso para este usuário > IPs afetados) a lista de endereços IP que estão restritos. Se o usuário estiver acessando o armazenamento de um host que tenha um IP diferente dos IPs restritos, o usuário ainda poderá acessar o armazenamento por meio do IP não restrito. Se o usuário estiver tentando acessar de hosts cujos IPs são restritos, o armazenamento não estará acessível.
Clicar manualmente em Restringir acesso resulta na mensagem “Endereços IP deste usuário já foram restringidos”.	O IP a ser restrito já está sendo restringido por outro usuário.
A política não pôde ser modificada. Motivo: não autorizado para esse comando.	Verifique se ao usar csuser, as permissões são concedidas ao usuário conforme mencionado acima.

Problema	Experimente isto
O bloqueio de usuário (endereço IP) para NFS funciona, mas para SMB/CIFS, vejo uma mensagem de erro: “Falha na transformação de SID para DomainName. Motivo do tempo limite: o soquete não foi estabelecido”	Isso pode acontecer se *csuser* não tiver permissão para executar ssh. (Garanta a conexão no nível do cluster e, em seguida, certifique-se de que o usuário pode executar o ssh). A função *csuser* requer essas permissões. https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blocking Para *csuser* com credenciais de cluster, faça o seguinte na linha de comando do ONTAP : security login role create -role csrole -cmddirname "vserver export-policy rule" -access all security login role create -role csrole -cmddirname set -access all security login role create -role csrole -cmddirname "vserver cifs session" -access all security login role create -role csrole -cmddirname "vserver services access-check authentication translate" -access all security login role create -role csrole -cmddirname "vserver name-mapping" -access all Se *csuser* não for usado e se o usuário administrador no nível do cluster for usado, certifique-se de que o usuário administrador tenha permissão ssh para o ONTAP.
Estou recebendo a mensagem de erro *Falha na tradução do SID. Motivo:255:Erro: comando falhou: não autorizado para esse comandoErro: "access-check" não é um comando reconhecido*, quando um usuário deveria ter sido bloqueado.	Isso pode acontecer quando *csuser* não tem permissões corretas. Ver "Pré-requisitos para bloqueio de acesso do usuário" para maiores informações. Após aplicar as permissões, é recomendável reiniciar o coletor de dados ONTAP e o coletor de dados do Diretório do Usuário. Os comandos de permissão necessários estão listados abaixo. ---- função de login de segurança create -role csrole -cmddirname "regra de política de exportação do vserver" -access all função de login de segurança create -role csrole -cmddirname set -access all função de login de segurança create -role csrole -cmddirname "sessão cifs do vserver" -access all função de login de segurança create -role csrole -cmddirname "autenticação de verificação de acesso aos serviços do vserver translate" -access all função de login de segurança create -role csrole -cmddirname "mapeamento de nomes do vserver" -access all ----

Segurança da carga de trabalho: Simulação de adulteração de arquivos

Você pode usar as instruções desta página para simular a adulteração de arquivos para testar ou demonstrar a segurança da carga de trabalho usando o script de simulação de adulteração de arquivos incluído.

Coisas a serem observadas antes de começar

- O script de simulação de adulteração de arquivos funciona apenas no Linux. O script de simulação também deve gerar alertas de alta confiança caso o usuário tenha integrado o ONTAP ARP com a Segurança de Carga de Trabalho.
- O Workload Security detectará eventos e alertas gerados com o NFS 4.1 somente se a versão do ONTAP for 9.15 ou superior.
- O script é fornecido com os arquivos de instalação do agente do Workload Security. Ele está disponível em qualquer máquina que tenha um agente de segurança de carga de trabalho instalado.
- Você pode executar o script na própria máquina do agente do Workload Security; não há necessidade de preparar outra máquina Linux. Entretanto, se você preferir executar o script em outro sistema, basta copiá-lo e executá-lo lá.
- Os usuários podem optar pelo Python ou pelo shell script com base em suas preferências e requisitos do sistema.
- O script Python tem instalações pré-requisitos. Se você não quiser usar python, use o script shell.

Diretrizes:

Este script deve ser executado em um SVM contendo uma pasta com um número substancial de arquivos para criptografia, idealmente 100 ou mais, incluindo arquivos em subpastas. Certifique-se de que os arquivos não estejam vazios.

Para gerar o alerta, pause temporariamente o coletor antes da criação dos dados de teste. Depois que os arquivos de amostra forem gerados, reinicie o coletor e inicie o processo de criptografia.

Passos:

Prepare o sistema:

Primeiro, monte o volume de destino na máquina. Você pode montar uma exportação NFS ou CIFS.

Para montar a exportação NFS no Linux:

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

Não monte o NFS versão 4.1; ele não é suportado pelo Fpolicy.

Para montar o CIFS no Linux:

```
mount -t cifs //10.193.77.91/sharedfolderincluster
/root/destinationfolder/ -o username=raisa
```

Ativar a Proteção Autônoma contra Ransomware do ONTAP (opcional):

Se a versão do seu cluster ONTAP for 9.11.1 ou superior, você poderá habilitar o serviço ONTAP Ransomware Protection executando o seguinte comando no console de comando do ONTAP .

```
 security anti-ransomware volume enable -volume [volume_name] -vserver
[svm_name]
Em seguida, configure um coletor de dados:
```

1. Configure o agente de segurança de carga de trabalho, caso ainda não tenha feito isso.
2. Configure um coletor de dados SVM se ainda não tiver feito isso.
3. Certifique-se de que o protocolo de montagem esteja selecionado ao configurar o coletor de dados.

Gere os arquivos de amostra programaticamente:

Antes de criar os arquivos, você deve primeiro parar ou"pausar o coletor de dados" processamento.

Antes de executar a simulação, você deve primeiro adicionar os arquivos a serem criptografados. Você pode copiar manualmente os arquivos a serem criptografados na pasta de destino ou usar um dos scripts incluídos para criar os arquivos programaticamente. Seja qual for o método usado, certifique-se de que haja pelo menos 100 arquivos presentes para criptografar.

Se você optar por criar os arquivos programaticamente, poderá usar o Shell ou o Python:

Concha:

1. Entre na caixa do Agente.
2. Monte um compartilhamento NFS ou CIFS do SVM do arquivador para a máquina do agente. Cd para essa pasta.
3. Copie o script do diretório de instalação do agente (%AGENT_INSTALL_DIR/ agent/install/ransomware_simulation/shell/create_dataset.sh) para o local de montagem de destino.
4. Execute o seguinte comando usando os scripts dentro do diretório montado (por exemplo, /root/demo) para criar a pasta e os arquivos do conjunto de dados de teste:

```
 './create_dataset.sh'
. Isso criará 100 arquivos não vazios com várias extensões dentro da
pasta de montagem em um diretório chamado "test_dataset".
```

Pitão:

Pré-requisito do script Python:

- Instale o Python (se ainda não estiver instalado).
  - Baixe o Python 3.5.2 ou superior em https://www.python.org/ .
  - Para verificar a instalação do Python, execute `python --version` .
  - O script Python foi testado em versões tão antigas quanto a 3.5.2.
- Instale o pip se ainda não estiver instalado:
  - Baixe o script get-pip.py em https://bootstrap.pypa.io/ .
  - Instalar pip usando `python get-pip.py` .

- Verifique a instalação do pip com `pip --version`.

- Biblioteca PyCryptodome:
  - O script usa a biblioteca PyCryptodome.
  - Instalar PyCryptodome com `pip install pycryptodome`.
  - Confirme a instalação do PyCryptodome executando `pip show pycryptodome`.

Script de criação de arquivo em Python:

1. Entre na caixa do Agente.
2. Monte um compartilhamento NFS ou CIFS do SVM do arquivador para a máquina do agente. Cd para essa pasta.
3. Copie o script do diretório de instalação do agente (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/python/create_dataset.py) para o local de montagem de destino.
4. Execute o seguinte comando usando os scripts dentro do diretório montado (por exemplo, /root/demo) para criar a pasta e os arquivos do conjunto de dados de teste:

```
 'python create_dataset.py'
. Isso criará 100 arquivos não vazios com várias extensões dentro da
pasta de montagem em um diretório chamado "test_dataset"
```

Retomar o coletor

Se você pausou o coletor antes de seguir estas etapas, certifique-se de retomá-lo depois que os arquivos de amostra forem criados.

Gere os arquivos de amostra programaticamente:

Antes de criar os arquivos, você deve primeiro parar ou"pausar o coletor de dados" processamento.

Para gerar um alerta de adulteração de arquivo, você pode executar o script incluído, que simulará um alerta de adulteração de arquivo no Workload Security.

Concha:

1. Copie o script do diretório de instalação do agente (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/shell/simulate_attack.sh) para o local de montagem de destino.
2. Execute o seguinte comando usando os scripts dentro do diretório montado (por exemplo, /root/demo) para criptografar o conjunto de dados de teste:

```
 './simulate_attack.sh'
. Isso criptografará os arquivos de amostra criados no diretório
"test_dataset".
```

Pitão:

1. Copie o script do diretório de instalação do agente (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/python/simulate_attack.py) para o local de montagem de destino.
2. Observe que os pré-requisitos do Python são instalados conforme a seção Pré-requisitos do script Python
3. Execute o seguinte comando usando os scripts dentro do diretório montado (por exemplo, /root/demo) para criptografar o conjunto de dados de teste:

```
 'python simulate_attack.py'
. Isso criptografará os arquivos de amostra criados no diretório
"test_dataset".
```

Gerar um alerta no Workload Security

Quando a execução do script do simulador for concluída, um alerta será exibido na interface do usuário da Web em alguns minutos.

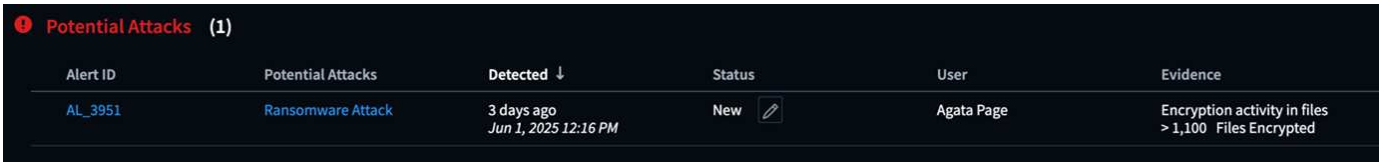
Observação: caso todas as condições a seguir sejam atendidas, um Alerta de Alta Confiança será gerado.

1. Monitorou a versão ONTAP do SVM superior a 9.11.1
2. Proteção autônoma contra ransomware ONTAP configurada
3. O coletor de dados de segurança da carga de trabalho é adicionado no modo Cluster.

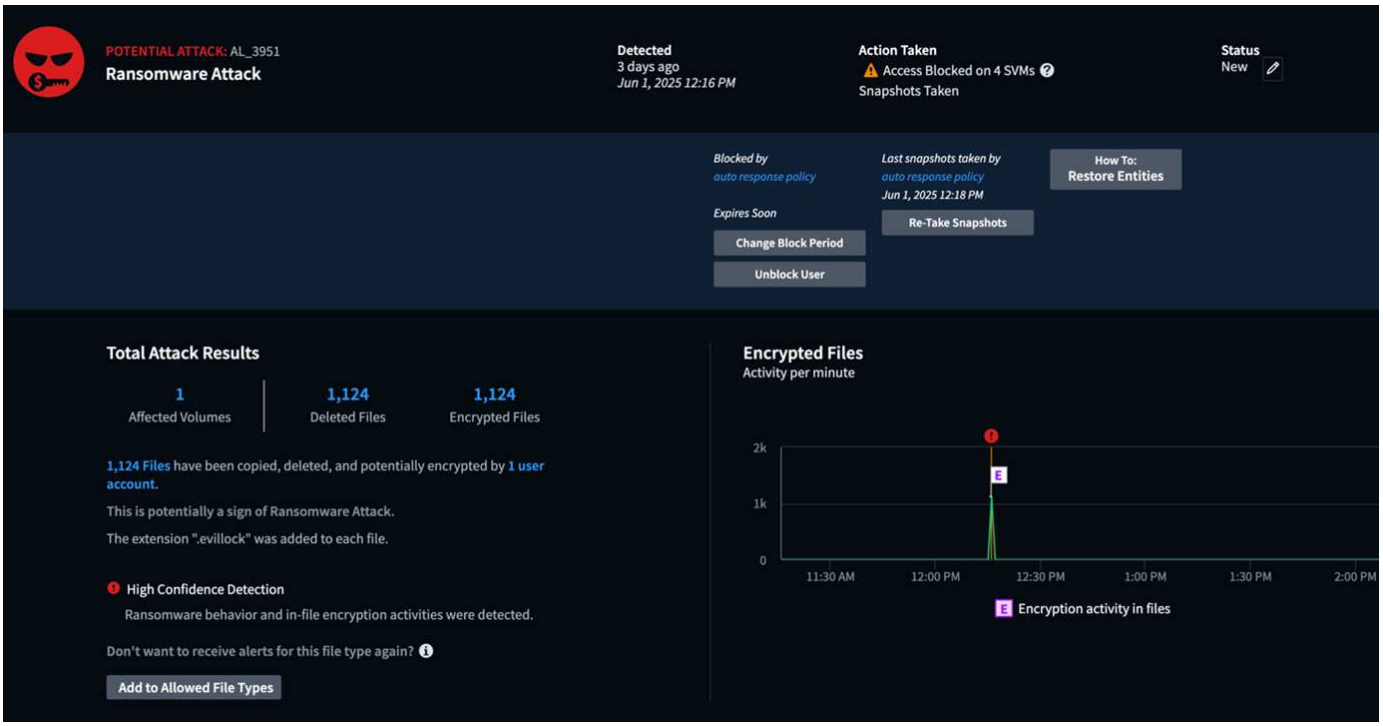
O Workload Security detecta padrões de adulteração de arquivos com base no comportamento do usuário, enquanto o ONTAP ARP detecta atividades de adulteração de arquivos com base em atividades de criptografia nos arquivos.

Se as condições forem atendidas, o Workload Security marcará os alertas como Alerta de Alta Confiança.

Exemplo de alerta de alta confiança na página Lista de alertas:



Exemplo de detalhe de alerta de alta confiança:



Disparando alertas várias vezes

O Workload Security aprende o comportamento do usuário e não gerará alertas sobre ataques repetidos de adulteração de arquivos dentro de 24 horas para o mesmo usuário.

Para gerar um novo alerta com um usuário diferente, siga os mesmos passos novamente (criando dados de teste e criptografando os dados de teste).

Configurando notificações por e-mail para alertas, avisos e integridade do agente/coletor de fonte de dados

As notificações por e-mail permitem que você se mantenha informado sobre possíveis ataques, alertas de segurança e problemas de infraestrutura assim que eles ocorrerem. Configure os endereços de e-mail dos destinatários em Administração > Notificações para receber alertas em tempo real personalizados de acordo com as responsabilidades de cada destinatário.

Alertas e avisos de ataques potenciais

Para enviar notificações de alerta de *Ataque Potencial*, insira os endereços de e-mail dos destinatários na seção *Enviar Alertas de Ataque Potencial*. Notificações por e-mail são enviadas para a lista de destinatários do alerta para cada ação no alerta.

Para enviar notificações de *Aviso*, insira os endereços de e-mail dos destinatários na seção *Enviar alertas de aviso*.

Monitoramento de integridade do agente e do coletor de dados

Você pode monitorar a integridade dos Agentes e Fontes de Dados por meio de notificações.

Para receber notificações caso um Agente ou coletor de Fonte de Dados não esteja funcionando, insira os endereços de e-mail dos destinatários na seção *Alertas de integridade da coleta de dados*.

Tenha em mente o seguinte:

- Os alertas de saúde serão enviados somente após o agente/coletor parar de reportar por pelo menos uma hora.
- Apenas uma notificação por e-mail é enviada aos destinatários pretendidos em um determinado período de 24 horas, mesmo que o Agente ou o Coletor de Dados esteja desconectado por um período mais longo.
- Em caso de falha de um Agente, um alerta será enviado (não um por coletor). O e-mail incluirá uma lista de todos os SVMs afetados.
- A falha na coleta de dados do Active Directory é relatada como um aviso; ela não afeta a detecção de ameaças.
- A lista de configuração de Introdução agora inclui uma nova fase *Configurar notificações por e-mail*.

Recebendo notificações de atualização do agente e do coletor de dados

- Insira o(s) ID(s) de e-mail em “Alertas de saúde de coleta de dados”.
- A caixa de seleção “Habilitar notificações de atualização” fica habilitada.
- As notificações por e-mail de atualização do Agente e do Coletor de Dados são enviadas para os IDs de e-mail um dia antes da atualização planejada.

Solução de problemas

Problema:	Experimente isto:
Os IDs de e-mail estão presentes nos “Alertas de saúde do coletor de dados”, mas não estou recebendo notificações.	Os e-mails de notificação são enviados do domínio do NetApp Data Infrastructure Insights , ou seja, de *accounts@service.cloudinsights.netapp.com*. Algumas empresas bloqueiam e-mails recebidos se eles forem de um domínio externo. Certifique-se de que as notificações externas dos domínios do NetApp Data Infrastructure Insights estejam na lista de permissões.

Notificações de webhook

Notificações de segurança de carga de trabalho usando webhooks

Os webhooks permitem que os usuários enviem notificações de alerta críticas ou de advertência para vários aplicativos usando um canal de webhook personalizado.

Muitos aplicativos comerciais oferecem suporte a webhooks como uma interface de entrada padrão, por exemplo: Slack, PagerDuty, Teams e Discord. Ao oferecer suporte a um canal webhook genérico e personalizável, o Workload Security pode oferecer suporte a muitos desses canais de entrega. Informações sobre como configurar os webhooks podem ser encontradas nos sites dos respectivos aplicativos. Por exemplo, o Slack fornece"este guia útil" .

Você pode criar vários canais de webhook, cada canal direcionado a uma finalidade diferente, aplicativos

separados, destinatários diferentes, etc.

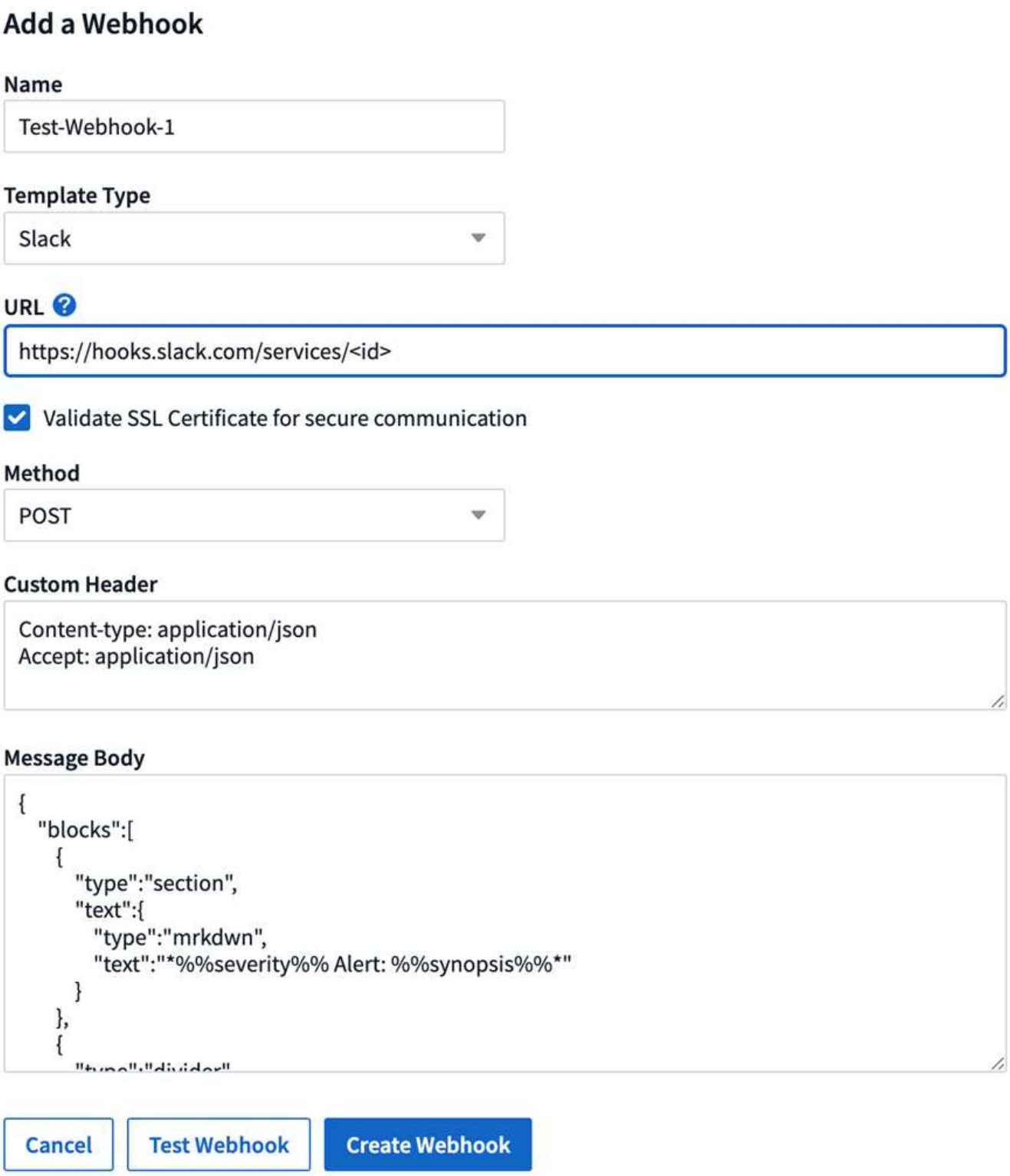
A instância do canal webhook é composta pelos seguintes elementos

Nome	Descrição
URL	URL de destino do webhook, incluindo o prefixo http:// ou https:// junto com os parâmetros de URL
Método	GET/POST - O padrão é POST
Cabeçalho personalizado	Especifique quaisquer cabeçalhos personalizados aqui
Corpo da mensagem	Coloque o corpo da sua mensagem aqui
Parâmetros de alerta padrão	Lista os parâmetros padrão para o webhook
Parâmetros e segredos personalizados	Parâmetros e segredos personalizados permitem que você adicione parâmetros exclusivos e elementos seguros, como senhas

Criando um webhook

Para criar um Webhook de segurança de carga de trabalho, vá para Admin > Notificações e selecione a aba “Webhooks de segurança de carga de trabalho”. A imagem a seguir mostra uma tela de exemplo de criação de webhook do Slack.

Observação: o usuário deve ser um *Administrador* do Workload Security para criar e gerenciar Webhooks do Workload Security.



- Insira as informações apropriadas para cada um dos campos e clique em "Salvar".
- Você também pode clicar no botão "Testar Webhook" para testar a conexão. Observe que isso enviará o "Corpo da Mensagem" (sem substituições) para a URL definida de acordo com o Método selecionado.
- Os webhooks do SWS compreendem uma série de parâmetros padrão. Além disso, você pode criar seus próprios parâmetros ou segredos personalizados.

Parâmetros: O que são e como usá-los?

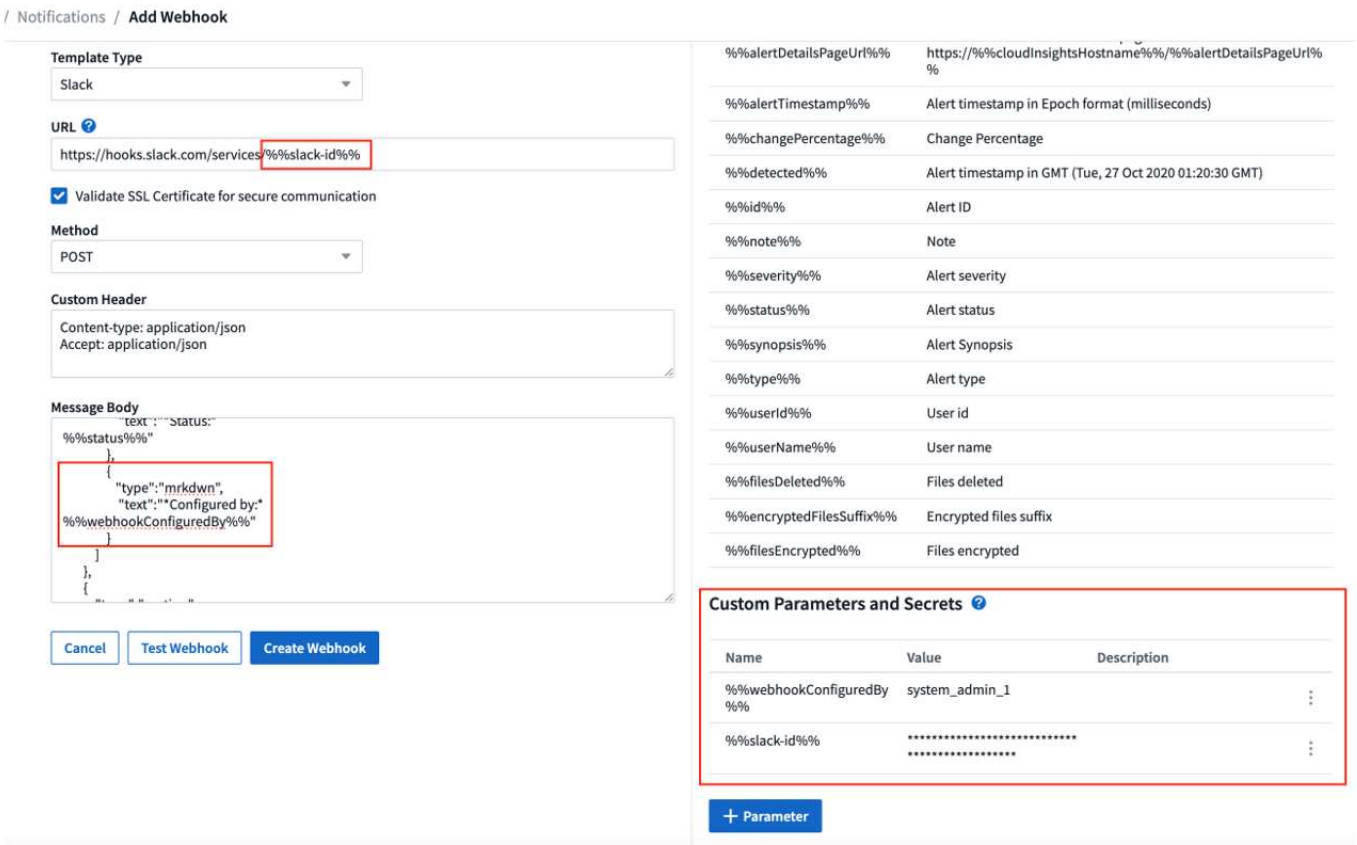
Parâmetros de alerta são valores dinâmicos preenchidos por alerta. Por exemplo, o parâmetro *%%severity%%* será substituído pelo tipo de gravidade do alerta.

Observe que as substituições não são realizadas ao clicar no botão "Testar Webhook"; o teste envia uma carga útil que mostra os espaços reservados do parâmetro (*%%<param-name>%%*), mas não os substitui por dados.

Parâmetros e segredos personalizados

Nesta seção, você pode adicionar quaisquer parâmetros personalizados e/ou segredos que desejar. Um parâmetro personalizado ou segredo pode estar no URL ou no corpo da mensagem. Os segredos permitem que o usuário configure um parâmetro personalizado seguro, como senha, apiKey etc.

A imagem de exemplo a seguir mostra como parâmetros personalizados são usados na criação de webhook.



Página da lista de webhooks de segurança de carga de trabalho

Na página da lista Webhooks, são exibidos os campos Nome, Criado por, Criado em, Status, Seguro e Último relatório. Observação: o valor da coluna 'status' continuará mudando com base no resultado do último gatilho do webhook. A seguir estão alguns exemplos de resultados de status.

Status	Descrição
OK	Notificação enviada com sucesso.
403	Proibido.
404	URL não encontrada.

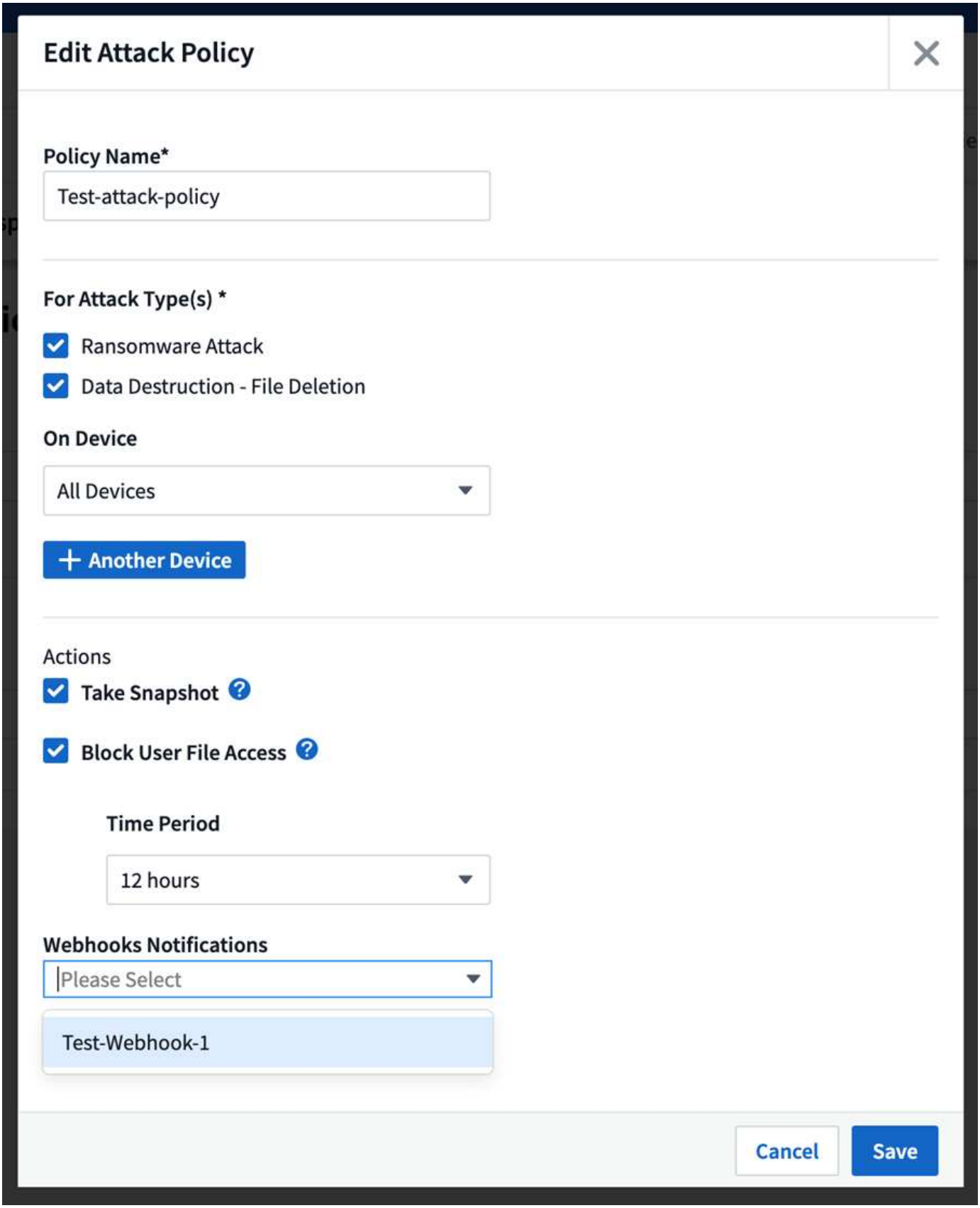
400	Pedido ruim. Você poderá ver esse status se houver algum erro no corpo da mensagem, por exemplo: • JSON mal formatado. • Fornecendo valor inválido para chaves reservadas. Por exemplo, o PagerDuty aceita apenas crítico/aviso/erro/informação para “Gravidade”. Qualquer outro resultado pode render um status 400. • Erros de validação específicos do aplicativo. Por exemplo, o Slack permite no máximo 10 campos dentro de uma seção. Incluir mais de 10 pode resultar em um status 400.
410	O recurso não está mais disponível

A coluna “Último relatório” indica o horário em que o webhook foi acionado pela última vez.

Na página de listagem de webhooks, os usuários também podem editar/duplicar/excluir webhooks.

Configurar notificação de Webhook na política de alerta

Para adicionar uma notificação de webhook a uma política de alerta, acesse -Segurança de carga de trabalho > Políticas- e selecione uma política existente ou adicione uma nova política. Na seção *Ações* > menu suspenso *Notificações de webhook*, selecione os webhooks necessários.



As notificações do webhook estão vinculadas às políticas. Quando o ataque (RW/DD/WARN) acontecer, a ação configurada (Tirar snapshot/bloqueio de usuário) será tomada e então a notificação de webhook associada será acionada.

Observação: as notificações por e-mail são independentes de políticas e serão acionadas normalmente.

- Se uma política for pausada, as notificações do webhook não serão acionadas.
- Vários webhooks podem ser anexados a uma única política, mas é recomendável anexar no máximo 5 webhooks a uma política.

Exemplos de webhook de segurança de carga de trabalho

Webhooks para"Folga"

Webhooks para"PagerDuty" Webhooks para"Equipes" Webhooks para"Discórdia"

Exemplo de webhook de segurança de carga de trabalho para Discord

Os webhooks permitem que os usuários enviem notificações de alerta para vários aplicativos usando um canal de webhook personalizado. Esta página fornece um exemplo de configuração de webhooks para o Discord.

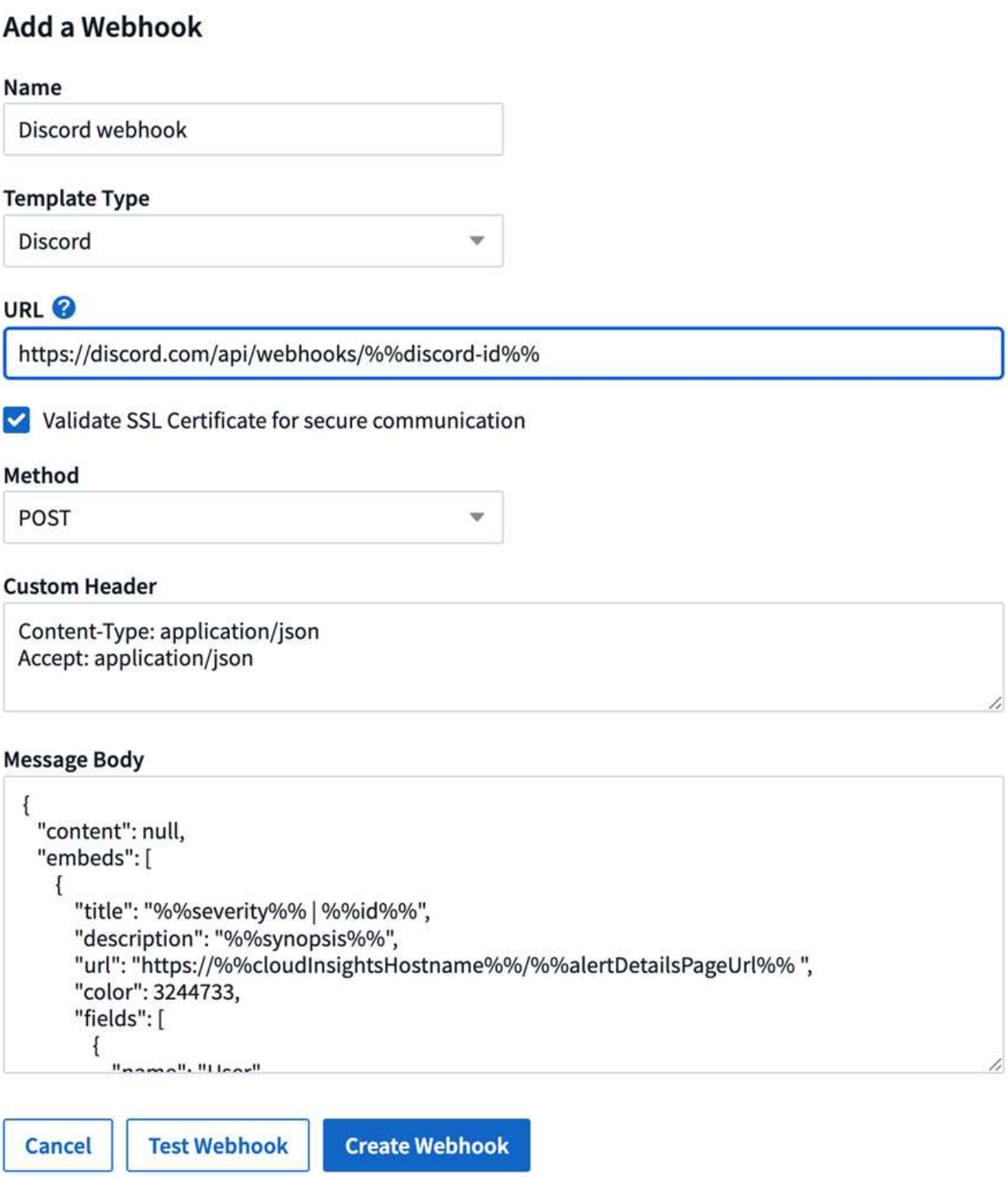
Esta página se refere a instruções de terceiros, que estão sujeitas a alterações. Consulte o"Documentação do Discord" para obter as informações mais atualizadas.

Configuração do Discord:

- No Discord, selecione o Servidor, em Canais de Texto, selecione Editar Canal (ícone de engrenagem)
- Selecione **Integrações > Exibir Webhooks** e clique em **Novo Webhook**
- Copie o URL do Webhook. Você precisará colar isso na configuração do webhook do Workload Security.

Criar Webhook de Segurança de Carga de Trabalho:

1. Navegue até Admin > Notificações e selecione a aba *Workload Security Webhooks*. Clique em "+ Webhook" para criar um novo webhook.
2. Dê ao webhook um nome significativo.
3. No menu suspenso *Tipo de modelo*, selecione **Discord**.
4. Cole a URL do Discord acima no campo *URL*.



Para testar o webhook, substitua temporariamente o valor da URL no corpo da mensagem por qualquer URL válida (como *https://netapp.com*) e clique no botão *Testar Webhook*. O Discord exige que uma URL válida seja fornecida para que a funcionalidade Test Webhook funcione.

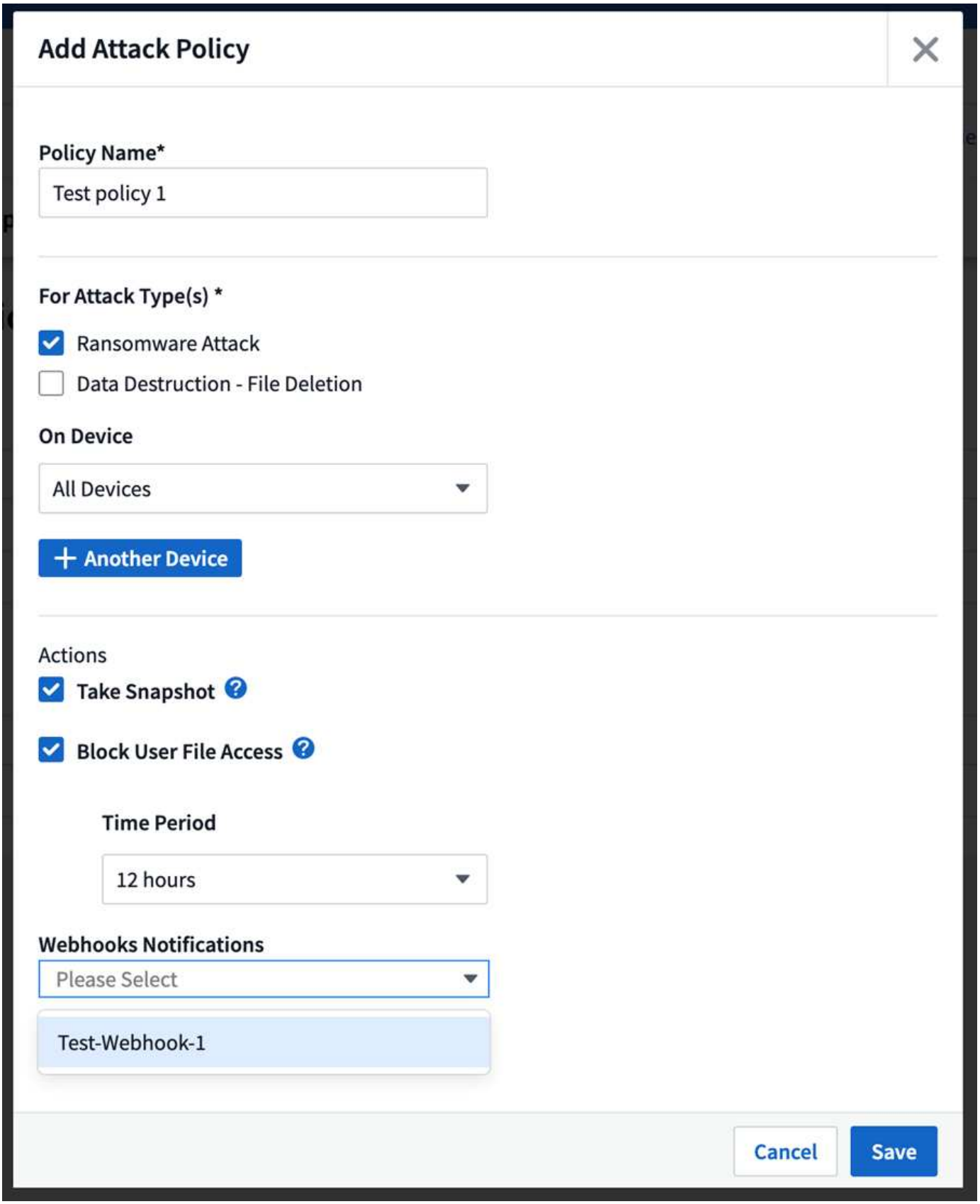
Não se esqueça de redefinir o corpo da mensagem quando o teste for concluído.

Notificações via Webhook

Para notificar eventos via webhook, navegue até *Segurança de carga de trabalho* > *Políticas*. Clique em *+Política de Ataque* ou *+Política de Aviso*.

- Insira um nome de política significativo.
- Selecione o(s) Tipo(s) de Ataque necessário(s), os Dispositivos aos quais a política deve ser anexada e as Ações necessárias.
- No menu suspenso *Notificações de Webhooks*, selecione os webhooks do Discord necessários e salve.

Observação: os webhooks também podem ser anexados às políticas existentes editando-as.



Exemplo de webhook de segurança de carga de trabalho para PagerDuty

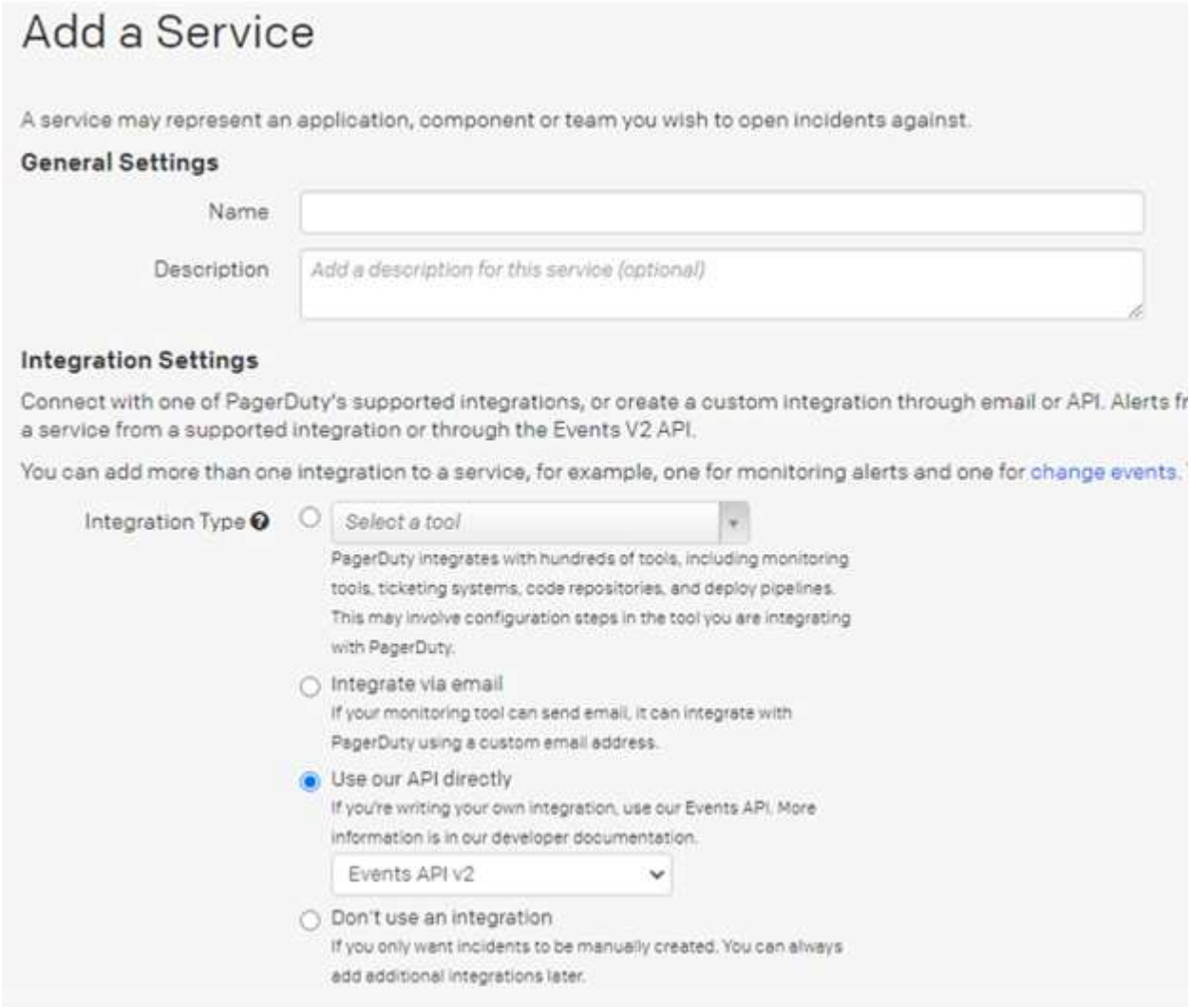
Os webhooks permitem que os usuários enviem notificações de alerta para vários aplicativos usando um canal de webhook personalizado. Esta página fornece um

exemplo de configuração de webhooks para o PagerDuty.

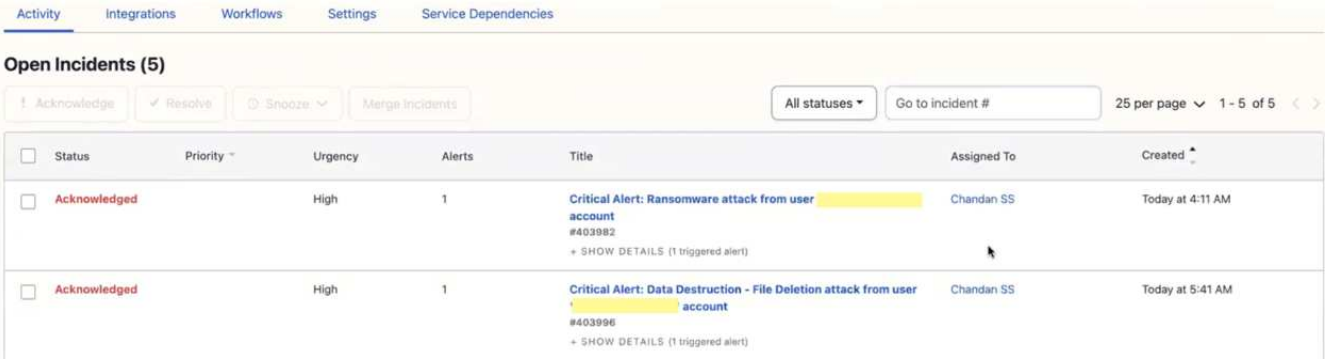
Esta página se refere a instruções de terceiros, que estão sujeitas a alterações. Consulte o"Documentação do PagerDuty" para obter as informações mais atualizadas.

Configuração do PagerDuty:

1. No PagerDuty, navegue até **Serviços > Diretório de serviços** e clique no botão **+Novo serviço**.
2. Digite um *Nome* e selecione *Usar nossa API diretamente*. Selecione *Adicionar serviço*.

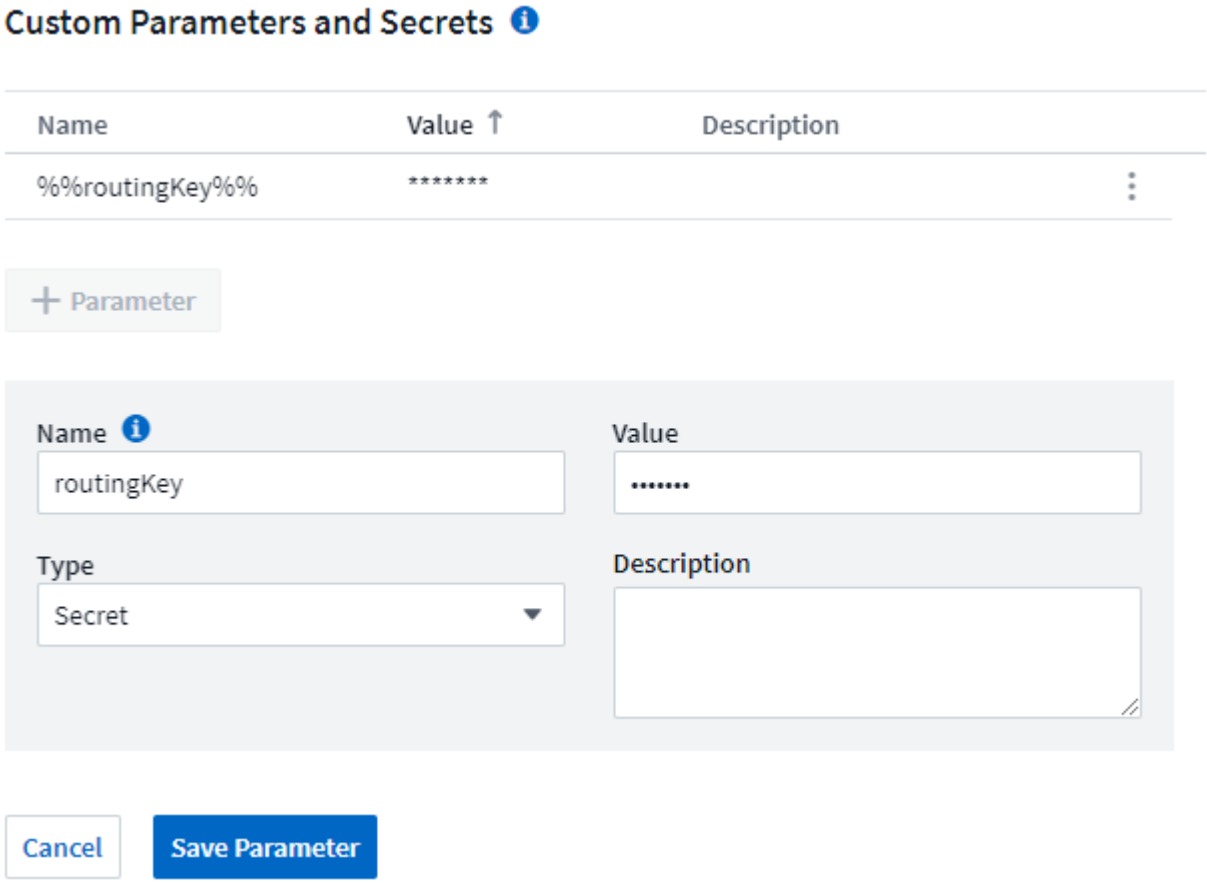


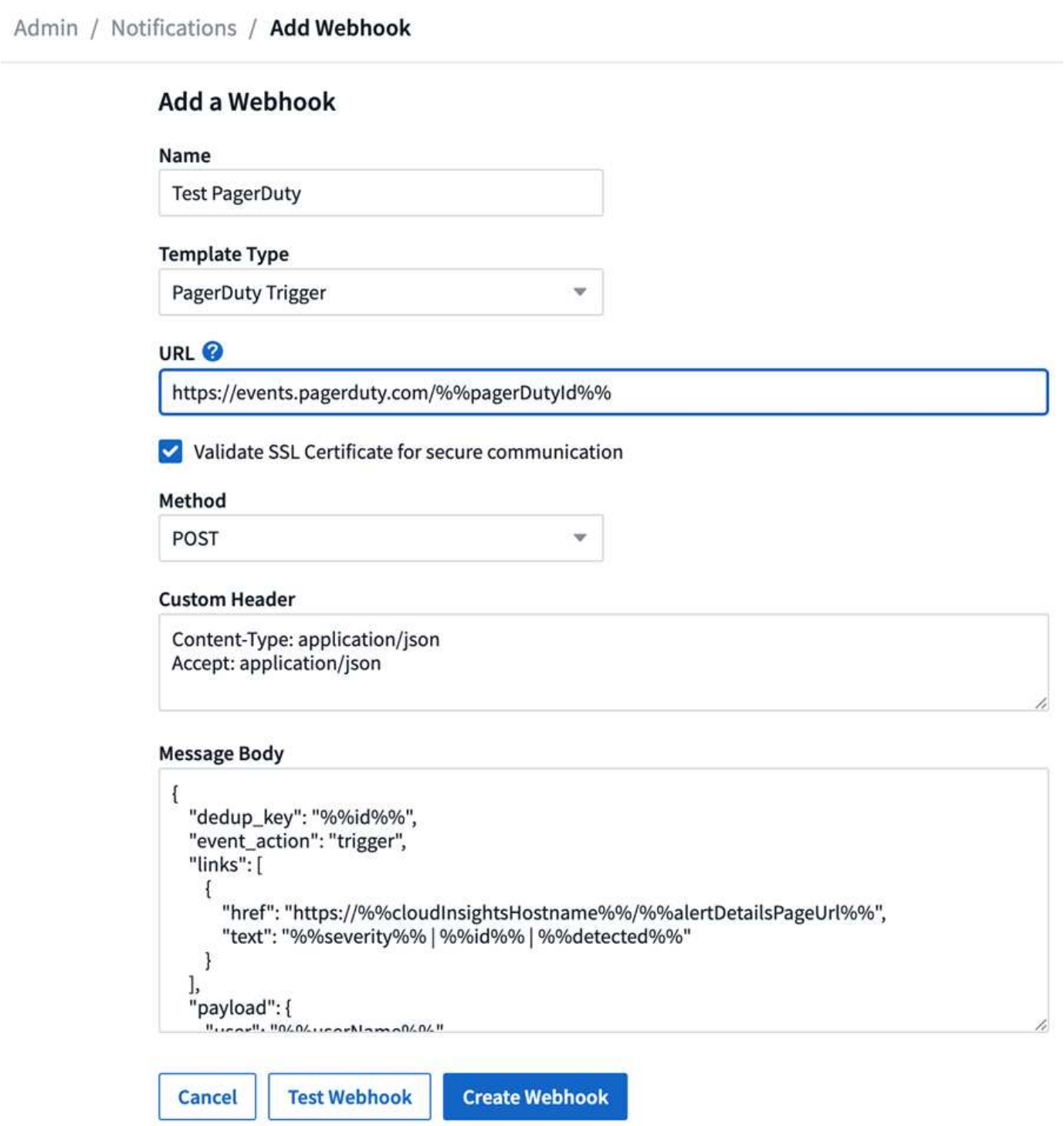
3. Selecione a aba *Integrações* para ver a **Chave de Integração**. Você precisará dessa chave ao criar o webhook do Workload Security abaixo.
4. Acesse **Incidentes** ou **Serviços** para visualizar Alertas.



Criar Webhook do PagerDuty de Segurança de Carga de Trabalho:

- Navegue até Admin > Notificações e selecione a aba *Workload Security Webhooks*. Selecione '+ Webhook' para criar um novo webhook.
- Dê ao webhook um nome significativo.
- No menu suspenso *Tipo de modelo*, selecione *Gatilho do PagerDuty*.
- Crie um segredo de parâmetro personalizado chamado *routingKey* e defina o valor como a *Chave de Integração* do PagerDuty criada acima.

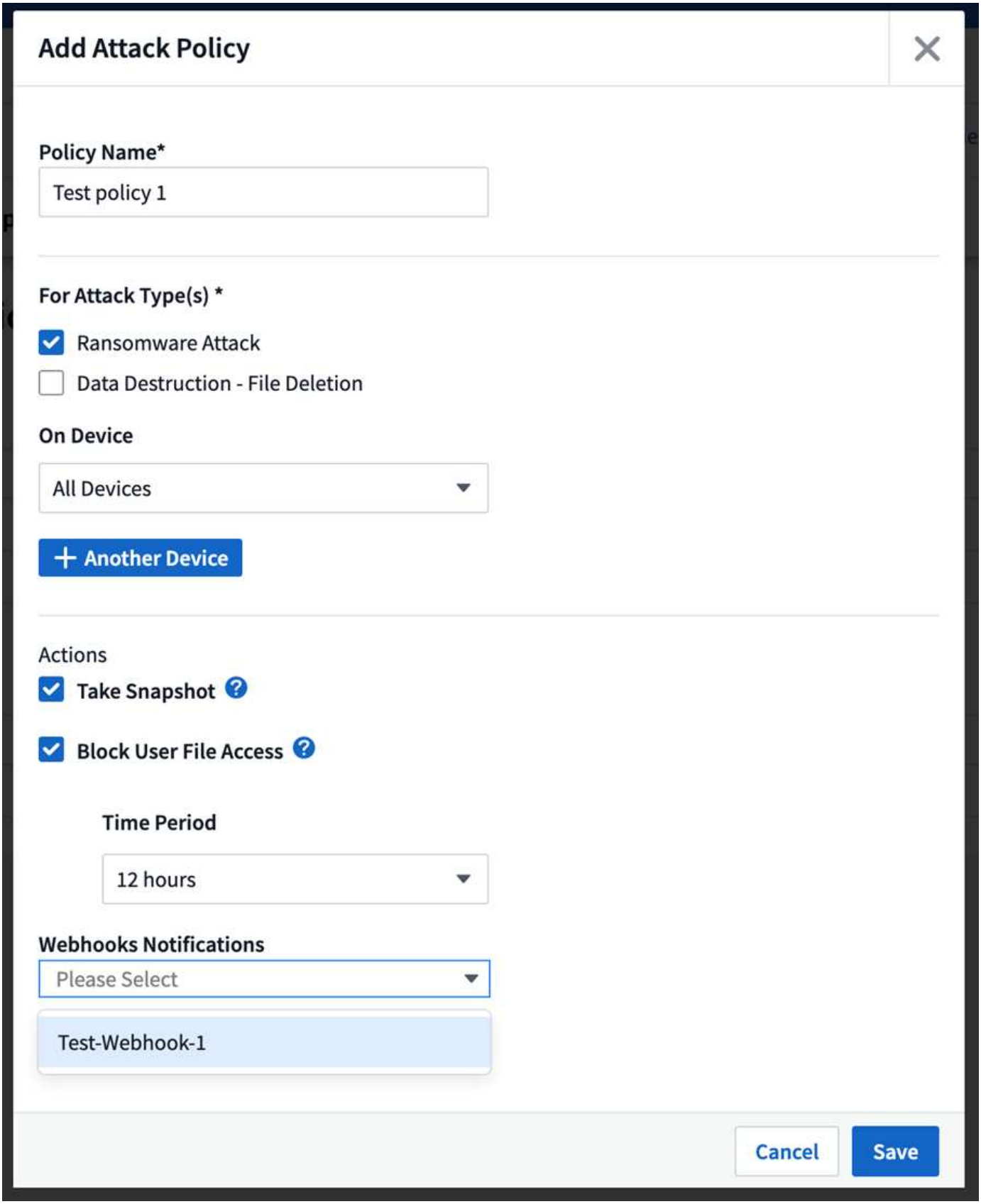




Notificações via Webhook

- Para notificar eventos via webhook, navegue até *Segurança de carga de trabalho > Políticas*. Selecione *+Política de Ataque* ou *+Política de Aviso*.
- Insira um nome de política significativo.
- Selecione os tipos de ataque necessários, os dispositivos aos quais a política deve ser anexada e as ações necessárias.
- No menu suspenso *Notificações de Webhooks*, selecione os webhooks do PagerDuty necessários. Salve a política.

Observação: os webhooks também podem ser anexados às políticas existentes editando-as.



Exemplo de webhook de segurança de carga de trabalho para Slack

Os webhooks permitem que os usuários enviem notificações de alerta para vários aplicativos usando um canal de webhook personalizado. Esta página fornece um exemplo de configuração de webhooks para o Slack.

Esta página se refere a instruções de terceiros, que estão sujeitas a alterações. Consulte a documentação do Slack para obter as informações mais atualizadas.

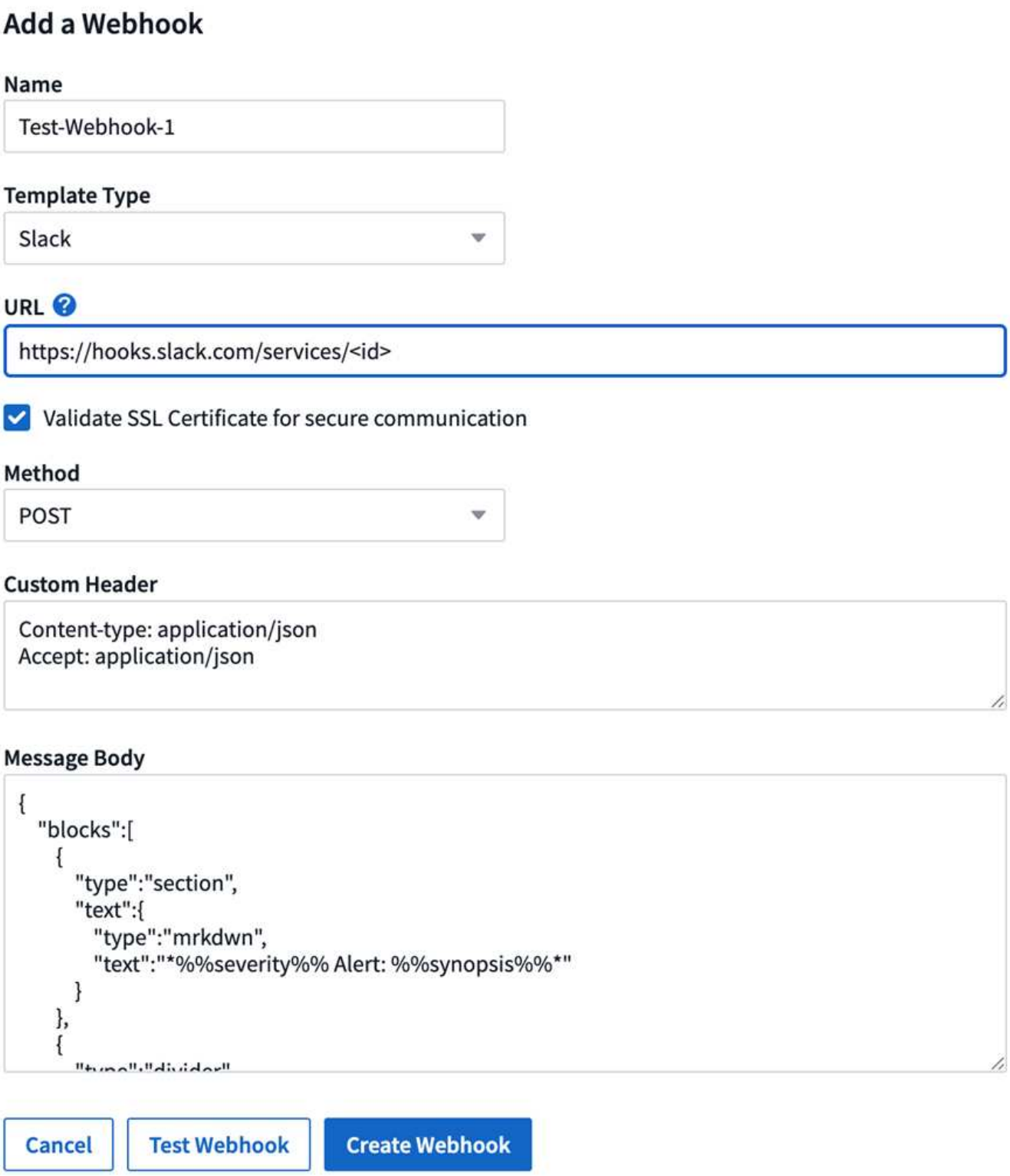
Exemplo de folga

- Vá para https://api.slack.com/apps e crie um novo aplicativo. Dê um nome significativo e selecione um espaço de trabalho.

- Vá para Webhooks de entrada, clique em *Ativar Webhooks de entrada*, selecione *Adicionar novo Webhook* e selecione o canal no qual deseja postar.
- Copie o URL do Webhook. Esta URL será fornecida ao criar um webhook de segurança de carga de trabalho.

Criar Webhook do Slack para Segurança de Carga de Trabalho

1. Navegue até Admin > Notificações e selecione a aba *Workload Security Webhooks*. Selecione + *Webhook* para criar um novo webhook.
2. Dê ao webhook um nome significativo.
3. No menu suspenso *Tipo de modelo*, selecione *Slack*.
4. Cole a URL copiada acima.

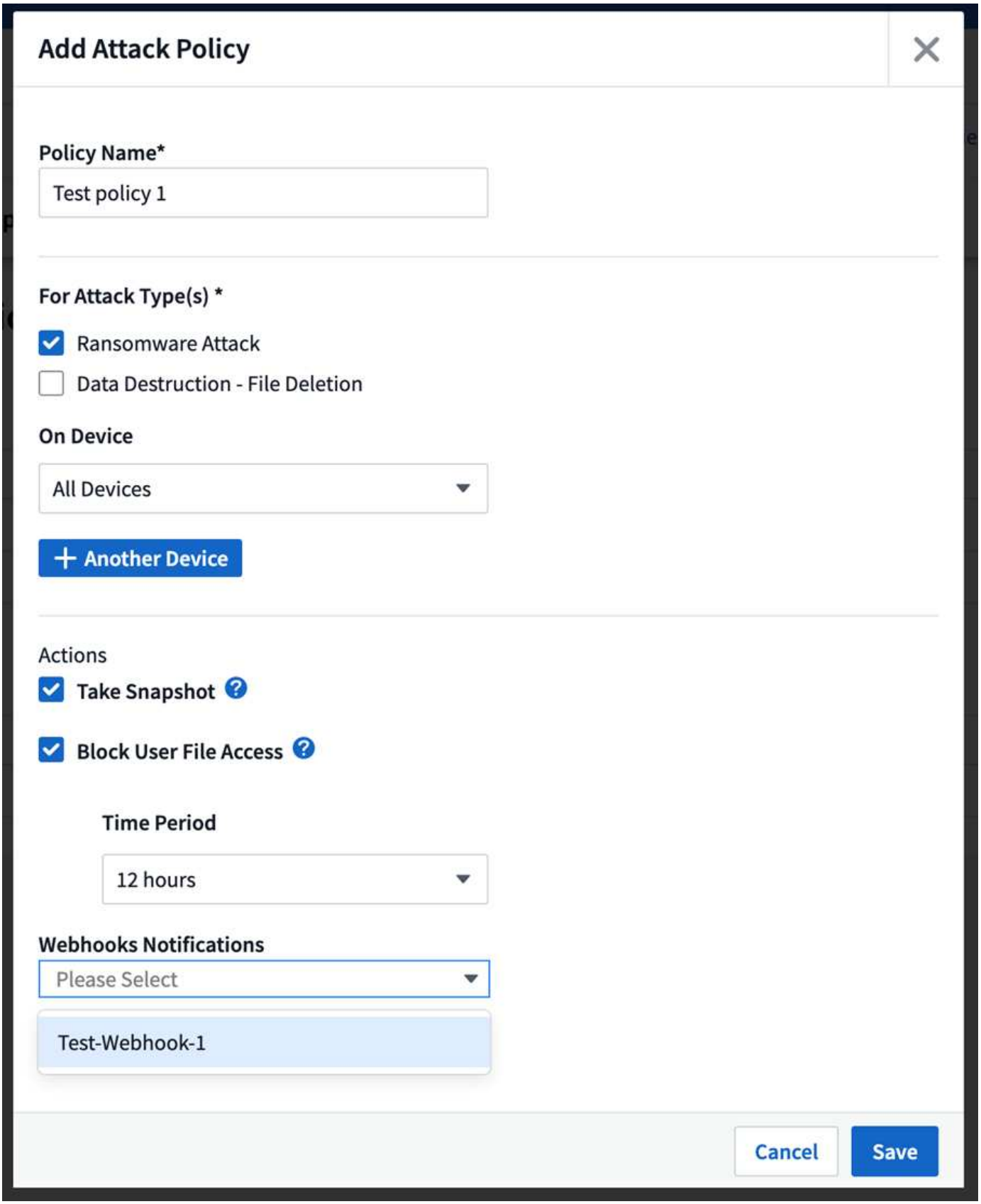


Notificações via webhook

- Para notificar eventos via webhook, navegue até *Segurança de carga de trabalho* > *Políticas*. Clique em *+Política de Ataque* ou *+Política de Aviso*.
- Insira um nome de política significativo.
- Selecione os tipos de ataque necessários, os dispositivos aos quais a política deve ser anexada e as ações necessárias.

- No menu suspenso *Notificações de webhooks*, selecione os webhooks necessários. Salve a política.

Observação: os webhooks também podem ser anexados às políticas existentes editando-as.



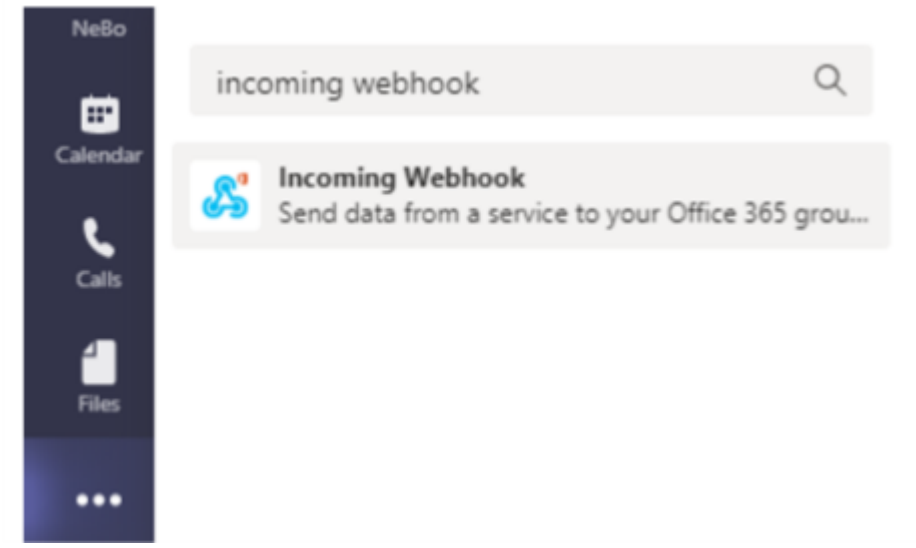
Exemplo de webhook de segurança de carga de trabalho para Microsoft Teams

Os webhooks permitem que os usuários enviem notificações de alerta para vários aplicativos usando um canal de webhook personalizado. Esta página fornece um exemplo de configuração de webhooks para o Teams.

Esta página se refere a instruções de terceiros, que estão sujeitas a alterações. Consulte o"Documentação das equipes" para obter as informações mais atualizadas.

Configuração das equipes:

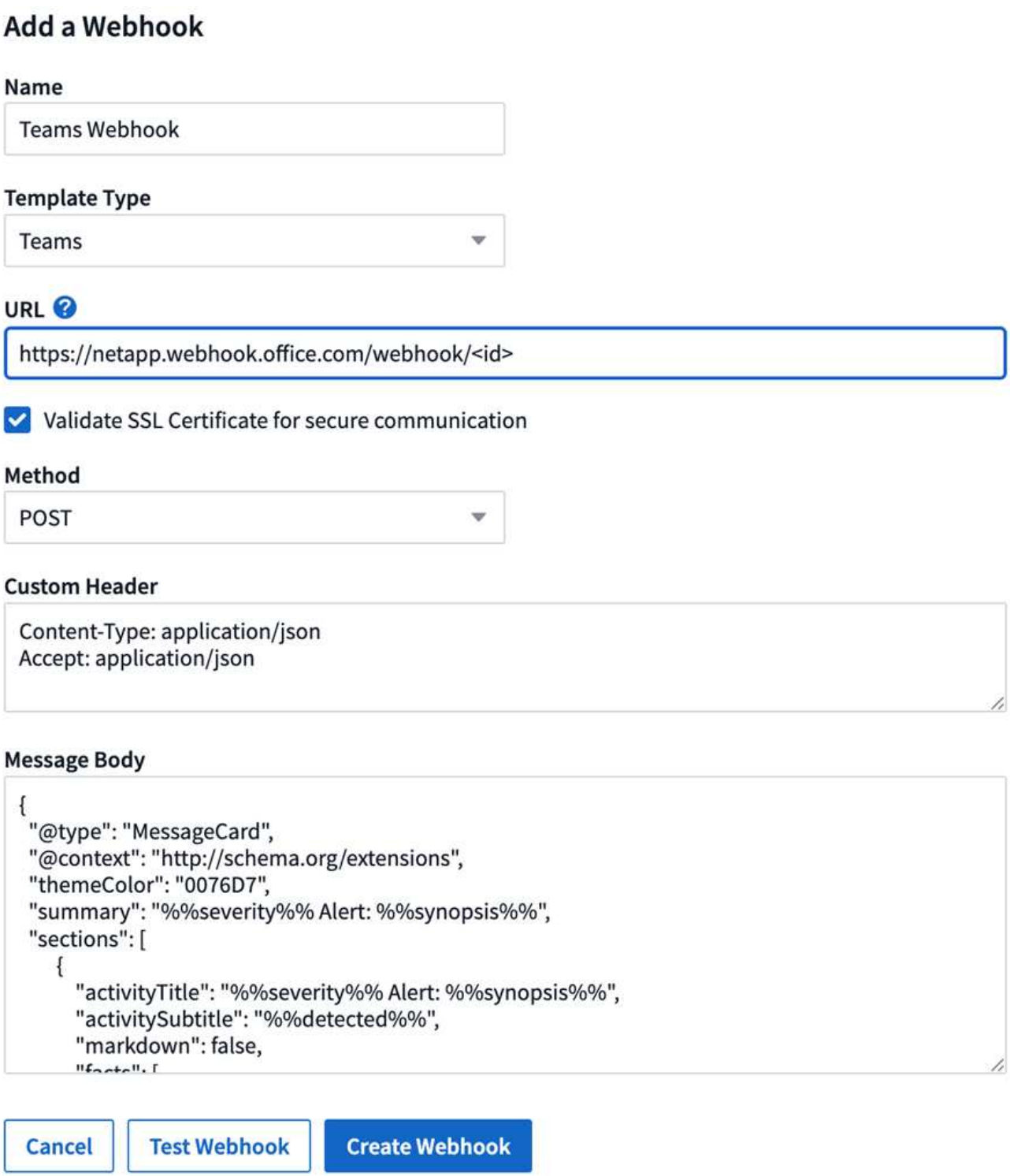
1. No Teams, selecione o kebab e pesquise por Webhook de entrada.



2. Selecione **Adicionar a uma equipe > Selecionar uma equipe > Configurar um conector**.
3. Copie o URL do Webhook. Você precisará colar isso na configuração do webhook do Workload Security.

Criar Webhook de Equipes de Segurança de Carga de Trabalho:

1. Navegue até Admin > Notificações e selecione a aba *"Workload Security Webhooks*. Selecione + *Webhook* para criar um novo webhook.
2. Dê ao webhook um nome significativo.
3. No menu suspenso *Tipo de modelo*, selecione **Equipes**.



4. Cole a URL acima no campo *URL*.

Passos para criar uma notificação do Teams com o modelo de Adaptive Card

1. Substitua o corpo da mensagem pelo seguinte modelo:

```
{
"type": "message",
"attachments": [
```

```
{
  "contentType": "application/vnd.microsoft.card.adaptive",
  "content": {
    "$schema": "http://adaptivecards.io/schemas/adaptive-card.json",
    "type": "AdaptiveCard",
    "version": "1.2",
    "body": [
      {
        "type": "TextBlock",
        "text": "%%severity%% Alert: %%synopsis%%",
        "wrap": true,
        "weight": "Bolder",
        "size": "Large"
      },
      {
        "type": "TextBlock",
        "text": "%%detected%%",
        "wrap": true,
        "isSubtle": true,
        "spacing": "Small"
      },
      {
        "type": "FactSet",
        "facts": [
          {
            "title": "User",
            "value": "%%userName%%"
          },
          {
            "title": "Attack/Abnormal Behavior",
            "value": "%%type%%"
          },
          {
            "title": "Action taken",
            "value": "%%actionTaken%%"
          },
          {
            "title": "Files encrypted",
            "value": "%%filesEncrypted%%"
          },
          {
            "title": "Encrypted files suffix",
            "value": "%%encryptedFilesSuffix%%"
          },
          {
            "title": "Files deleted",
```

```
                "value": "%%filesDeleted%%"
              },
              {
                "title": "Activity Change Rate",
                "value": "%%changePercentage%%"
              },
              {
                "title": "Severity",
                "value": "%%severity%%"
              },
              {
                "title": "Status",
                "value": "%%status%%"
              },
              {
                "title": "Notes",
                "value": "%%note%%"
              }
            ]
          }
        ],
        "actions": [
          {
            "type": "Action.OpenUrl",
            "title": "View Details",
            "url":
"https://%%cloudInsightsHostname%%/%%alertDetailsPageUrl%%"
          }
        ]
      }
    }
  ]
}
```

2. Se você estiver usando Power Automate Flows, os parâmetros de consulta na URL estarão em formato codificado. Você deve decodificar a URL antes de inserir.
3. Clique em "Test Webhook" para garantir que não haja erros.
4. Salve o webhook.

Notificações via Webhook

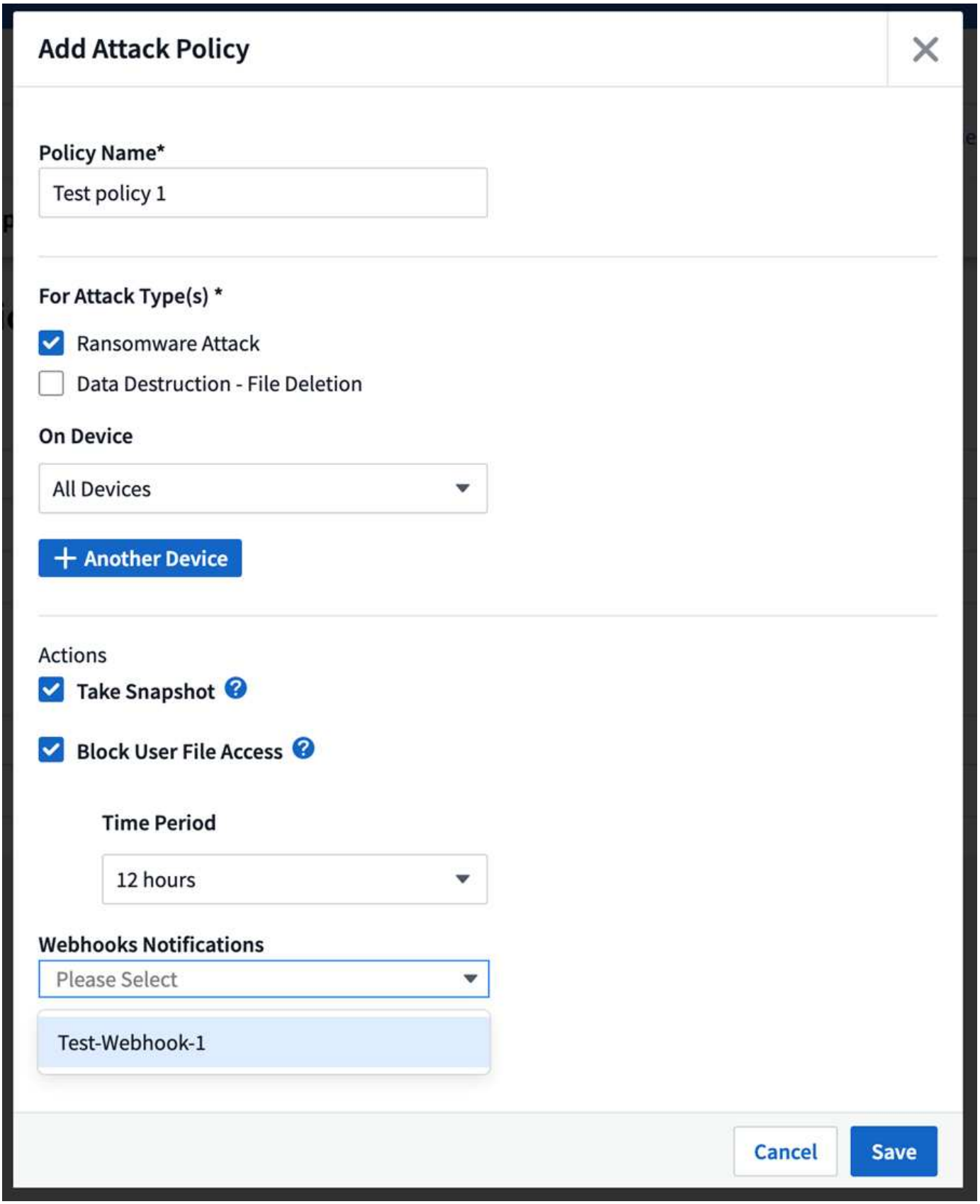
Para notificar eventos via webhook, navegue até *Segurança de carga de trabalho* > *Políticas*. Selecione *+Política de Ataque* ou *+Política de Aviso*.

- Insira um nome de política significativo.
- Selecione os tipos de ataque necessários, os dispositivos aos quais a política deve ser anexada e as

ações necessárias.

- No menu suspenso *Notificações de Webhooks*, selecione os webhooks do Teams necessários. Salve a política.

Observação: os webhooks também podem ser anexados às políticas existentes editando-as.



API de segurança de carga de trabalho

Integre Workload Security ao seu ecossistema empresarial usando uma API REST

protegida por autenticação segura baseada em token. Recupere dados de atividades forenses, gerencie tokens de acesso à API e desenvolva integrações personalizadas com CMDBs, sistemas de ticket e outros aplicativos. A documentação interativa do Swagger fornece especificações completas da API e permite que você teste os endpoints diretamente.

Requisitos para acesso à API:

- Um modelo de token de acesso de API é usado para conceder acesso.
- O gerenciamento do token de API é realizado por usuários do Workload Security com a função de administrador.

Documentação da API (Swagger)

As informações mais recentes da API podem ser encontradas fazendo login no Workload Security e navegando até **Admin > Acesso à API**. Clique no link **Documentação da API**. A documentação da API é baseada no Swagger, que fornece uma breve descrição e informações de uso da API e permite que você a experimente em seu locatário.

Se estiver chamando a API de atividade forense, use a API cloudsecure_forensics.activities.**v2**. Se você estiver fazendo várias chamadas para esta API, certifique-se de que as chamadas ocorram sequencialmente, não em paralelo. Várias chamadas paralelas podem causar tempo limite na API.

Tokens de acesso à API

Antes de usar a API de segurança de carga de trabalho, você deve criar um ou mais **Tokens de acesso à API**. Os tokens de acesso concedem permissões de leitura. Você também pode definir a expiração de cada token de acesso.

Para criar um Token de Acesso:

- Clique em **Admin > Acesso à API**
- Clique em **+Token de acesso à API**
- Digite **Nome do Token**
- Especifique **Expiração do Token**

Seu token só estará disponível para ser copiado para a área de transferência e salvo durante o processo de criação. Os tokens não podem ser recuperados depois de criados, por isso é altamente recomendável copiar o token e salvá-lo em um local seguro. Você será solicitado a clicar no botão Copiar token de acesso à API antes de fechar a tela de criação do token.

Você pode desabilitar, habilitar e revogar tokens. Tokens que estão desabilitados podem ser habilitados.

Os tokens concedem acesso de propósito geral às APIs da perspectiva do cliente, gerenciando o acesso às APIs no escopo de seu próprio locatário.

O aplicativo recebe um Token de Acesso depois que um usuário autentica e autoriza o acesso com sucesso e, em seguida, passa o Token de Acesso como uma credencial quando chama a API de destino. O token passado informa à API que o portador do token foi autorizado a acessar a API e executar ações específicas

com base no escopo concedido durante a autorização.

O cabeçalho HTTP onde o token de acesso é passado é **X-CloudInsights-ApiKey:**

Por exemplo, use o seguinte para recuperar ativos de armazenamento:

```
 curl https://<Workload Security tenant>/rest/v1/cloudsecure/activities -H
'X-CloudInsights-ApiKey: <API_Access_Token>'
Onde _<API_Access_Token>_ é o token que você salvou durante a criação da
chave de acesso à API e _<Workload Security Tenant>_ é a URL do locatário
do seu ambiente de Workload Security.
```

Informações detalhadas podem ser encontradas no link *Documentação da API* em **Administrador > Acesso à API**.

Script para extrair dados via API

Os agentes de segurança de carga de trabalho incluem um script de exportação para facilitar chamadas paralelas à API v2, dividindo o intervalo de tempo solicitado em lotes menores.

O script está localizado em */opt/netapp/cloudsecure/agent/export-script*. Um arquivo README no mesmo diretório fornece instruções de uso.

Aqui está um exemplo de comando para invocar o script:

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

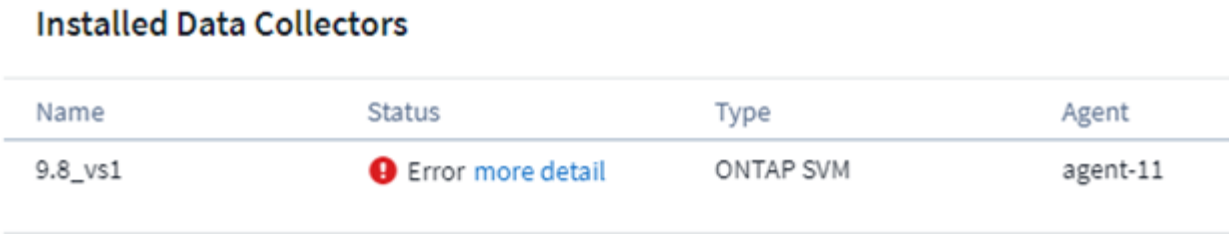
Parâmetros principais: - `--iteration_interval 12` : Divide o intervalo de tempo solicitado em intervalos de 12 horas. - `--num_workers 3` : Busca esses intervalos em paralelo usando 3 threads.

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**.

Informações sobre direitos autorais

Informações sobre marcas comerciais