# Segurança da carga de trabalho

## Data Infrastructure Insights

NetApp
January 10, 2025

# Índice

# Segurança da carga de trabalho

## Sobre o Storage Workload Security

A segurança de workload de storage (anteriormente Cloud Secure) ajuda a proteger seus dados com inteligência acionável sobre ameaças internas. Ele fornece visibilidade e controle centralizados de todos os acessos a dados corporativos em ambientes de nuvem híbrida para garantir que as metas de segurança e conformidade sejam atingidas.

### Visibilidade

Obtenha visibilidade centralizada e controle do acesso do usuário aos dados corporativos essenciais armazenados no local ou na nuvem.

Substitua as ferramentas e os processos manuais que não fornecem visibilidade atempada e precisa do acesso e controlo dos dados. O Workload Security opera exclusivamente em sistemas de storage na nuvem e no local para fornecer alertas em tempo real de comportamento mal-intencionado do usuário.

### Proteção

Proteja os dados organizacionais contra a utilização indevida por parte de usuários mal-intencionados ou comprometidos por meio do aprendizado de máquina avançado e da detecção de anomalias.

Alerta você para acesso anormal aos dados por meio do aprendizado de máquina avançado e da detecção de anomalias de comportamento do usuário.

### Conformidade

Garanta a conformidade empresarial auditando o acesso aos dados dos usuários aos dados corporativos essenciais armazenados no local ou na nuvem.

# Como começar

### Introdução ao Workload Security

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

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

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

| Tarefa | Informações relacionadas |
| --- | --- |

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

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

## Requisitos do Agente de Segurança de carga de trabalho

Você deve"Instale um agente", a fim de adquirir informações de seus coletores de dados. Antes de instalar o agente, você deve garantir que seu ambiente atenda aos requisitos do sistema operacional, CPU, memória e espaço em disco.

| Componente | Requisito Linux |
|---|---|
| Sistema operacional | Um computador executando uma versão licenciada de um dos seguintes: * CentOS 64 64 64 24,04 11 9,4 Stream (9,2 15 SP3 20,04 64 64 64-bit), CentOS 9 9,4 15 SP5 22,04 10 9,3 Stream, SELinux * OpenSUSE Leap 8,8 a 15,5 (64-bit) * Oracle Linux 8,6 - 64, 9,1 a 9,4 (8,8-bit) * Red Hat Enterprise Linux 8,6 a 15,3, 9,1 a 9,4 (8-bit), SELinux * Rocky 64 Recomenda-se um servidor dedicado. |
| 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 | Requisito Linux |
|---|---|
| Espaço disponível em disco | O espaço em disco deve ser alocado desta maneira: /Opt/NetApp 36 GB (mínimo de 35 GB de espaço livre após a criação do sistema de arquivos) Nota: Recomenda-se alocar um pouco de espaço em disco extra para permitir a criação do sistema de arquivos. Certifique-se de que haja pelo menos 35 GB de espaço livre no sistema de arquivos. Se /opt for uma pasta montada a partir de um armazenamento nas, certifique-se de que os utilizadores locais têm acesso a esta pasta. O Agent ou Data Collector pode falhar na instalação se os usuários locais não tiverem permissão para essa pasta. Consulte "solução de problemas"a seção para obter mais detalhes. |
| Rede | Conexão Ethernet de 100 Mbps a 1 Gbps, endereço IP estático, conetividade IP a todos os dispositivos e uma porta necessária para a instância de segurança de carga de trabalho (80 ou 443). |

Observação: O agente Workload Security pode ser instalado na mesma máquina que uma unidade de aquisição e/ou agente do Data Infrastructure Insights. No entanto, é uma prática recomendada instalá-los em máquinas separadas. No caso de estes estarem instalados na mesma máquina, atribua espaço em disco, conforme ilustrado abaixo:

| | |
|---|---|
| Espaço disponível em disco | 50-55 GB para Linux, o espaço em disco deve ser alocado desta maneira: /Opt/NetApp 25-30 GB /var/log/NetApp 25 GB |

**Recomendações adicionais**

- É altamente recomendável sincronizar a hora no sistema ONTAP e na máquina do agente usando **Protocolo de tempo de rede (NTP)** ou **Protocolo de tempo de rede simples (SNTP)**.

**Regras de acesso à rede na nuvem**

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

| Protocolo | Porta | Fonte | Destino | Descrição |
|---|---|---|---|---|
| TCP | 443 | Agente de segurança de carga de trabalho | <site_name>.cs01.cloudinsights.NetApp.com <site_name>.c01.cloudinsights.NetApp.com <site_name>.c02.cloudinsights.NetApp.com | Acesso ao Data Infrastructure Insights |
| TCP | 443 | Agente de segurança de carga de trabalho | gateway.c01.cloudinsights.netapp.com agentlogin.cs01.cloudinsights.netapp.com | Acesso aos serviços de autenticação |

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

| Protocolo | Porta | Fonte | Destino | Descrição |
|---|---|---|---|---|
| TCP | 443 | Agente de segurança de carga de trabalho | <site_name>.cs01-eu-1.cloudinsights.NetApp.com <site_name>.c01-eu-1.cloudinsights.NetApp.com <site_name>.c02-eu-1.cloudinsights.NetApp.com | Acesso ao Data Infrastructure Insights |
| TCP | 443 | Agente de segurança de carga de trabalho | gateway.c01.cloudinsights.NetApp.com agentlogin.cs01-eu-1.cloudinsights.NetApp.com | Acesso aos serviços de autenticação |

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

| Protocolo | Porta | Fonte | Destino | Descrição |
|---|---|---|---|---|
| TCP | 443 | Agente de segurança de carga de trabalho | <site_name>.cs01-ap-1.cloudinsights.NetApp.com <site_name>.c01-ap-1.cloudinsights.NetApp.com <site_name>.c02-ap-1.cloudinsights.NetApp.com | Acesso ao Data Infrastructure Insights |
| TCP | 443 | Agente de segurança de carga de trabalho | gateway.c01.cloudinsights.NetApp.com agentlogin.cs01-ap-1.cloudinsights.NetApp.com | Acesso aos serviços de autenticação |

**Regras na rede**

| Protocolo | Porta | Fonte | Destino | Descrição |
|---|---|---|---|---|
| TCP | 389 (LDAP) 636 (LDAPS/start-tls) | Agente de segurança de carga de trabalho | URL do servidor LDAP | Ligar ao LDAP |

| Protocolo | Porta | Fonte | Destino | Descrição |
|---|---|---|---|---|
| TCP | 443 | Agente de segurança de carga de trabalho | Endereço IP do gerenciamento do cluster ou SVM (dependendo da configuração do coletor do SVM) | Comunicação de API com o ONTAP |
| TCP | 35000 - 55000 | Endereços IP de LIF de dados SVM | Agente de segurança de carga de trabalho | Comunicação do ONTAP para o agente de segurança de carga de trabalho para eventos Fpolicy. Essas portas devem ser abertas para o Agente de Segurança de carga de trabalho para que o ONTAP envie eventos para ele, incluindo qualquer firewall no próprio Agente de Segurança de carga de trabalho (se presente). OBSERVE que você não precisa reservar **todos** dessas portas, mas as portas que você reserva para isso devem estar dentro desse intervalo. Recomenda-se começar reservando cerca de 100 portas e aumentando, se necessário. |
| TCP | 7 | Agente de segurança de carga de trabalho | Endereços IP de LIF de dados SVM | ECHO de LIFs de dados de agente para SVM |
| SSH | 22 | Agente de segurança de carga de trabalho | Gerenciamento de clusters | Necessário para bloqueio de usuários CIFS/SMB. |

**Dimensionamento do sistema**

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

## Instalação do Agente de Segurança de carga de trabalho

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

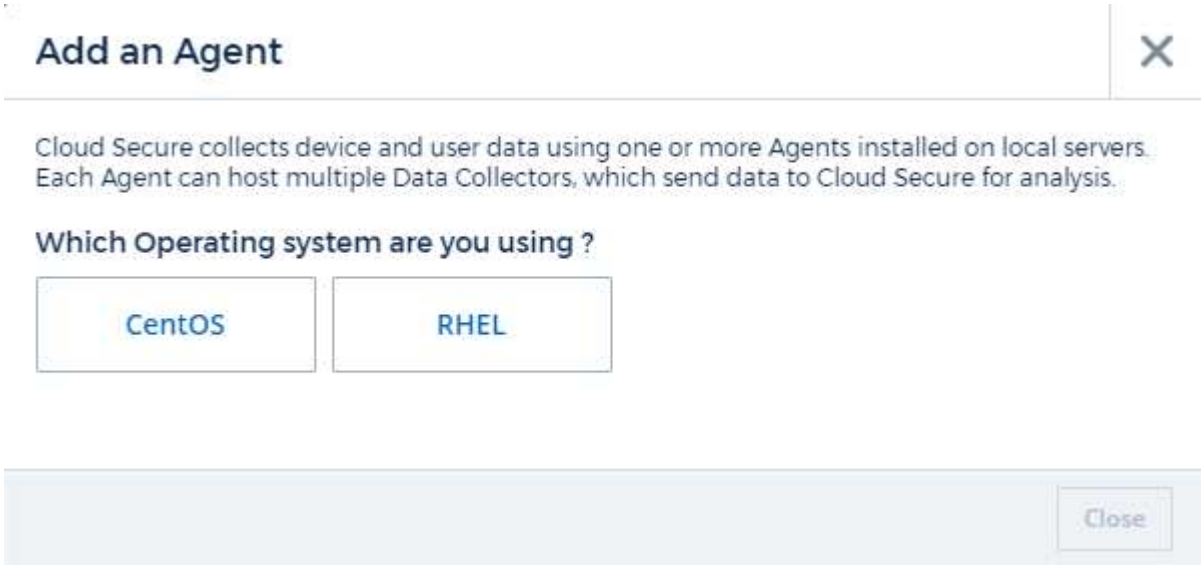
### Antes de começar

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

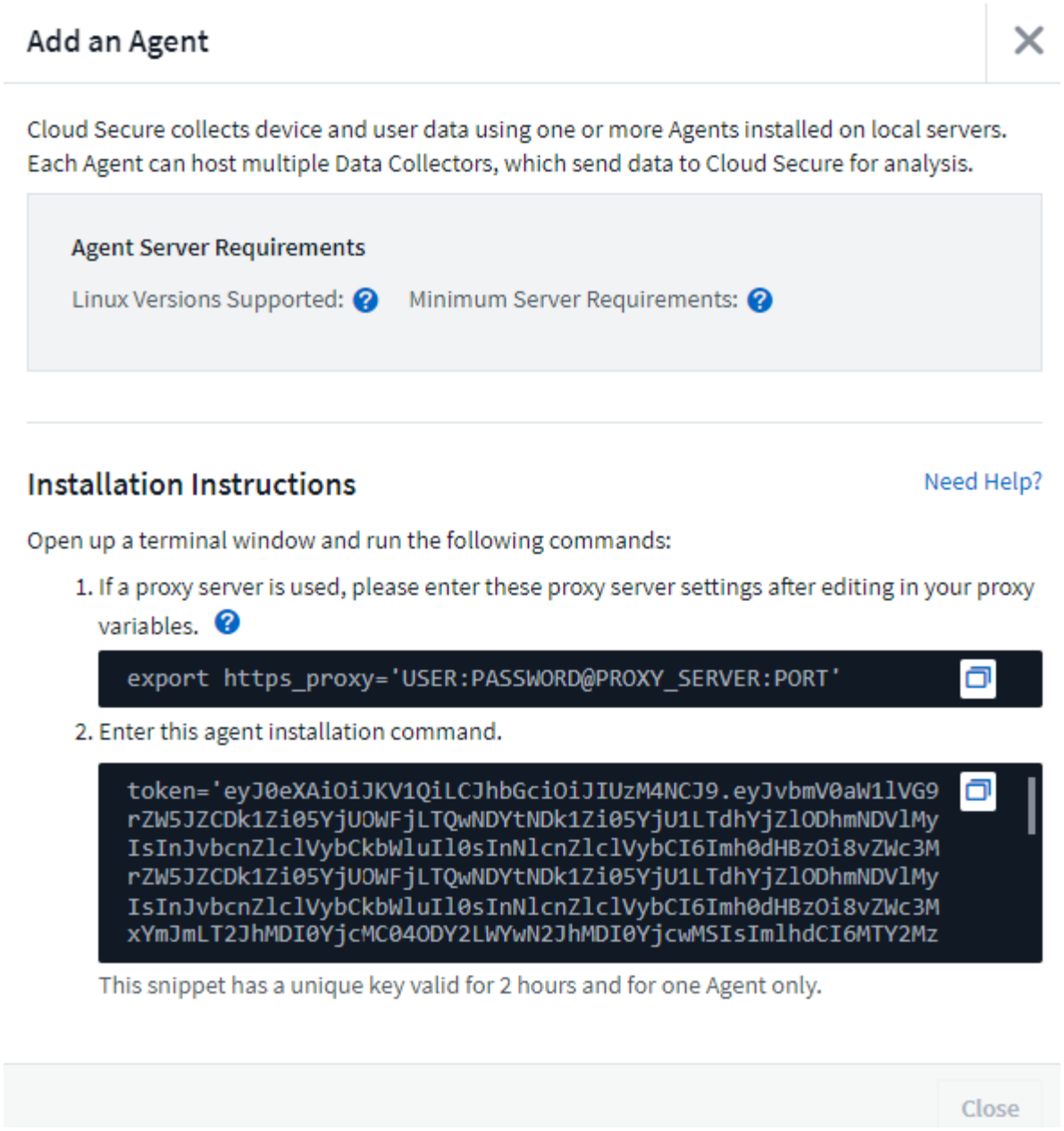
### Etapas para instalar o agente

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

   O sistema exibe a página Adicionar um agente:




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




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


**Depois de concluir**

1. É necessário configurar um "Coletor de diretório de usuários".
2. Você precisa configurar um ou mais coletores de dados.

**Configuração de rede**

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

**Passos**

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

Siga os próximos passos de acordo com a sua plataforma:

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

Saída da amostra:

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

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

Saída da amostra:

```
35000-55000/tcp
```

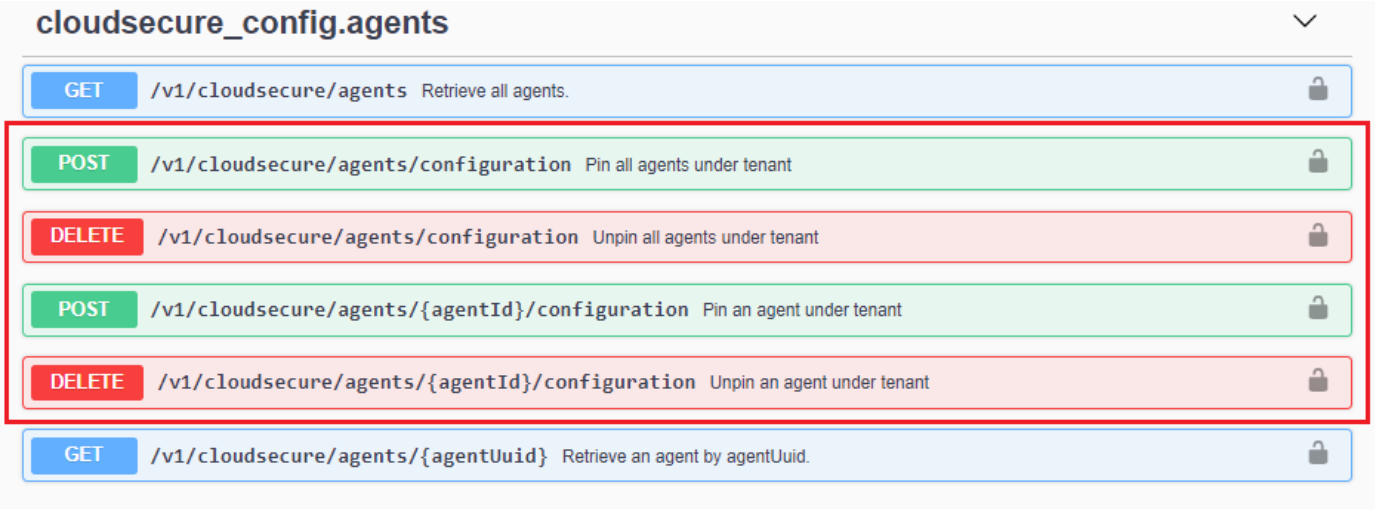
**"Fixar" um agente na versão atual**

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

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

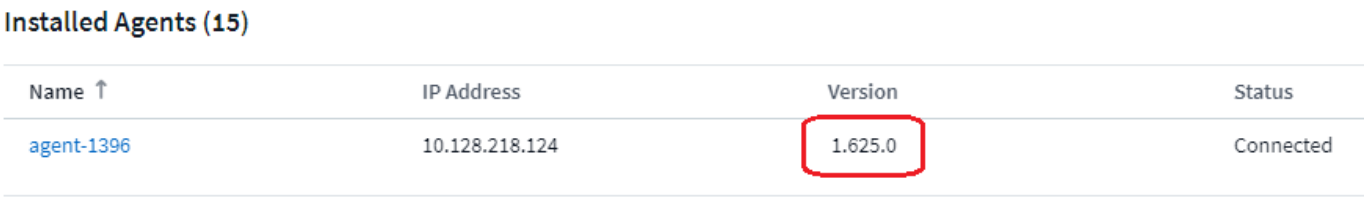
Em cada um desses casos, o agente será atualizado na próxima atualização de Segurança de carga de trabalho.

Para pausar ou retomar atualizações automáticas de agentes, use as APIs *cloudsecure_config.agents*:




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

Você pode exibir suas versões atuais do Agente na página **Segurança de carga de trabalho > coletores**, na guia **agentes**.




### Solução de problemas de erros do agente

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

| Problema: | Resolução: |
| --- | --- |
| A instalação do agente falha ao criar a pasta /opt/NetApp/cloudsecure/Agent/logs/agent.log e o arquivo install.log não fornece informações relevantes. | Esse erro ocorre durante o bootstrapping do agente. O erro não é registrado em arquivos de log porque ocorre antes que o logger seja inicializado. O erro é redirecionado para a saída padrão e é visível no log de serviço usando o `journalctl -u cloudsecure-agent.service` comando. Este comando pode ser usado para solucionar o problema ainda mais. est |
| A instalação do agente falha com 'esta distribuição linux não é suportada. Sair da instalação'. | Esse erro aparece quando você tenta instalar o Agente em um sistema não suportado. "Requisitos do agente"Consulte . |
| Falha na instalação do agente com o erro: "-bash: Unzip: Comando not found" | Instale o descompacte e execute o comando de instalação novamente. Se o Yum estiver instalado na máquina, tente "yum install unzip" para instalar o software deszip. Depois disso, copie novamente o comando da IU de instalação do agente e cole-o na CLI para executar a instalação novamente. |

| Problema: | Resolução: |
| --- | --- |
| O agente foi instalado e estava em execução. No entanto, o agente parou de repente. | SSH para a máquina Agent. Verifique o status do serviço do agente através `sudo systemctl status cloudsecure-agent.service`do . 1. Verifique se os logs mostram uma mensagem "Falha ao iniciar o serviço daemon de Segurança do Workload" . 2. Verifique se o usuário cssys existe ou não na máquina Agente. Execute os seguintes comandos um por um com permissão root e verifique se o usuário e o grupo cssys existem. `sudo id cssys` `sudo groups cssys` 3. Se nenhuma existir, uma política de monitorização centralizada pode ter eliminado o utilizador cssys. 4. Crie o usuário e o grupo cssys manualmente executando os seguintes comandos. `sudo useradd cssys` `sudo groupadd cssys` 5. Reinicie o serviço do agente depois disso executando o seguinte comando: `sudo systemctl restart cloudsecure-agent.service` 6. Se ainda não estiver em execução, verifique as outras opções de resolução de problemas. |
| Não é possível adicionar mais de 50 coletores de dados a um agente. | Apenas 50 coletores de dados podem ser adicionados a um Agente. Isso pode ser uma combinação de todos os tipos de coletor, por exemplo, ative Directory, SVM e outros coletores. |
| A IU mostra que o Agente está no estado NÃO LIGADO. | Etapas para reiniciar o Agente. 1. SSH para a máquina Agent. 2. Reinicie o serviço do agente depois disso executando o seguinte comando: `sudo systemctl restart cloudsecure-agent.service` 3. Verifique o status do serviço do agente através `sudo systemctl status cloudsecure-agent.service`do . 4. O agente deve ir para o estado CONETADO. |
| A VM do agente está atrás do proxy Zscaler e a instalação do agente está falhando. Devido à inspeção SSL do proxy Zscaler, os certificados de Segurança da carga de trabalho são apresentados à medida que são assinados pela Zscaler CA para que o agente não confie na comunicação. | Desative a inspeção SSL no proxy Zscaler para o url *.cloudinsights.NetApp.com. Se o Zscaler fizer a inspeção SSL e substituir os certificados, o Workload Security não funcionará. |

| Problema: | Resolução: |
| --- | --- |
| Durante a instalação do agente, a instalação trava após o desbloqueio. | O comando "chmod 755 -RF" está falhando. O comando falha quando o comando de instalação do agente está sendo executado por um usuário sudo não-root que tem arquivos no diretório de trabalho, pertencentes a outro usuário, e as permissões desses arquivos não podem ser alteradas. Devido ao comando chmod com falha, o resto da instalação não é executado. 1. Crie um novo diretório chamado "cloudsecure". 2. Vá para esse diretório. 3. Copie e cole o comando completo de instalação "token……" e pressione ENTER. 4. A instalação deve ser capaz de prosseguir. |
| Se o agente ainda não conseguir se conetar ao SaaS, abra um caso com o suporte da NetApp. Forneça o número de série do Data Infrastructure Insights para abrir um caso e anexe logs ao caso, conforme observado. | Para anexar logs ao caso: 1. Execute o seguinte script com permissão root e compartilhe o arquivo de saída (cloudsecure-Agent-sympats.zip). A. /opt/NetApp/cloudsecure/Agent/bin/cloudsecure-agent-symptom-collector.sh 2. Execute os seguintes comandos um a um com permissão root e compartilhe a saída. a. id cssys b. Groups cssys c. Cat /etc/os-release |
| O script cloudsecure-agent-symptom-collector.sh falha com o seguinte erro. /Opt/NetApp/cloudsecure/Agent/bin/cloudsecure-agent-symptom-collector.sh coletando log de serviço coletando logs de aplicativos coletando configurações de agentes tomando snapshot de status de serviço tomando snapshot da estrutura de diretórios de agentes…… …… /Opt/NetApp/cloudsecure/Agent/bin/cloudsecure-Agent-sintoma-Collector.sh: Linha 52: Zip: ERRO de comando não encontrado: Falha ao criar /tmp/cloudsecure-agent-symptoms.zip | A ferramenta zip não está instalada. Instale a ferramenta zip executando o comando "yum install zip". Em seguida, execute o cloudsecure-agent-symptom-collector.sh novamente. |
| Falha na instalação do agente com useradd: Não é possível criar diretório /home/cssys | Esse erro pode ocorrer se o diretório de login do usuário não puder ser criado em /home, devido à falta de permissões. A solução alternativa seria criar o usuário cssys e adicionar seu diretório de login manualmente usando o seguinte comando: *Sudo useradd user_name -m -d home_DIR* -m :criar o diretório home do usuário se ele não existir. -D : o novo usuário é criado usando home_DIR como o valor para o diretório de login do usuário. Por exemplo, *sudo useradd cssys -m -d /cssys*, adiciona um usuário *cssys* e cria seu diretório de login sob root. |

| Problema: | Resolução: |
| --- | --- |
| O agente não está em execução após a instalação. *Systemctl status cloudsecure-agent.service* NetApp 25889 12:26 126 1 mostra o seguinte: [Root at demo] no. Systemctl status cloudsecure-agent.service agent.service 25889 126 1 03 21 cloudsecure-agent.service – Workload Agente de Segurança Serviço Daemon carregado: Carregado (/usr/lib/systemd/system/cloudsecure-agent.service; 126 03 21 cloudsecure-agent.service: 12:26 ativado; predefinição do fornecedor: Desativado) Ativo: Ativando (auto-restart) (resultado: Exit-code) desde Tue 2s-08-03 21:12:26 PDT; 2021 Aug 03 21:12:26 demo systemd[1]: cloudsecure-agent.service falhou. | Isso pode estar falhando porque o usuário *cssys* pode não ter permissão para instalar. Se /opt/NetApp for uma montagem NFS e se o usuário *cssys* não tiver acesso a essa pasta, a instalação falhará. *Cssys* é um usuário local criado pelo instalador do Workload Security que pode não ter permissão para acessar o compartilhamento montado. Você pode verificar isso tentando acessar /opt/NetApp/cloudsecure/Agent/bin/cloudsecure-Agent usando *cssys* usuário. Se retornar "permissão negada", a permissão de instalação não está presente. Em vez de uma pasta montada, instale em um diretório local para a máquina. |
| O agente foi inicialmente conetado através de um servidor proxy e o proxy foi definido durante a instalação do Agente. Agora, o servidor proxy mudou. Como a configuração do proxy do Agente pode ser alterada? | Você pode editar o agent.properties para adicionar os detalhes do proxy. Siga estes passos: 1. Mude para a pasta que contém o arquivo de propriedades: cd /opt/NetApp/cloudsecure/conf 2. Usando seu editor de texto favorito, abra o arquivo *agent.properties* para edição. 3. Adicione ou modifique as seguintes linhas: AGENT_PROXY_HOST scspa1950329001.vm.NetApp.com AGENT_PROXY_PORT 80 AGENT_PROXY_USER pass1234 4. Salve o arquivo. 5. Reinicie o agente: Sudo systemctl restart cloudsecure-agent.service |

## Excluindo um agente de segurança de carga de trabalho

Quando você exclui um agente de segurança de carga de trabalho, todos os coletores de dados associados ao agente devem ser excluídos primeiro.

### Excluindo um agente

A exclusão de um agente exclui todos os coletores de dados associados ao agente. Se você pretende configurar os coletores de dados com um agente diferente, você deve criar um backup das configurações do Data Collector antes de excluir o Agente.

**Antes de começar**

1. Certifique-se de que todos os coletores de dados associados ao agente sejam excluídos do portal Workload Security.

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

**Etapas para excluir um agente:**

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

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

2. Clique em **Workload Security > Collectors > Agents**

   O sistema exibe a lista de agentes configurados.

3. Clique no menu de opções para o agente que você está excluindo.
4. Clique em **Excluir**.

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

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

## Configurando um Coletor de diretório de usuários do ative Directory (AD)

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

**Antes de começar**

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

**Passos para configurar um Coletor de diretório de usuários**

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

   O sistema exibe a tela Adicionar diretório do usuário.

Configure o Coletor de diretório de usuários inserindo os dados necessários nas seguintes tabelas:

| Nome | Descrição |
|---|---|
| Nome | Nome exclusivo para o diretório do usuário. Por exemplo *GlobalADCollector* |
| Agente | Selecione um agente configurado na lista |
| Nome de domínio/IP do servidor | Endereço IP ou nome de domínio totalmente qualificado (FQDN) do servidor que hospeda o diretório ativo |
| Nome da floresta | Nível de floresta da estrutura do diretório. O nome da floresta permite ambos os seguintes formatos: *X.y.z*> nome de domínio direto como você o tem no SVM. [Exemplo: hq.companyname.com]_DC,DC_DC_com] ou você pode especificar como o seguinte: _Ou NetApp <username> <engineering> |

| | |
|---|---|
| Vincular DN | Usuário autorizado a pesquisar o diretório. Por exemplo: *username@companyname.com* ou *username@domainname.com* além disso, a permissão de domínio somente leitura é necessária. O usuário deve ser um membro do grupo Segurança *Controladores de domínio somente leitura*. |
| Palavra-passe BIND | Senha do servidor de diretório (ou seja, senha para nome de usuário usado no DN de vinculação) |
| Protocolo | ldap, ldaps, ldap-start-tls |
| Portas | Selecione a porta |

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

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

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

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

**Testando a configuração do coletor do diretório de usuários**

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

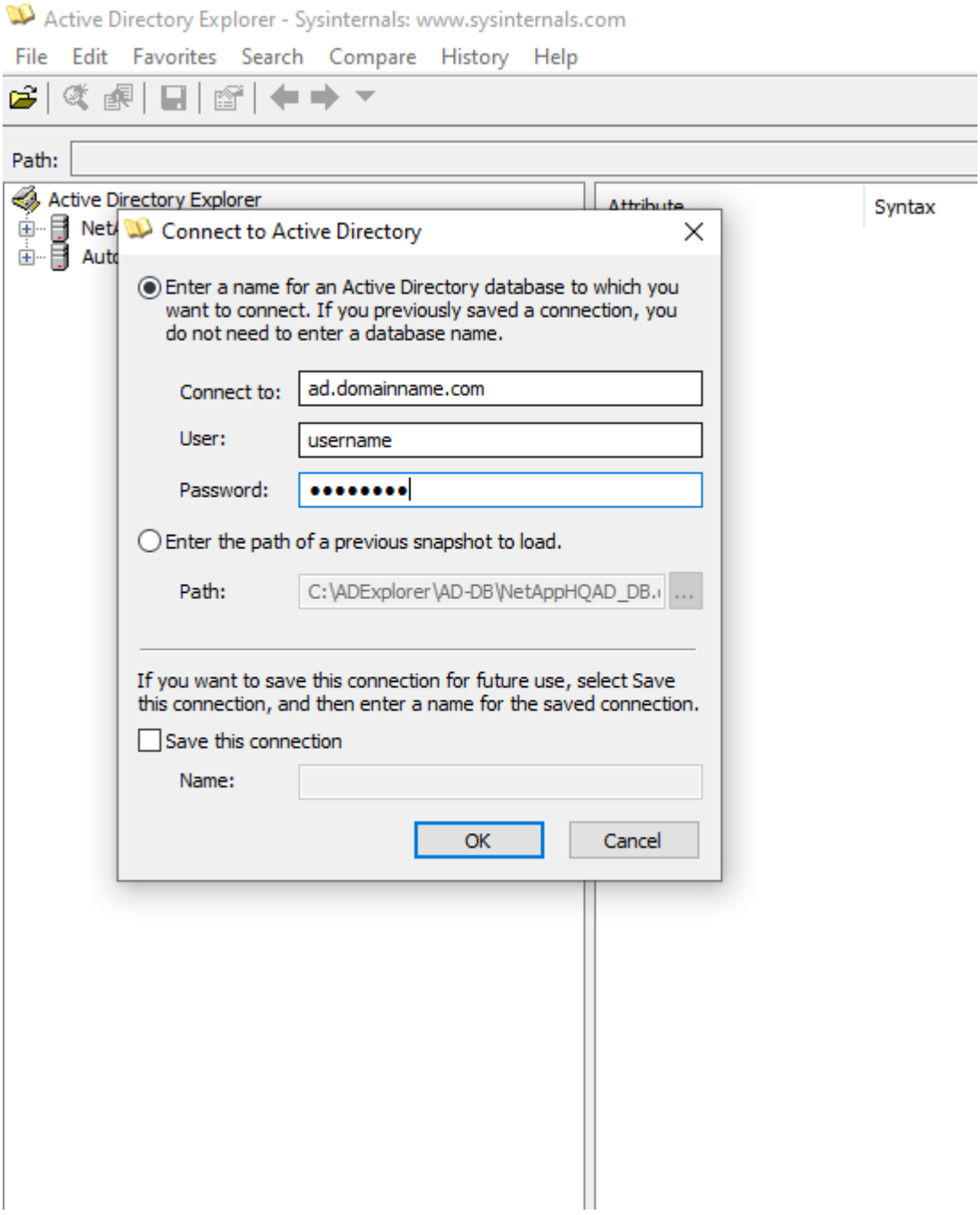
- Use o seguinte comando para validar a permissão de usuário LDAP de segurança de workload:

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

- Use o AD Explorer para navegar em um banco de dados do AD, exibir propriedades e atributos de objetos, exibir permissões, exibir o esquema de um objeto, executar pesquisas sofisticadas que você pode

salvar e executar novamente.

- Instale "Explorador de ANÚNCIOS" em qualquer máquina Windows que possa se conetar ao servidor AD.
- Conete-se ao servidor AD usando o nome de usuário/senha do servidor de diretório AD.




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

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

| Problema: | Resolução: |
| --- | --- |
| Adicionar um conetor do diretório de usuários resulta no estado "erro". O erro diz: "Credenciais inválidas fornecidas para o servidor LDAP". | Nome de utilizador ou palavra-passe incorretos fornecidos. Edite e forneça o nome de usuário e a senha corretos. |
| Adicionar um conetor do diretório de usuários resulta no estado "erro". Erro diz: "Falha ao obter o objeto correspondente a DN | Nome da floresta incorreto fornecido. Edite e forneça o nome correto da floresta. |
| Os atributos opcionais do usuário de domínio não estão aparecendo na página Perfil de usuário de Segurança de carga de trabalho. | Isso provavelmente se deve a uma incompatibilidade entre os nomes de atributos opcionais adicionados no CloudSecure e os nomes de atributos reais no ative Directory. Edite e forneça o(s) nome(s) do atributo opcional correto(s). |
| Coletor de dados no estado de erro com "Falha ao recuperar usuários LDAP. Motivo da falha: Não é possível conetar no servidor, a conexão é nula" | Reinicie o coletor clicando no botão *Restart*. |
| Adicionar um conetor do diretório de usuários resulta no estado "erro". | Certifique-se de que forneceu valores válidos para os campos obrigatórios (servidor, nome da floresta, bind-DN, bind-Password). Certifique-se de que a entrada BIND-DN é sempre fornecida como "Administrador <domain_forest_name>" ou como uma conta de usuário com Privileges de administrador de domínio. |
| Adicionar um conetor do diretório de usuários resulta no estado "TENTAR NOVAMENTE". Mostra o erro "não é possível definir o estado do comando Collector,Reason TCP [Connect(localhost:35012,None,List(),some(,seconds),true)] falhou por causa de java.net.ConnectionException:Connection recusado." | IP ou FQDN incorreto fornecido para o servidor AD. Edite e forneça o endereço IP ou FQDN correto. |
| Adicionar um conetor do diretório de usuários resulta no estado "erro". O erro diz: "Falha ao estabelecer a conexão LDAP". | IP ou FQDN incorreto fornecido para o servidor AD. Edite e forneça o endereço IP ou FQDN correto. |
| Adicionar um conetor do diretório de usuários resulta no estado "erro". O erro diz: "Falha ao carregar as configurações. Motivo: A configuração da fonte de dados tem um erro. Razão específica: /Connector/conf/application.conf: 70: LDAP.ldap-port tem STRING de tipo em vez DE NÚMERO" | Valor incorreto para a porta fornecida. Tente usar os valores de porta padrão ou o número de porta correto para o servidor AD. |
| Comecei com os atributos obrigatórios, e funcionou. Depois de adicionar os opcionais, os dados de atributos opcionais não são obtidos do AD. | Isso provavelmente se deve a uma incompatibilidade entre os atributos opcionais adicionados no CloudSecure e os nomes de atributos reais no ative Directory. Edite e forneça o nome do atributo obrigatório ou opcional correto. |
| Depois de reiniciar o coletor, quando acontecerá a sincronização AD? | A sincronização DE ANÚNCIOS ocorrerá imediatamente após o coletor ser reiniciado. Levará aproximadamente 15 minutos para obter dados do usuário de aproximadamente 300K usuários e é atualizado a cada 12 horas automaticamente. |

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

## Configurando um LDAP Directory Server Collector

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

**Antes de começar**

- Você deve ser um Administrador do Data Infrastructure Insights ou um proprietário de conta para executar

esta tarefa.

- Você deve ter o endereço IP do servidor que hospeda o servidor LDAP Directory.
- Um agente deve ser configurado antes de configurar um conetor de diretório LDAP.

**Passos para configurar um Coletor de diretório de usuários**

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

   O sistema exibe a tela Adicionar diretório do usuário.

Configure o Coletor de diretório de usuários inserindo os dados necessários nas seguintes tabelas:

| Nome | Descrição |
|---|---|
| Nome | Nome exclusivo para o diretório do usuário. Por exemplo *GlobalLDAPCollector* |
| Agente | Selecione um agente configurado na lista |
| Nome de domínio/IP do servidor | Endereço IP ou nome de domínio totalmente qualificado (FQDN) do servidor que hospeda o servidor de diretório LDAP |
| Base de pesquisa | Base de pesquisa do servidor LDAP a base de pesquisa permite ambos os seguintes formatos: *X.y.z*> nome de domínio direto como você o tem no SVM. *DC_DC_DC_DC_NetApp c*<username> c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_<engineering>_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c_c |
| Vincular DN | Usuário autorizado a pesquisar o diretório. Por exemplo: uid, uid, uid, uid, uid, uid, uid, ucn, contas, dc, empresa, dc, dc, com para um usuário john@dorp.company.com. dorp.company.com |
| --contas | --usuários |
| --john | --anna |
| Palavra-passe BIND | Senha do servidor de diretório (ou seja, senha para nome de usuário usado no DN de vinculação) |
| Protocolo | ldap, ldaps, ldap-start-tls |
| Portas | Selecione a porta |

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

| Atributos | Nome do atributo no Directory Server |
|---|---|
| Nome de exibição | nome |
| UNIXID | número de identificação |

| | |
|---|---|
| Nome de utilizador | uid |

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

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

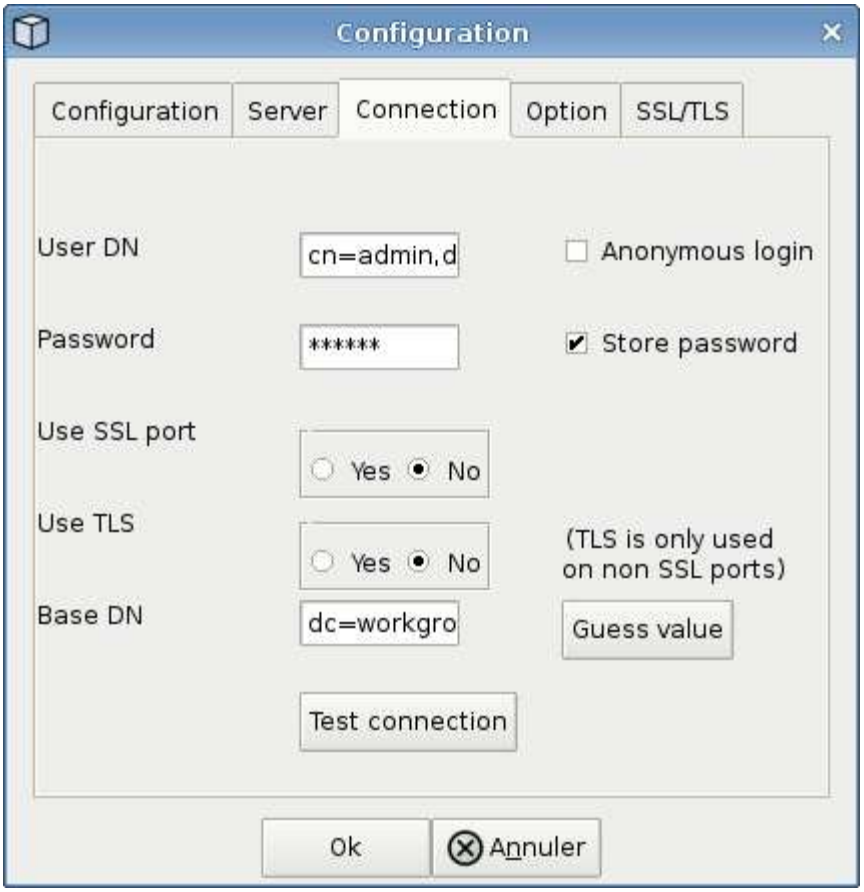
**Testando a configuração do coletor do diretório de usuários**

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

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

```
 ldapsearch -D "uid=john
,cn=users,cn=accounts,dc=dorp,dc=company,dc=com" -W -x -LLL -o ldif-
wrap=no -b "cn=accounts,dc=dorp,dc=company,dc=com" -H
ldap://vmwipaapp08.dorp.company.com
* Use o LDAP Explorer para navegar em um banco de dados LDAP, exibir
propriedades e atributos de objetos, exibir permissões, exibir o esquema
de um objeto, executar pesquisas sofisticadas que você pode salvar e
executar novamente.
```

  - Instale o LDAP Explorer (http://ldaptool.sourceforge.net/) ou o Java LDAP (http://jxplorer.org/Explorer ) em qualquer máquina Windows que possa se conetar ao servidor LDAP.
  - Conete-se ao servidor LDAP usando o nome de usuário/senha do servidor de diretório LDAP.




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

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

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

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

| Problema: | Resolução: |
| --- | --- |
| O conetor de diretório LDAP resulta no estado "erro". "O conetor está no estado de erro. Nome do serviço: UsersLdap. Motivo da falha: Falha ao recuperar usuários LDAP. Motivo da falha: 80090308: LdapErr: DSID-0C090453, comentário: AcceptSecurityContext error, data 52e, v3839" | Nome da floresta incorreto fornecido. Veja acima como fornecer o nome correto da floresta. |
| O número de telefone não está a ser preenchido na página de perfil de utilizador. | Isso é provavelmente devido a um problema de mapeamento de atributos com o ative Directory. 1. Edite o coletor específico do ative Directory que está obtendo as informações do usuário do ative Directory. 2. Em atributos opcionais, há um nome de campo "número de telefone" mapeado para o atributo do ative Directory 'número de telefone'. 4. Agora, utilize a ferramenta Explorador do ative Directory conforme descrito acima para navegar no servidor LDAP Directory e ver o nome do atributo correto. 3. Certifique-se de que no diretório LDAP existe um atributo chamado "número de telefone" que tem realmente o número de telefone do usuário. 5. Digamos que no diretório LDAP ele foi modificado para "número de telefone". 6. Em seguida, edite o coletor CloudSecure User Directory. Na seção de atributo opcional, substitua 'número de telefone' por 'número de telefone'. 7. Salve o coletor do ative Directory, o coletor reiniciará e obterá o número de telefone do usuário e exibirá o mesmo na página do perfil do usuário. |
| Se o certificado de encriptação (SSL) estiver ativado no servidor AD (ative Directory), o Coletor do diretório de utilizadores de Segurança de carga de trabalho não pode ligar-se ao servidor AD. | Desative a criptografia do AD Server antes de configurar um coletor de diretório de usuários. Uma vez que os detalhes do usuário são obtidos, ele estará lá por 13 meses. Se o servidor AD for desconetado após buscar os detalhes do usuário, os usuários recém-adicionados no AD não serão obtidos. Para buscar novamente, o coletor de diretório do usuário precisa ser conetado ao AD. |

## Configurando o coletor de dados SVM do ONTAP

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

### Antes de começar

- Este coletor de dados é suportado com o seguinte:
  - Data ONTAP 9,2 e versões posteriores. Para obter o melhor desempenho, use uma versão do Data ONTAP superior a 9.13.1.
  - Protocolo SMB versão 3,1 e anterior.
  - Versões NFS até NFS 4,1 com ONTAP 9.15,1 ou posterior, inclusive.

- O FlexGroup é suportado a partir do ONTAP 9 .4 e versões posteriores
- O ONTAP Select é suportado

- Somente SVMs do tipo de dados são compatíveis. SVMs com volumes infinitos não são compatíveis.
- O SVM tem vários subtipos. Destes, apenas *default*, *Sync_source* e *Sync_destination* são suportados.
- Um agente "tem de ser configurado" antes de poder configurar coletores de dados.
- Certifique-se de ter um conetor do diretório de usuário configurado corretamente, caso contrário, os eventos mostrarão nomes de usuário codificados e não o nome real do usuário (como armazenado no ative Directory) na página "Activity Forensics".
- • O ONTAP Persistent Store é suportado a partir de 9.14.1.
- Para um desempenho ideal, você deve configurar o servidor FPolicy para estar na mesma sub-rede que o sistema de armazenamento.
- É necessário adicionar um SVM usando um dos dois métodos a seguir:
  - Usando o IP do cluster, o nome do SVM e o nome de usuário e a senha do gerenciamento de cluster. ***este é o método recomendado.***
    - O nome da SVM deve ser exatamente como mostrado no ONTAP e diferencia maiúsculas de minúsculas.
  - Usando o SVM Management IP, Nome de usuário e Senha
  - Se você não puder ou não estiver disposto a usar o nome de usuário e senha completos do gerenciamento do cluster do administrador/SVM, você poderá criar um usuário personalizado com Privileges menor, conforme mencionado na "Uma nota sobre permissões"seção abaixo. É possível criar esse usuário personalizado para SVM ou acesso a cluster.
    - O você também pode usar um usuário do AD com uma função que tenha pelo menos as permissões de csrole como mencionado na seção "Uma nota sobre permissões" abaixo. Consulte também a "Documentação do ONTAP".
- Verifique se os aplicativos corretos estão definidos para o SVM executando o seguinte comando:

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

Exemplo de saída:

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

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

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

- Defina uma senha para o usuário SVM vsadmin. Se estiver usando usuário personalizado ou usuário de

administrador de cluster, pule esta etapa. Clustershell::> `security login password -username vsadmin -vserver svmname`

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

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

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

### Pré-requisitos para bloqueio de acesso do usuário

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

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

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

Se você estiver usando um usuário personalizado (por exemplo, *csuser*) com permissões dadas ao usuário, siga as etapas abaixo para conceder permissões ao Workload Security para bloquear o usuário.

Para csuser com credenciais de cluster, faça o seguinte na linha de comando 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
```

### Uma Nota sobre permissões

#### Permissões ao adicionar via Cluster Management IP:

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

Para criar o novo usuário, faça login no ONTAP com o nome de usuário/senha do administrador de gerenciamento de cluster e execute os seguintes comandos no servidor ONTAP:

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

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

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

**Permissões ao adicionar via SVM Management IP:**

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

Para criar o novo usuário, faça login no ONTAP com o nome de usuário/senha do administrador de gerenciamento de cluster e execute os seguintes comandos no servidor ONTAP. Para facilitar, copie esses comandos para um editor de texto e substitua o <vservername> pelo nome do SVM antes e execute esses comandos no ONTAP:

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

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

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

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

#### Modo Protobuf

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

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

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

Modo de cluster:

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

Modo SVM:

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

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

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

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

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

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

### Configurar o coletor de dados

#### Passos para a configuração

1. Faça login como Administrador ou proprietário de conta no seu ambiente Data Infrastructure Insights.
2. Clique em **Workload Security > Collectors > Coletores de dados**

   O sistema exibe os coletores de dados disponíveis.

3. Passe o Mouse sobre o bloco **NetApp SVM e clique em * Monitor**.

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

| Campo | Descrição |
|---|---|
| Nome | Nome exclusivo para o Data Collector |
| Agente | Selecione um agente configurado na lista. |
| Ligar através de IP de gestão para: | Selecione Cluster IP ou SVM Management IP |
| Endereço IP do gerenciamento de cluster/SVM | O endereço IP do cluster ou do SVM, dependendo da sua seleção acima. |
| Nome SVM | O Nome do SVM (este campo é obrigatório ao se conetar via IP de cluster) |
| Nome de utilizador | Nome de usuário para acessar o SVM/cluster ao adicionar via IP de cluster as opções são: 1. Cluster-admin 2. 'csuser' 3. AD-user com papel semelhante ao csuser. Ao adicionar via SVM IP, as opções são: 4. Vsadmin 5. 'csuser' 6. AD-username com função semelhante ao csuser. |
| Palavra-passe | Senha para o nome de usuário acima |
| Filtre compartilhamentos/volumes | Escolha se deseja incluir ou excluir compartilhamentos / volumes da coleção de eventos |
| Introduza nomes de partilha completos para excluir/incluir | Lista de compartilhamentos separados por vírgulas para excluir ou incluir (conforme apropriado) da coleção de eventos |
| Introduza nomes de volume completos para excluir/incluir | Lista de volumes separados por vírgulas para excluir ou incluir (conforme apropriado) da coleção de eventos |

| | |
|---|---|
| Monitorar o acesso à pasta | Quando marcada, ativa eventos para monitoramento de acesso a pastas. Observe que a pasta criar/renomear e excluir será monitorada mesmo sem essa opção selecionada. Ativar isto aumentará o número de eventos monitorizados. |
| Definir o tamanho do buffer de envio do ONTAP | Define o tamanho do buffer de envio do Fpolicy do ONTAP. Se uma versão do ONTAP anterior a 9.8p7 for usada e um problema de desempenho for visto, o tamanho do buffer de envio do ONTAP pode ser alterado para obter um desempenho aprimorado do ONTAP. Entre em Contato com o suporte da NetApp se você não vir essa opção e deseja explorá-la. |

**Depois de terminar**

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

### Configuração recomendada para MetroCluster

O seguinte é recomendado para o MetroCluster:

1. Conecte dois coletores de dados, um ao SVM de origem e outro ao SVM de destino.
2. Os coletores de dados devem ser conetados por *Cluster IP*.
3. A qualquer momento, um coletor de dados deve estar em execução, outro estará em erro.

   O coletor de dados do SVM atual será exibido como *Running*. O coletor de dados do SVM 'parado' atual será exibido como *Error*.

4. Sempre que houver um switchover, o estado do coletor de dados mudará de "execução" para "erro" e vice-versa.
5. Levará até dois minutos para que o coletor de dados se mova do estado de erro para o estado de execução.

### Política de Serviço

Se estiver usando a política de serviço com o ONTAP **versão 9.9.1 ou mais recente**, a fim de se conetar ao coletor de origem de dados, o serviço *data-fpolicy-client* será necessário junto com o serviço de dados *data-nfs* e/ou *data-cifs*.

Exemplo:

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

Em versões do ONTAP anteriores a 9,9.1, *data-fpolicy-client* não precisam ser definidas.

**Play-Pause Data Collector**

2 novas operações são agora mostradas no menu kebab do coletor (PAUSA e RETOMADA).

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

Observe que se novos volumes, etc. forem criados no ONTAP enquanto o coletor estiver em pausa, a Segurança de carga de trabalho não coletará os dados e esses volumes, etc., não serão refletidos em painéis ou tabelas.

Tenha em mente o seguinte:

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

**Armazenamento persistente**

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

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

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

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

Modo de cluster:

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster-name>
security login rest-role create -role csrestrole -api /api/cluster/jobs/
-access readonly -vserver <cluster-name>
```

Modo SVM:

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <vserver-name>
security login rest-role create -role csrestrole -api /api/cluster/jobs/
-access readonly -vserver <vserver-name>
```

#### Solução de problemas

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

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

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

#### Configuração de armazenamento Cloud Volumes ONTAP

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

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

#### Plataformas compatíveis

- Cloud Volumes ONTAP, compatível com todos os fornecedores de serviços de nuvem disponíveis, onde disponível. Por exemplo: Amazon, Azure, Google Cloud.
- ONTAP no FSX

#### Configuração da Máquina do Agente

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

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

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

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

trabalho:

**Passos**

1. Faça login no console da AWS e navegue até a página de instâncias EC2 e selecione *Launch instance*.
2. Selecione uma AMI RHEL ou CentOS com a versão apropriada, conforme mencionado nesta página: https://docs.netapp.com/us-en/cloudinsights/concept_cs_agent_requirements.html
3. Selecione a VPC e a sub-rede em que a instância do Cloud ONTAP reside.
4. Selecione *T2.xlarge* (4 vcpus e 16 GB de RAM) como recursos alocados.
   a. Crie a instância EC2.
5. Instale os pacotes Linux necessários usando o gerenciador de pacotes YUM:
   a. Instale os pacotes Linux nativos *wget* e *unzip*.

**Instale o agente de segurança de carga de trabalho**

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

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

**Solução de problemas**

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

| Problema | Resolução |
| --- | --- |
| "Segurança de carga de trabalho: Falha ao determinar o tipo de ONTAP para o coletor de dados do Amazon FxSN" é mostrado pelo coletor de dados. O cliente não consegue adicionar um novo coletor de dados Amazon FSxN ao Workload Security. A conexão com o cluster FSxN na porta 443 do agente está esgotando. Os grupos de segurança do firewall e da AWS têm as regras necessárias habilitadas para permitir a comunicação. Um agente já está implantado e também está na mesma conta da AWS. Esse mesmo agente é usado para conetar e monitorar os dispositivos NetApp restantes (e todos eles estão funcionando). | Resolva esse problema adicionando o segmento de rede fsxadmin LIF à regra de segurança do agente. Permitido todas as portas se você não tiver certeza sobre as portas. |

## Gerenciamento de usuários

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

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

| Função | Acesso à segurança do workload |
|---|---|
| Administrador | Pode executar todas as funções de Segurança de carga de trabalho, incluindo as de Alertas, Forensics, coletores de dados, políticas de resposta automatizadas e APIs para Segurança de carga de trabalho. Um administrador também pode convidar outros usuários, mas só pode atribuir funções de Segurança de carga de trabalho. |
| Utilizador | Pode visualizar e gerir Alertas e visualizar Forensics. A função de usuário pode alterar o status de alerta, adicionar uma nota, tirar snapshots manualmente e restringir o acesso do usuário. |
| Convidado | Pode visualizar Alertas e Forensics. A função convidado não pode alterar o status de alerta, adicionar uma nota, tirar snapshots manualmente ou restringir o acesso do usuário. |

**Passos**

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

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

3. Selecione a função pretendida para cada utilizador.

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

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

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

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

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

**Requisitos:**

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

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

Passos:

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

```
 /opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
. Este script requer _sshpass_ para ser instalado na máquina linux. Há
duas maneiras de instalá-lo:
```

   a. Execute o seguinte comando:

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

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

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

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

Cada coletor de dados do ONTAP SVM pode ser associado a um único SVM, ou seja, cada coletor de dados poderá receber o número de eventos gerados por um único SVM.

Tenha em mente o seguinte:

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

| Configuração da Máquina do Agente | Número de coletores de dados SVM | Taxa máxima de eventos que a máquina do agente pode lidar |
|---|---|---|
| 4 núcleo, 16GB | 10 coletores de dados | 20k eventos/seg |
| 4 núcleo, 32GB | 20 coletores de dados | 20k eventos/seg |

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

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

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

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

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

**Exemplo**

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

Aplicamos a fórmula:

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

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

O script pode dar resultados errôneos nos seguintes casos:

- Credenciais, IP ou nome do SVM incorretos são fornecidos.
- Um fpolicy já existente com o mesmo nome, número de sequência, etc. irá dar erro.
- O script é interrompido abruptamente durante a execução.

Um exemplo de execução de script é mostrado abaixo:

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

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

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

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

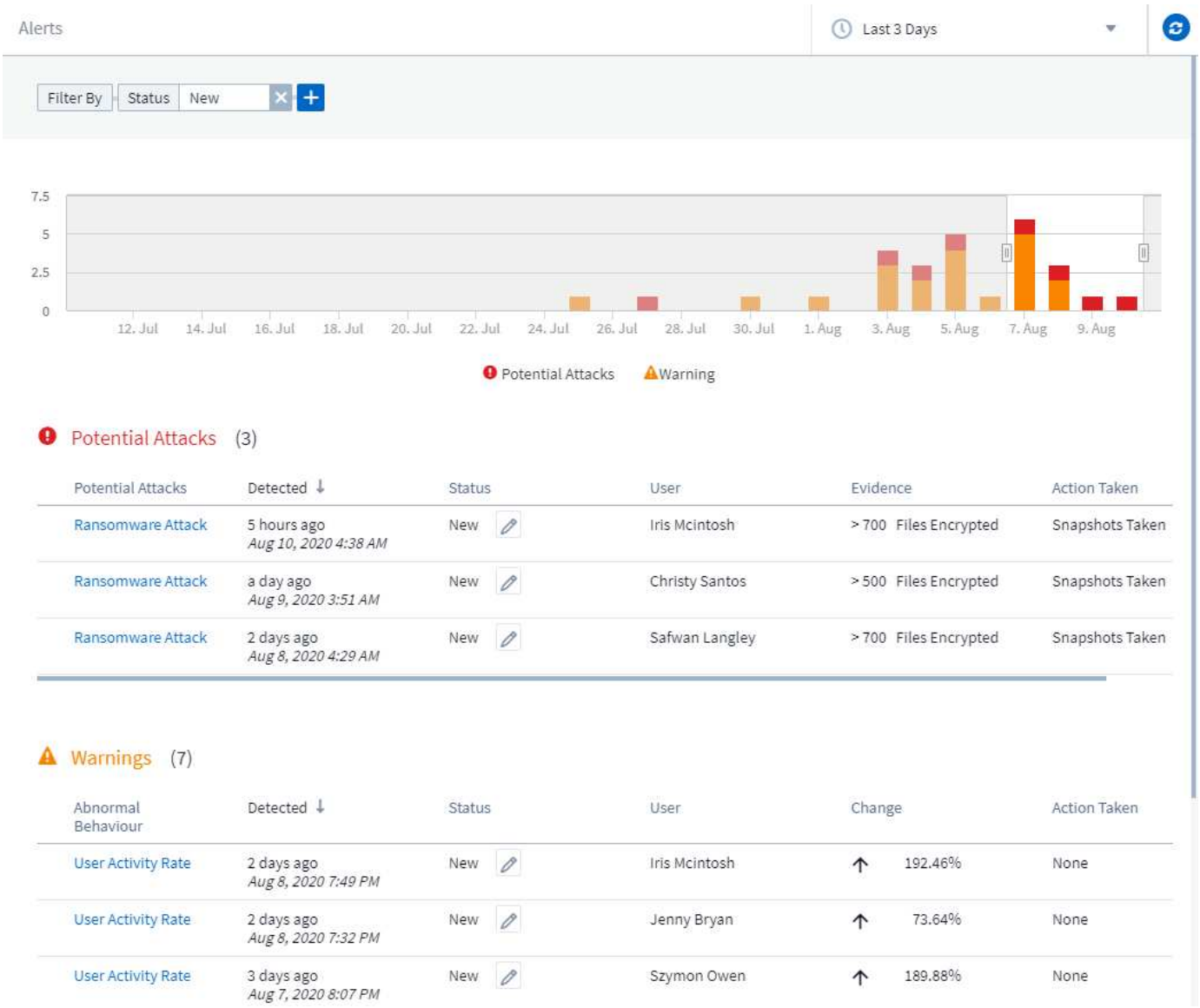
**Solução de problemas**

| Pergunta | Resposta |
| --- | --- |

| | |
|---|---|
| Se eu executar esse script em um SVM que já esteja configurado para o Workload Security, ele só usará a configuração fpolicy existente no SVM ou configurará uma configuração temporária e executará o processo? | O Event Rate Checker pode ser executado corretamente mesmo para um SVM já configurado para Workload Security. Não deve haver impactos. |
| Posso aumentar o número de SVMs em que o script pode ser executado? | Sim. Basta editar o script e alterar o número máximo de SVMs de 5 para qualquer número desejável. |
| Se eu aumentar o número de SVMs, isso aumentará o tempo de execução do script? | Não. O script será executado por um máximo de 5 minutos, mesmo que o número de SVMs seja aumentado. |
| Posso aumentar o número de SVMs em que o script pode ser executado? | Sim. Você precisa editar o script e alterar o número máximo de SVMs de 5 para qualquer número desejável. |
| Se eu aumentar o número de SVMs, isso aumentará o tempo de execução do script? | Não. O script será executado por um máximo de 5mins, mesmo que o número de SVMs seja aumentado. |
| O que acontece se eu executar o Event Rate Checker com um agente existente? | A execução do Event Rate Checker em relação a um agente já existente pode causar um aumento na latência do SVM. Este aumento será temporário por natureza enquanto o verificador de taxa de eventos estiver em execução. |

# Alertas

A página Alertas de Segurança de carga de trabalho mostra uma linha do tempo de ataques e/ou avisos recentes e permite visualizar detalhes de cada problema.




## Alerta

A lista Alerta apresenta um gráfico que mostra o número total de potenciais ataques e/ou Avisos que foram levantados no intervalo de tempo selecionado, seguido de 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 fim no gráfico.

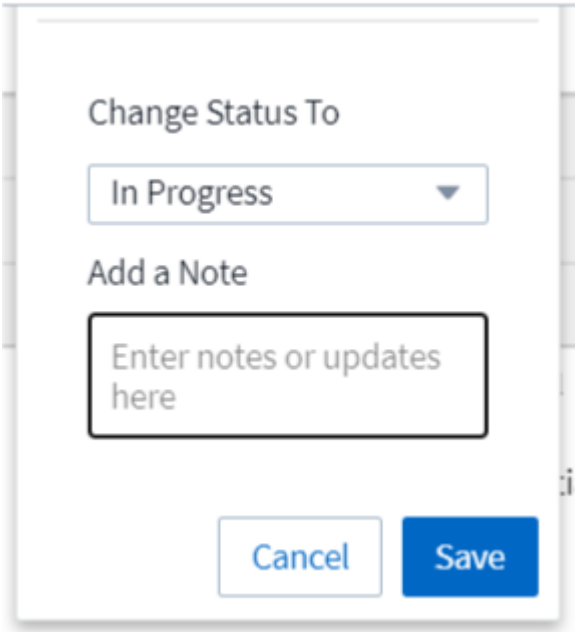
É apresentado o seguinte para cada alerta:

**Potenciais ataques:**

- O tipo *potential Attack* (por exemplo, ransomware ou Sabotage)
- A data e a hora em que o ataque potencial foi *detetado*
- O *Status* do alerta:
  - **Novo**: Este é o padrão para novos alertas.
  - **Em andamento**: O alerta está sob investigação por um membro da equipe ou membros.
  - **Resolvido**: O alerta foi marcado como resolvido por um membro da equipe.

- **Demitido**: O alerta foi rejeitado como comportamento falso positivo ou esperado.

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




- O *User* cujo comportamento acionou 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 acionou o aviso
- A data e a hora em que o comportamento foi *detetado*
- O *Status* do alerta (novo, em andamento, etc.)
- O *User* cujo comportamento acionou o alerta
- Uma descrição do *change* (por exemplo, um aumento anormal no acesso ao arquivo)
- A *Ação tomada*

## Opções de filtro

Você pode filtrar os alertas pelo seguinte:

- O *Status* do alerta
- Texto específico na *Nota*
- O tipo de *ataques/Avisos*
- O *User* cujas ações desencadearam o alerta/aviso

## A página Detalhes do alerta

Você pode clicar em um link de alerta na página da lista Alertas para abrir uma página de detalhes para o alerta. Os detalhes do alerta podem variar de acordo com o tipo de ataque ou alerta. Por exemplo, uma

página de detalhes do ataque do ransomware pode mostrar as seguintes informações:

**Secção de resumo:**

- Tipo de ataque (ransomware, sabotagem) e ID de alerta (atribuído pela Workload Security)
- Data e hora em que o ataque foi detetado
- Ação tomada (por exemplo, um instantâneo automático foi feito. A hora do instantâneo é mostrada imediatamente abaixo da seção de resumo))
- Estado (novo, em curso, etc.)

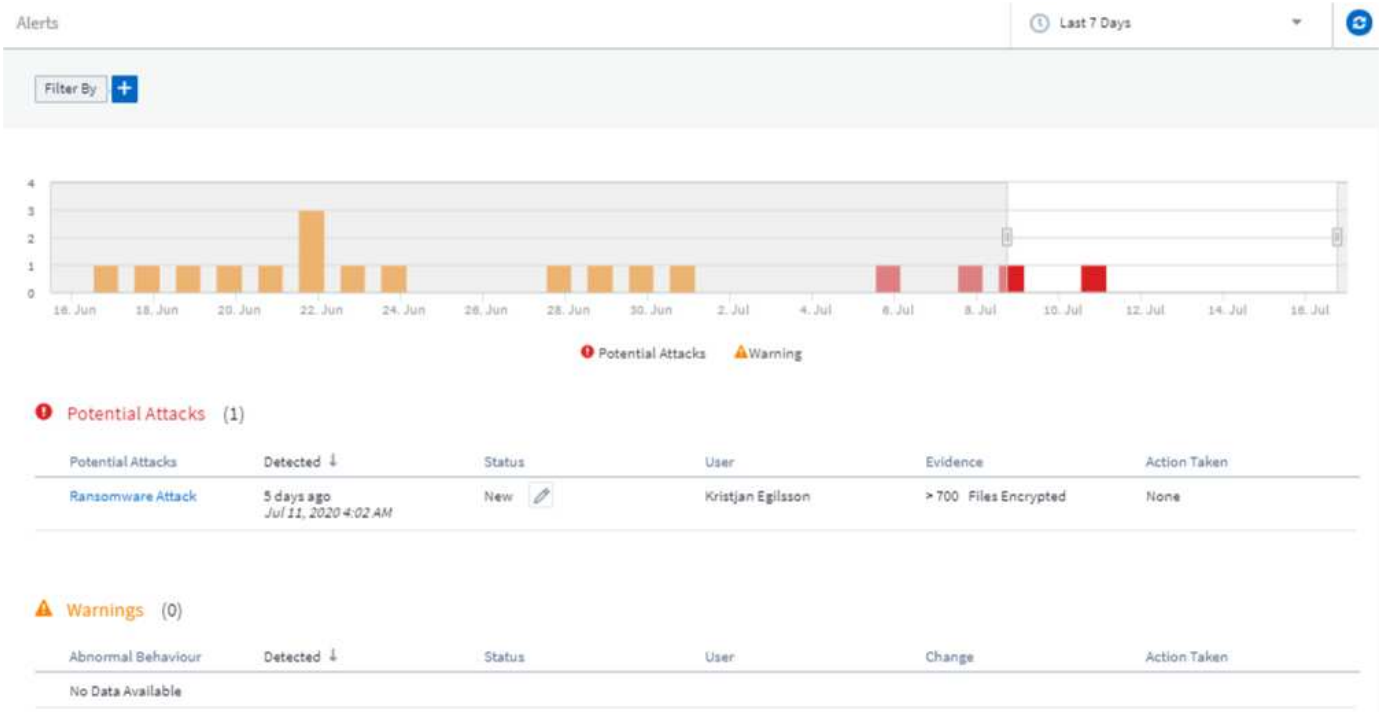
**Seção de resultados do ataque:**

- Contagens de volumes e arquivos afetados
- Um resumo que acompanha a deteção
- Um gráfico mostrando a atividade do arquivo durante o ataque

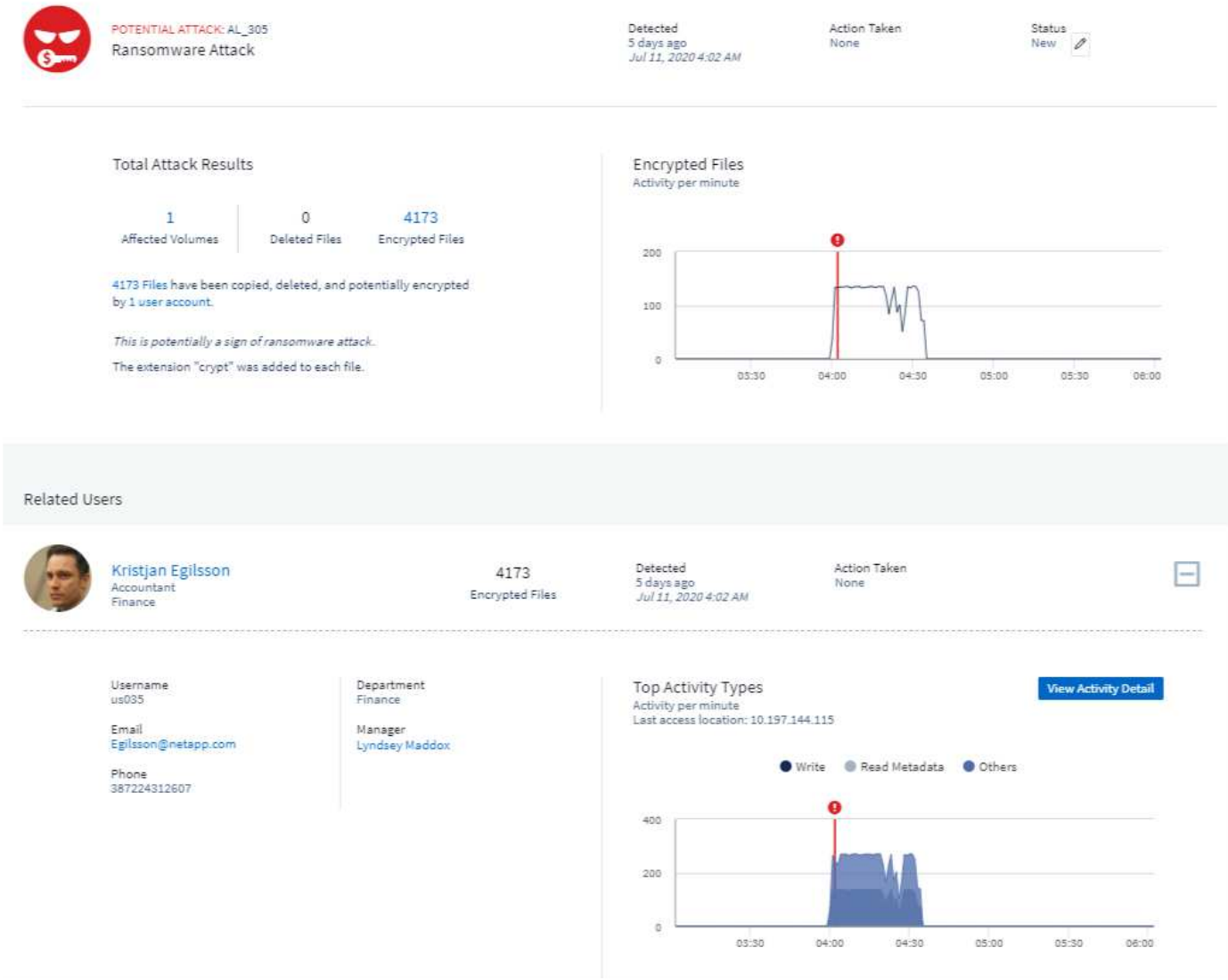
**Secção utilizadores relacionados:**

Esta seção mostra detalhes sobre o usuário envolvido no ataque potencial, incluindo um gráfico de atividade superior para o usuário.

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




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

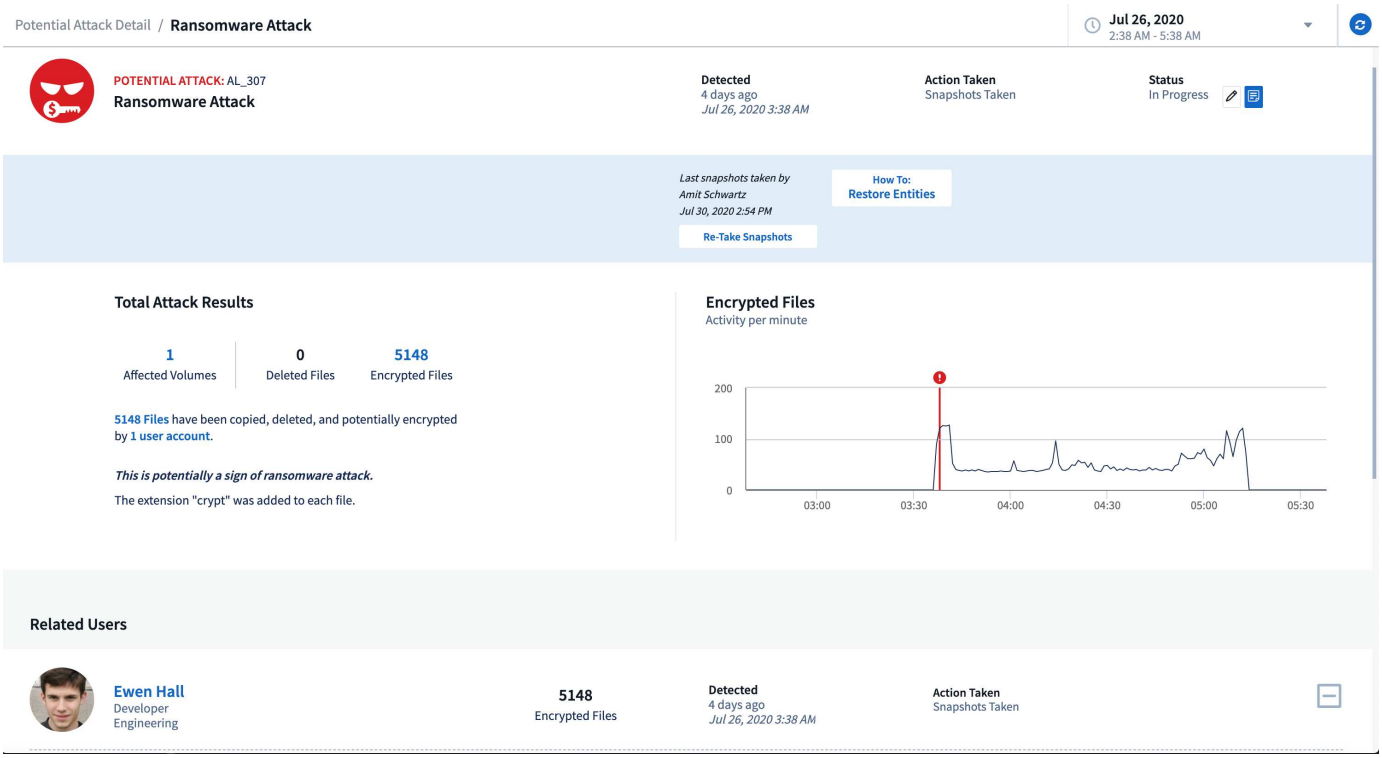



## *Faça um instantâneo* **Ação**

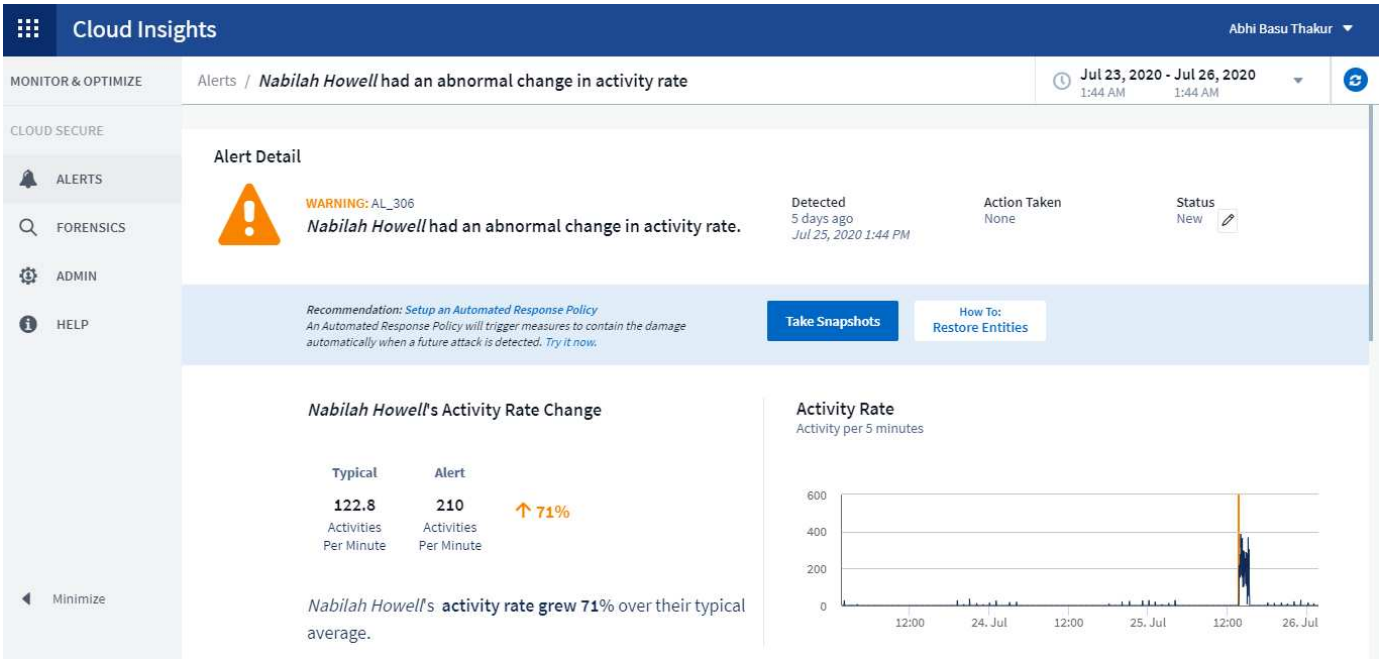
O Workload Security protege seus dados tirando automaticamente um snapshot quando uma atividade maliciosa é detetada, garantindo que seus dados sejam copiados com segurança.

Você pode definir "políticas de resposta automatizadas" essa captura instantânea quando um ataque de ransomware ou outra atividade anormal do usuário é detetada. Também pode tirar um instantâneo manualmente a partir da página de alerta.

Instantâneo automático captado:




Instantâneo manual:




## Notificações de alerta

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

## Política de retenção

Os alertas e avisos são mantidos por 13 meses. Os alertas e avisos com mais de 13 meses serão eliminados. Se o ambiente de Segurança de workload for excluído, todos os dados associados ao ambiente também

serão excluídos.

### Solução de problemas

| Problema: | Tente isto: |
| --- | --- |
| Há uma situação em que o ONTAP tira snapshots por hora por dia. Os snapshots do Workload Security (WS) afetarão isso? O instantâneo WS fará o instantâneo por hora local? O instantâneo por hora padrão será interrompido? | Os snapshots de segurança da carga de trabalho não afetarão os instantâneos por hora. Os instantâneos WS não tirarão o espaço instantâneo por hora e isso deverá continuar como antes. O instantâneo por hora padrão não será interrompido. |
| O que acontecerá se a contagem máxima de instantâneos for atingida no ONTAP? | Se a contagem máxima de instantâneos for atingida, a captura subsequente de instantâneos falhará e o Workload Security mostrará uma mensagem de erro observando que o instantâneo 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 Snapshot. No ONTAP 9.4 e posterior, um volume pode conter até 1023 cópias snapshot. Consulte a documentação do ONTAP para obter informações "Definição da política de eliminação de instantâneos"sobre . |
| A segurança do workload não consegue tirar snapshots. | Certifique-se de que a função que está sendo usada para criar snapshots tenha o xref:./ https://docs.NetApp.com/US-en/cloudinsights/ task_add_Collector_svm.html. Certifique-se de que *csrole* é criado com direitos de acesso adequados para tirar snapshots: Função de login de segurança criar -vserver <vservername> -role csrole -cmddirname "volume snapshot" -acessar tudo |
| Os snapshots estão falhando em alertas mais antigos em SVMs que foram removidos do Workload Security e posteriormente adicionados novamente. Para novos alertas que ocorrem após a adição da SVM novamente, snapshots são feitos. | Este é um cenário raro. Caso isso ocorra, faça login no ONTAP e tire os snapshots manualmente para os alertas mais antigos. |
| Na página *Detalhes do alerta*, a mensagem erro "Falha na última tentativa" é vista abaixo do botão *tirar instantâneo*. Passar o Mouse sobre o erro exibe "Invoke API comando excedeu o tempo limite para o coletor de dados com id". | Isso pode acontecer quando um coletor de dados é adicionado à segurança de carga de trabalho por meio do IP de gerenciamento de SVM, se o LIF da SVM estiver no estado *disabled* no ONTAP. Ative o LIF em particular no ONTAP e acione *tirar instantâneo manualmente* da Segurança da carga de trabalho. A ação Snapshot será então bem-sucedida. |

# Forense

## Forensics - todas as atividades

A página All Activity ajuda você a entender as ações executadas em entidades no

ambiente Workload Security.

#### Examinando todos os dados de atividade

Clique em **Forensics > Activity Forensics** e clique na guia **All Activity** para acessar a página All Activity. Esta página fornece uma visão geral das atividades do seu inquilino, destacando as seguintes informações:

- Um gráfico mostrando *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 ampliada, é apresentado um botão que permite ao utilizador reduzir o zoom.

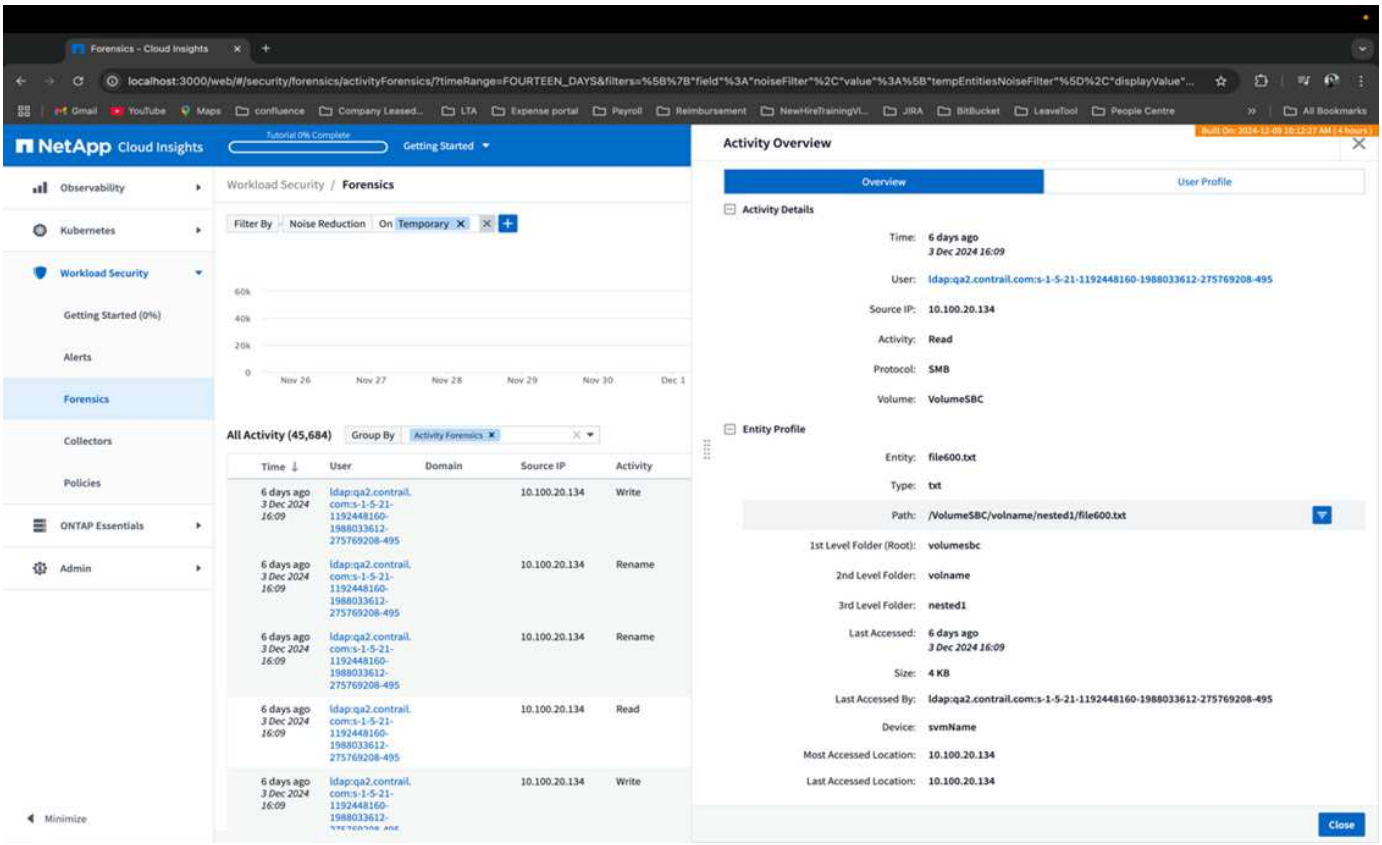
- Uma lista dos dados *All Activity*.
- Um grupo por lista suspensa fornecerá a opção de agrupar a atividade por usuários, caminho, tipo de entidade etc.
- Um botão de caminho comum estará disponível acima da tabela em clique da qual podemos obter slide out painel com detalhes de caminho de entidade.

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

- A **hora** 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 utilizador" como um painel deslizante.
- A **atividade** realizada pelo usuário. Os tipos suportados são:
  - **Alterar propriedade do grupo** - a propriedade do grupo é de arquivo ou pasta é alterada. Para obter 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 de arquivo ou pasta é alterada.
  - * Criar* - criar arquivo ou pasta.
  - **Excluir** - Excluir arquivo ou pasta. Se uma pasta for excluída, os eventos *delete* serão obtidos para todos os arquivos dessa pasta e subpastas.
  - **Leia** - o ficheiro é lido.
  - **Leia metadados** - somente na opção de monitoramento de pastas ativada. Será gerado ao abrir uma pasta no Windows ou executando "ls" dentro de uma pasta no Linux.
  - **Renomear** - Renomear arquivo ou pasta.
  - **Write** - os dados são gravados em um arquivo.
  - **Write Metadata** - os metadados do arquivo são escritos, por exemplo, permissão alterada.
  - **Outra alteração** - qualquer outro evento que não esteja descrito acima. Todos os eventos não mapeados são mapeados para o tipo de atividade "outra mudança". Aplicável a ficheiros e pastas.
- O **Path** é *entity* path.
- A pasta de nível **1st (raiz)** é o diretório raiz do caminho da entidade em letras minúsculas.
- A pasta de nível **2nd** é o diretório de segundo nível do caminho da entidade em letras minúsculas.
- A pasta de nível **3rd** é o diretório de terceiro nível do caminho da entidade em letras minúsculas.

- A pasta **4th Level** é o diretório de quarto nível do caminho da entidade em letras minúsculas.
- A extensão **Entity Type**, incluindo 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 renomear eventos quando o arquivo original foi renomeado. Esta coluna não está visível na tabela por padrão. Use o seletor de coluna para adicionar essa coluna à tabela.
- O **volume** onde as entidades residem. Esta coluna não está visível na tabela por padrão. Use o seletor de coluna para adicionar essa coluna à tabela.

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




O método padrão *Group by* é *Activity Forensics*. Se você selecionar um método *Group by* diferente—por exemplo, tipo de entidade—a tabela entidade *Group by* será exibida. Se nenhuma seleção for feita, *Group by* **All** será exibido.

- A contagem de atividades é apresentada como uma hiperligação; selecionar esta opção irá adicionar o agrupamento selecionado como um filtro. A tabela de atividade será atualizada com base nesse filtro.
- Observe que se você alterar o filtro, alterar o intervalo de tempo ou atualizar a tela, não será possível retornar aos resultados filtrados sem definir o filtro novamente.

### Filtragem de dados do histórico de atividades forenses

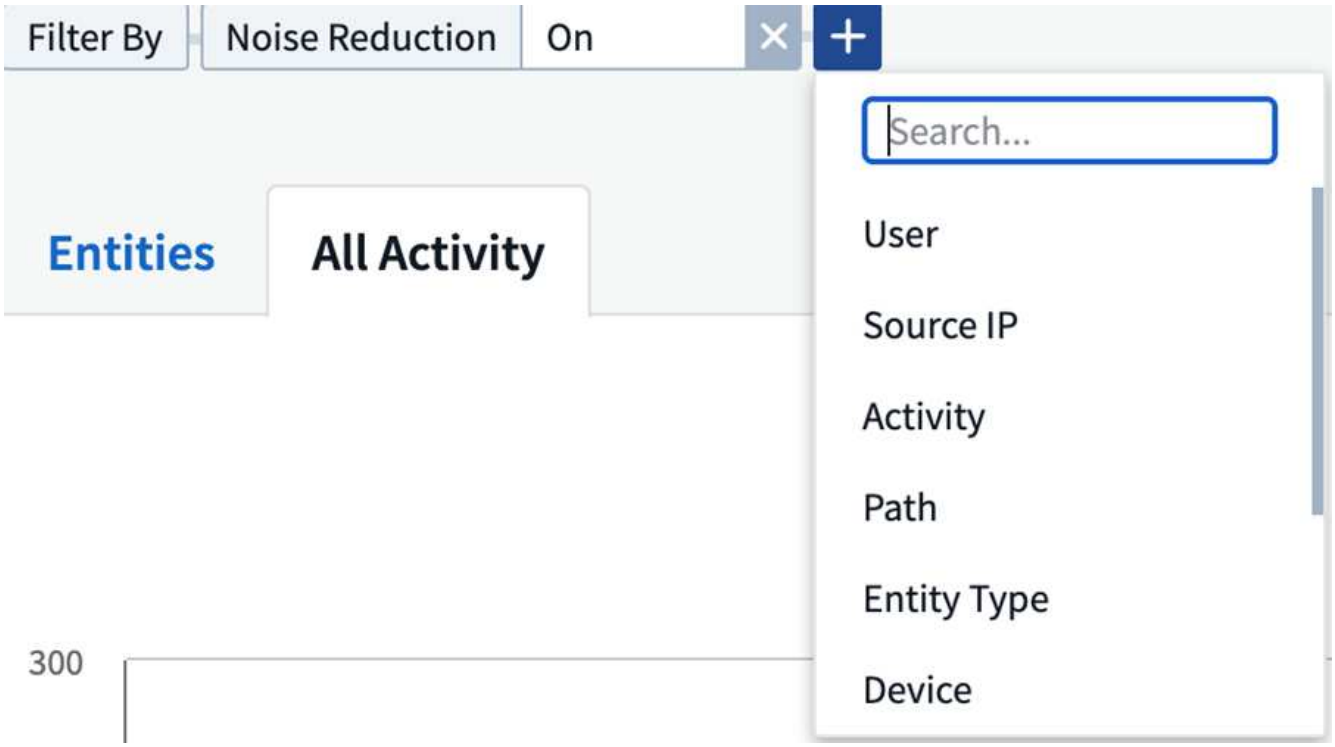
Existem dois métodos que você pode usar para filtrar dados.

- O filtro pode ser adicionado a partir do painel deslizante. O valor é adicionado aos filtros apropriados na

lista acima *Filtrar por*.

- Filtre dados digitando no campo *Filtrar por*:

  Selecione o filtro apropriado no topo do widget 'Filtrar por' clicando no botão *[




  Introduza o texto de pesquisa

  Pressione Enter ou clique fora da caixa de filtro para aplicar o filtro.

Você pode filtrar os dados de atividade Forense pelos seguintes campos:

- O tipo **Activity**.
- **IP de origem** a partir do qual a entidade foi acessada. Você deve fornecer um endereço IP de origem válido em aspas duplas, por exemplo "10,1.1,1". IPs incompletos, como "10,1.1.**", "10,1.**.*", etc., não funcionarão.
- **Protocolo** para buscar atividades específicas do protocolo.
- **Nome de usuário** do usuário que realiza a atividade. Você precisa fornecer o nome de usuário exato para filtrar. A pesquisa com nome de usuário parcial ou nome de usuário parcial pré-fixado ou sufixo 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 realiza a atividade. Você precisa fornecer o **domínio exato** para filtrar. Procurar domínio parcial, ou domínio parcial prefixado ou sufixo com curinga ('*'), não funcionará. *None* pode ser especificado para procurar domínio ausente.

Os seguintes campos estão sujeitos a regras especiais de filtragem:

- **Entity Type**, usando a extensão entity (file) - é preferível especificar o tipo exato de entidade dentro de aspas. Por exemplo *"txt"*.

- **Path** da entidade - filtros de caminho de diretório (string de caminho que termina com /) até 4 diretórios profundos são recomendados para resultados mais rápidos. Por exemplo, *"/home/userX/nested1/nested2/"*. Consulte a tabela abaixo para obter mais detalhes.
- 1st Level Folder (root) - diretório raiz do Entity Path como filtros. Por exemplo, se o caminho da entidade for /home/userX/nested1/nested2/, então Home OU "Home" pode ser usado.
- Pasta de nível 2nd - diretório de nível 2nd dos filtros Entity Path. Por exemplo, se o caminho da entidade é /home/userX/nested1/nested2/, então userX OU "userX" pode ser usado.
- Pasta de nível 3rd – diretório de nível 3rd dos filtros Entity Path.
- Por exemplo, se o caminho da entidade é /home/userX/nested1/nested2/, então nested1 OU "nested1" pode ser usado.
- Pasta de nível 4th - diretório de nível 4th dos filtros Entity Path. Por exemplo, se o caminho da entidade é /home/userX/nested1/nested2/, então nested2 OU "nested2" pode ser usado.
- **Usuário** realizando a atividade - é preferível especificar o usuário exato dentro de aspas. Por exemplo, *"Administrador"*.
- **Dispositivo** (SVM) onde as entidades residem
- **Volume** onde as entidades residem
- O **caminho original** usado para renomear eventos quando o arquivo original foi renomeado.

Os campos anteriores estão sujeitos ao seguinte ao filtrar:

- O valor exato deve estar entre aspas: Exemplo: "Searchtext"
- Strings curinga não devem conter aspas: Exemplo: Searchtext, * searchtext*, irá filtrar para quaisquer strings contendo 'searchtext'.
- String com um prefixo, exemplo: Searchtext* , pesquisará quaisquer strings que começam com 'searchtext'.

**Exemplos de filtro de atividade Forensics:**

| Expressão de filtro aplicada pelo usuário | Resultado esperado | Avaliação de desempenho | Comentário |
|---|---|---|---|
| Caminho: "/home/userX/nested1/nested2/" | Pesquisa recursiva de todos os arquivos e pastas sob determinado diretório | Rápido | Pesquisas de diretório até 4 diretórios serão rápidas. |
| Caminho: "/home/userX/nested1/" | Pesquisa recursiva de todos os arquivos e pastas sob determinado diretório | Rápido | Pesquisas de diretório até 4 diretórios serão rápidas. |
| Caminho: "/home/userX/nested1/test" | Pesquisa recursiva de todos os arquivos e pastas sob determinado caminho regex(test* pode significar ARQUIVO OU diretório OU ambos) | Mais lento | A pesquisa de regex será mais lenta em comparação com as pesquisas de diretório. |

| Expressão de filtro aplicada pelo usuário | Resultado esperado | Avaliação de desempenho | Comentário |
|---|---|---|---|
| Caminho: "/home/userX/nested1/nested2/nested3/" | Pesquisa recursiva de todos os arquivos e pastas sob determinado diretório | Mais lento | Mais de 4 buscas de diretórios são mais lentas para pesquisar. |
| Quaisquer outros filtros não baseados em caminho. Filtros de tipo de usuário e entidade recomendados para estar entre aspas, por exemplo, | | Rápido | |

NOTA:

1. A contagem de atividades exibida ao lado do ícone todas as atividades é arredondada para 30 minutos quando o intervalo de tempo selecionado se estende por mais de 3 dias. Por exemplo, um intervalo de tempo de *Set 1st 10:15 am a Set 7th 10:15 am* mostrará contagens de atividades de Set 1st 10:00 am a Sept 7th 10:30 am.
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 se estende por mais de 3 dias.

### Ordenar 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 nível 1st (raiz), pasta de nível 2nd, pasta de nível 3rd e pasta de nível 4th. Por padrão, a tabela é ordenada por ordem decrescente *time*, o que significa que os dados mais recentes serão exibidos primeiro. A ordenação está desativada para os campos *Device* e *Protocol*.

### Guia do usuário para exportações assíncronas

#### Visão geral

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

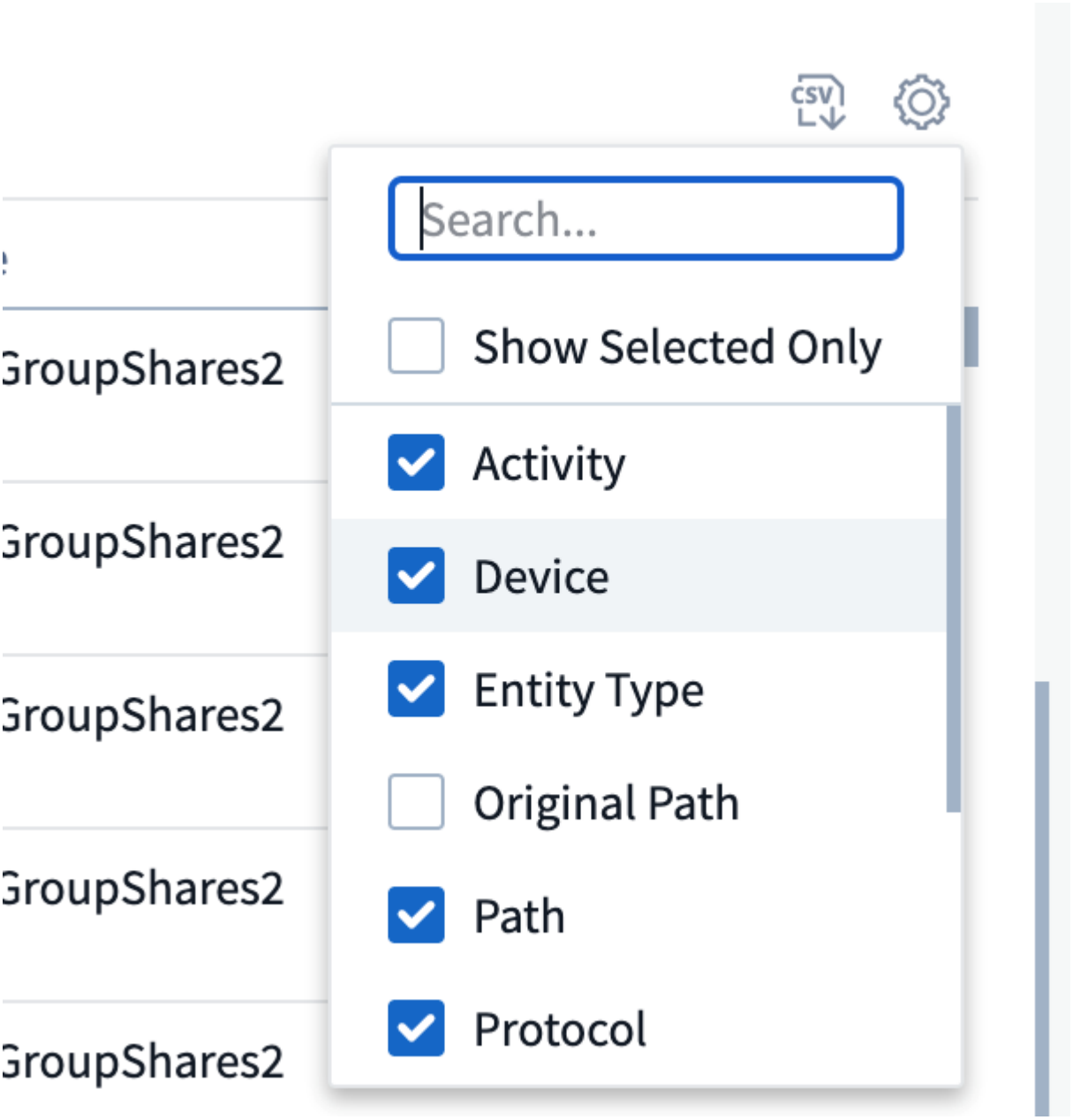
#### Guia passo a passo: Exportando dados com exportações assíncronas

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. Talvez seja necessário atualizar a página forense algumas vezes. Quando o trabalho de exportação estiver concluído, o botão "Transferir último ficheiro CSV de exportação" será ativado.
3. * Download*: Clique no botão "Download último arquivo de exportação criado" para obter os dados exportados em um formato .zip. Esses dados estarão disponíveis para download até que o usuário inicie outra exportação assíncrona ou decorram 3 dias, o que ocorrer primeiro. O botão permanecerá ativado até que outra exportação assíncrona seja iniciada.
4. **Limitações**:
   - O número de downloads assíncronos está atualmente limitado a 1 por usuário e 3 por locatário.
   - Os dados exportados estão limitados a um máximo de 1 milhões de Registros.

Um script de exemplo para extrair dados forenses via API está presente em */opt/NetApp/cloudsecure/Agent/export-script/* no agente. Consulte o readme neste local para obter mais detalhes sobre o script.

**Seleção de coluna para todas as atividades**

A tabela *all activity* mostra as 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 da atividade**

O histórico de atividades é retido por 13 meses para ambientes ativos de segurança de workload.

**Aplicabilidade dos filtros na Página Forensics**

| Filtro | O que faz | Exemplo | Aplicável a estes filtros | Não aplicável a estes filtros | Resultado |
|---|---|---|---|---|---|
| * (Asterisco) | permite-lhe procurar tudo | Auto*03172022 se o texto de pesquisa contiver hífen ou sublinhado, dê expressão entre parênteses. Por exemplo, (svm*) para pesquisar svm-123 | Usuário, tipo de entidade, dispositivo, volume, caminho original, pasta 1stLevel, pasta 2ndLevel, pasta 3rdLevel, pasta 4thLevel | | Retorna todos os recursos que começam com "Auto" e terminam com "03172022" |
| ? (ponto de interrogação) | permite-lhe procurar um número específico de carateres | AutoSabotageUser1_03172022? | Usuário, tipo de entidade, dispositivo, volume, pasta 1stLevel, pasta 2ndLevel, pasta 3rdLevel, pasta 4thLevel | | Retorna AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022B, AutoSabotageUser1_031720225 e assim por diante |
| OU | permite especificar várias entidades | AutoSabotageUser1_03172022 OR AutoRansomUser4_03162022 | Usuário, domínio, tipo de entidade, caminho original | | Retorna qualquer um de AutoSabotageUser1_03172022 OU AutoRansomUser4_03162022 |
| NÃO | permite excluir texto dos resultados da pesquisa | NOT AutoRansomUser4_03162022 | Usuário, domínio, tipo de entidade, caminho original, pasta 1stLevel, pasta 2ndLevel, pasta 3rdLevel, pasta 4thLevel | Dispositivo | Retorna tudo o que não começa com"AutoRansomUser4_03162022" |
| Nenhum | Procura valores NULL em todos os campos | Nenhum | Domínio | | retorna resultados onde o campo de destino está vazio |

**Pesquisa de caminho / caminho original**

Os resultados da pesquisa com e sem / serão diferentes

| | |
|---|---|
| "/AutoDir1/AutoFile03242022" | Somente a busca exata funciona; retorna todas as atividades com o caminho exato como /AutoDir1/AutoFile03242022 (caso insensível) |

| | |
|---|---|
| "/AutoDir1/ " | Trabalha; retorna todas as atividades com diretório de 1st níveis correspondente a AutoDir1 (caso insensível) |
| "/AutoDir1/AutoFile03242022/" | Funciona; retorna todas as atividades com diretório de 1st níveis que correspondem com diretório de AutoDir1 e 2nd níveis que correspondem com AutoFile03242022 (caso insensível) |
| /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 do SVM raiz local**

Se um usuário local root SVM estiver executando qualquer atividade, o IP do cliente no qual o compartilhamento NFS é montado agora é considerado no nome de usuário, que será mostrado como root at <ip-address-of-the-client> em ambas as páginas de atividade forense e atividade do usuário.

Por exemplo:

- Se o SVM-1 for monitorado pelo Workload Security e o usuário raiz desse SVM montar o compartilhamento em um cliente com endereço IP 10.197.12.40, o nome de usuário exibido na página de atividade forense será *root@10.197.12.40*.
- Se o mesmo SVM-1 estiver 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 raiz NFS pelo endereço IP. Anteriormente, toda a atividade foi considerada feita apenas pelo usuário *root*, sem distinção de IP.

**Solução de problemas**

| Problema | Tente isto |
|---|---|

| | |
|---|---|
| Na tabela "todas as atividades", sob a coluna "Usuário", o nome de usuário é mostrado como: "ldap:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817” ou "LDAP:default:80038003" | Possíveis razões podem ser: 1. Ainda não foram configurados coletores de diretório de utilizadores. Para adicionar um, vá para **Workload Security > Collectors > User Directory Collectors** e clique em * User Directory Collector*. Escolha *ative Directory* ou *LDAP Directory Server*. 2. Um Coletor de diretório de usuários foi configurado, no entanto ele parou ou está em estado de erro. Aceda a **Collectors > User Directory Collectors** e verifique o estado. Consulte "Solução de problemas do User Directory Collector"a seção da documentação para obter dicas de solução de problemas. Depois de configurar corretamente, o nome será resolvido automaticamente dentro de 24 horas. Se ele ainda não for resolvido, verifique se você adicionou o coletor de dados de usuário correto. Certifique-se de que o usuário faz parte do ative Directory/LDAP Directory Server adicionado. |
| Alguns eventos NFS não são vistos na IU. | Verifique o seguinte: 1. Um coletor de diretório de usuário para servidor AD com conjunto de atributos POSIX deve ser executado com o atributo unixid habilitado a partir da UI. 2. Qualquer usuário que fizer acesso NFS deve ser visto quando pesquisado na página de usuário da IU 3. Eventos brutos (Eventos para os quais o usuário ainda não foi descoberto) não são compatíveis com NFS 4. O acesso anônimo à exportação NFS não será monitorado. 5. Certifique-se de que a versão NFS usada em menos de NFS4,1. |
| Depois de digitar algumas letras contendo um caractere curinga como asterisco (*) nos filtros nas páginas Forensics *All Activity* ou *entities*, as páginas são carregadas muito lentamente. | Um asterisco (**) na cadeia de pesquisa procura tudo. No entanto, as cadeias de carateres curinga principais como <searchTerm>** ou *<*searchTerm*>* resultarão em uma consulta lenta. Para obter um melhor desempenho, use strings de prefixo no formato <*searchTerm*>* (em outras palavras, anexe o asterisco (*) *after* 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 abaixo de uma determinada pasta recursivamente (pesquisa hierárquica). Por exemplo, "/path1/path2/path3/" listará todas as atividades recursivamente em /path1/path2/path3. Alternativamente, use a opção "Adicionar ao filtro" na guia todas as atividades." |
| Estou encontrando um erro "solicitação falhou com o código de status 500/503" ao usar um filtro Path. | Tente usar um intervalo de datas menor para filtrar Registros. |
| A IU forense está carregando dados lentamente ao usar o filtro *path*. | Filtros de caminho de diretório (string de caminho terminando com /) até 4 diretórios profundos são recomendados para resultados mais rápidos. Por exemplo, se o caminho de diretório for /AAA/BBB/CCC/DDD, tente pesquisar "/AAA/BBB/CCC/DDD/" para carregar dados mais rapidamente. |

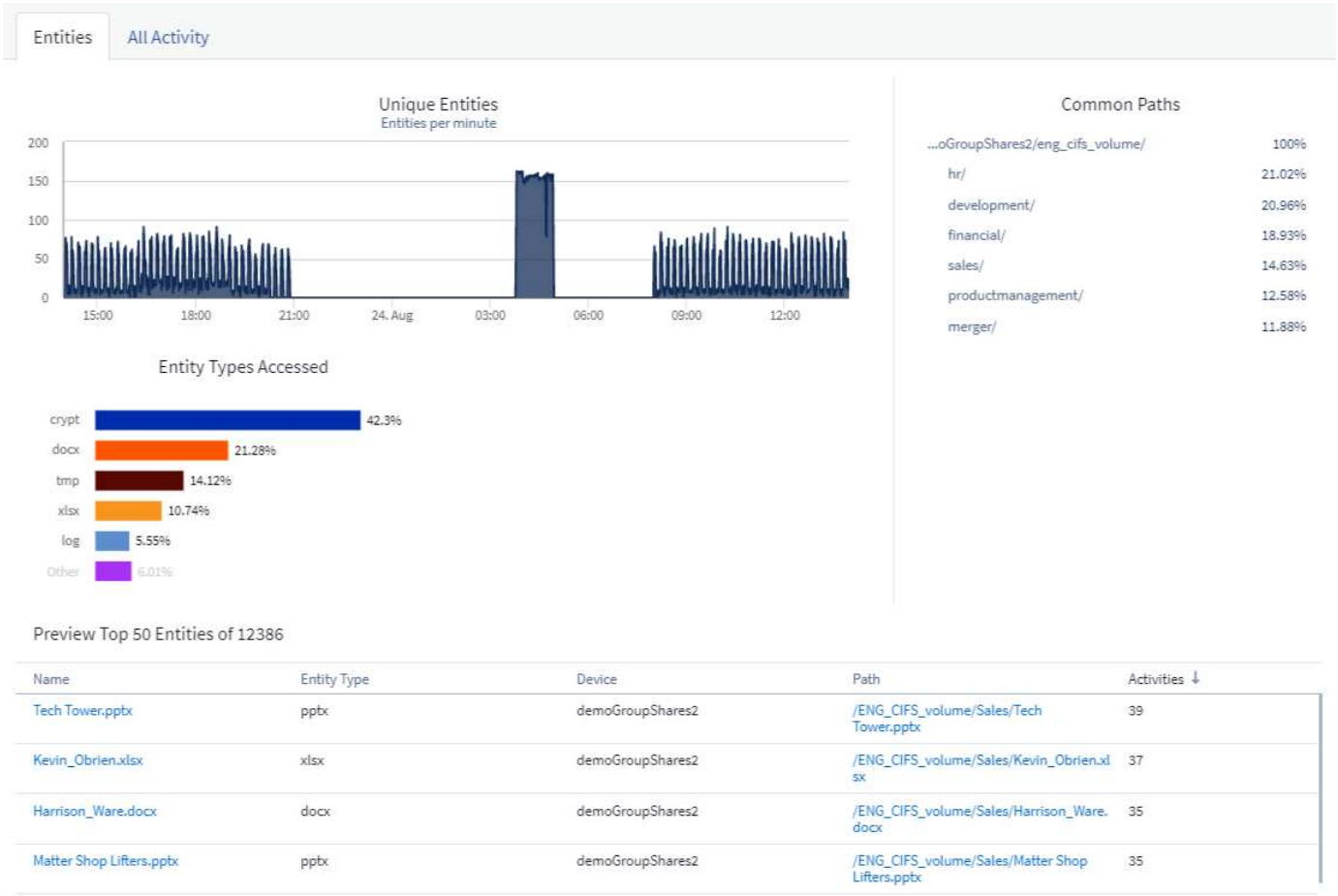
## Página de entidades forenses

A página entidades Forensics fornece informações detalhadas sobre a atividade da entidade no seu inquilino.

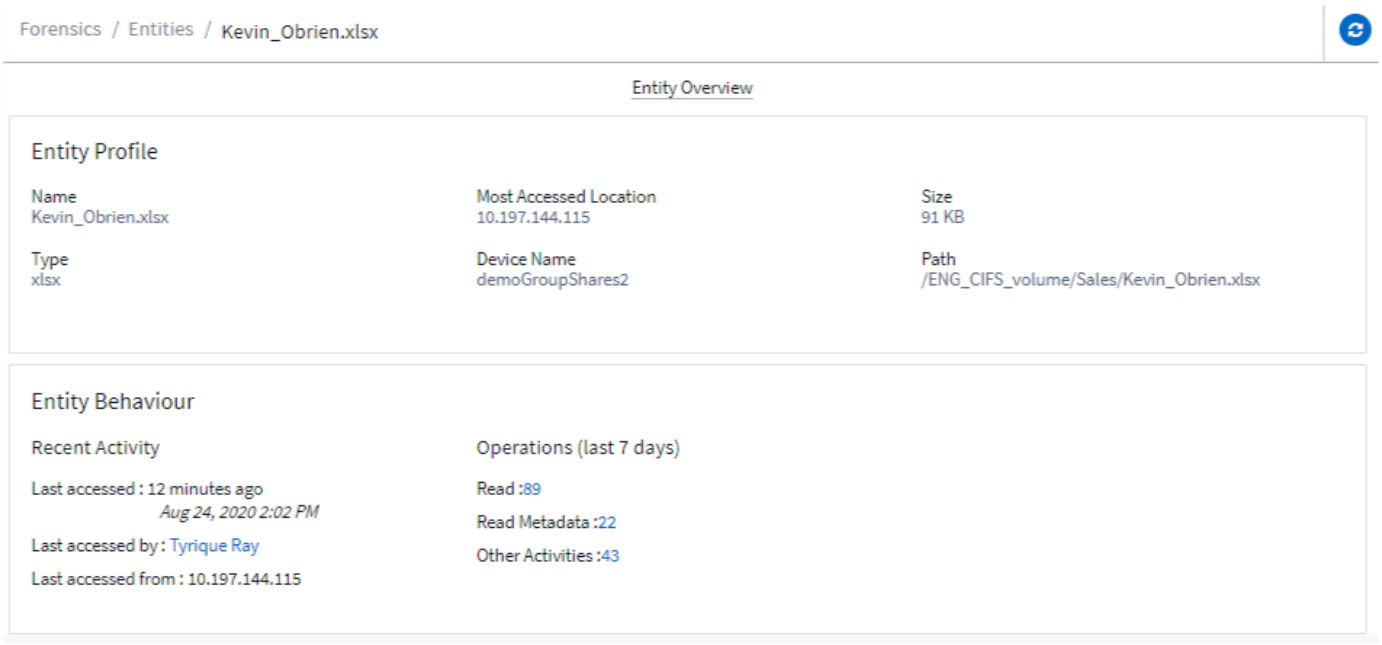
### Examinando informações da entidade

Clique em **Forensics > Activity Forensics** e clique na guia *entities* para acessar a página entidades.

Esta página fornece uma visão geral da atividade da entidade no seu inquilino, destacando as seguintes informações: * Um gráfico mostrando *entidades únicas* acessadas por minuto * Um gráfico de *tipos de entidade acessados* * um detalhamento dos *caminhos comuns* * Uma lista das *principais 50 entidades* do número total de entidades




Clicar em uma entidade na lista abre uma página de visão geral para a entidade, mostrando um perfil da entidade com detalhes como nome, tipo, nome do dispositivo, IP de localização mais acessada e caminho, bem como o comportamento da entidade, como o usuário, IP e hora em que a entidade foi acessada pela última vez.




## Visão geral do utilizador forense

As informações para cada usuário são fornecidas na Visão geral do usuário. Use essas visualizações para entender as caraterísticas do usuário, entidades associadas e atividades recentes.

### Perfil de utilizador

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

- Nome do utilizador
- Endereço de e-mail do usuário
- Gestor do utilizador
- Contacto telefónico para o utilizador
- Localização do utilizador

### Comportamento do usuário

As informações de comportamento do usuário identificam atividades e operações recentes realizadas pelo usuário. Esta informação inclui:

- Atividade recente
  - Localização do último acesso
  - Gráfico de atividade
  - Alertas
- Operações nos últimos sete dias
  - Número de operações

**Intervalo de atualização**

A lista de utilizadores é atualizada a cada 12 horas.

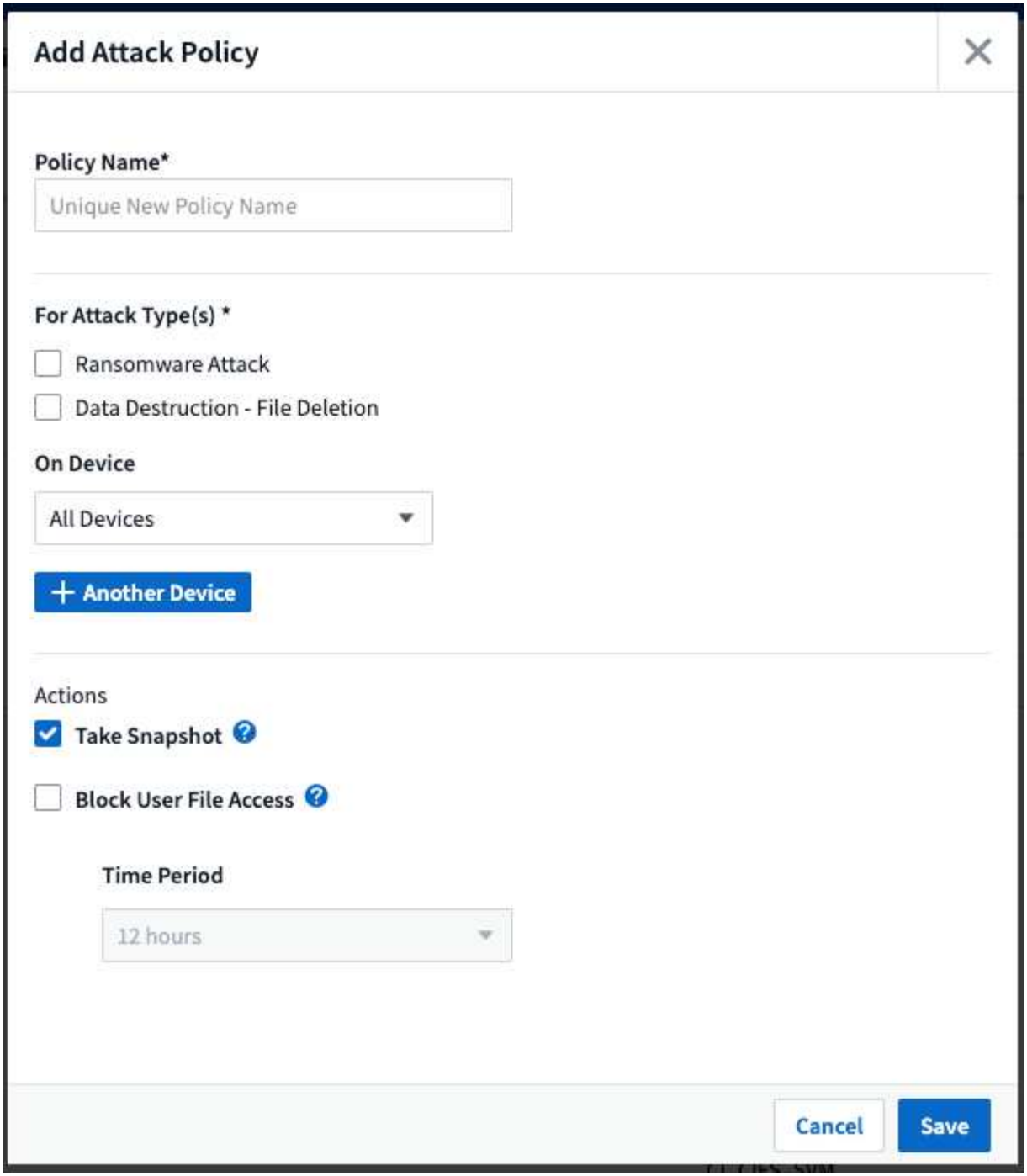
**Política de retenção**

Se não for atualizada novamente, a lista de utilizadores é mantida durante 13 meses. Após 13 meses, os dados serão apagados. Se o ambiente do Workload Security for excluído, todos os dados associados ao ambiente serão excluídos.

# Políticas de resposta automatizadas

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.

Pode definir políticas em dispositivos específicos ou em todos os dispositivos. Para definir uma política de resposta, selecione **Admin > Automated Response Policies** e clique no botão apropriado. Você pode criar políticas para ataques ou avisos.




Você deve salvar a política com um nome exclusivo.

Para desativar uma ação de resposta automatizada (por exemplo, tirar Snapshot), basta desmarcar a ação e salvar a política.

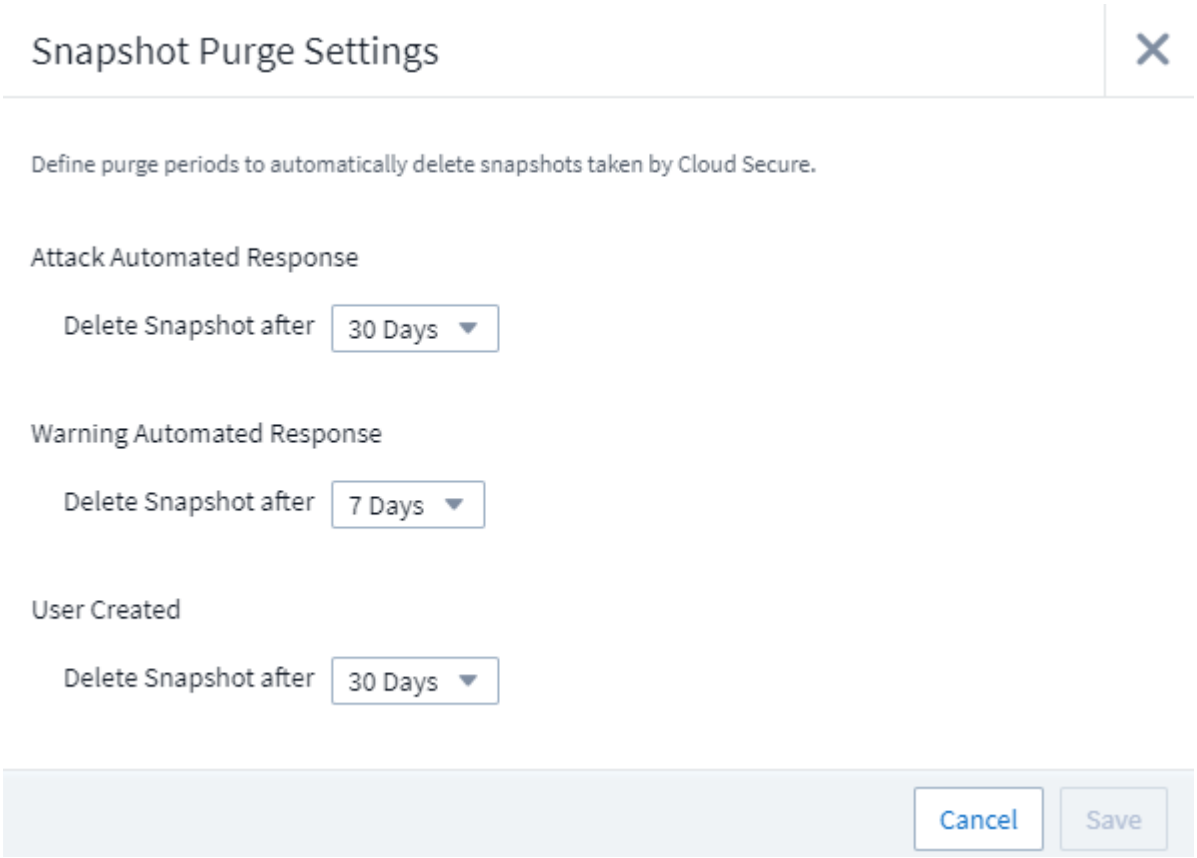
Quando um alerta é acionado contra os dispositivos especificados (ou todos os dispositivos, se selecionados), a política de resposta automática tira um instantâneo dos seus dados. Pode ver o estado do instantâneo no "Página de detalhes do alerta".

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

Você pode modificar ou pausar uma Política de resposta automatizada escolhendo a opção no menu

suspenso da política.

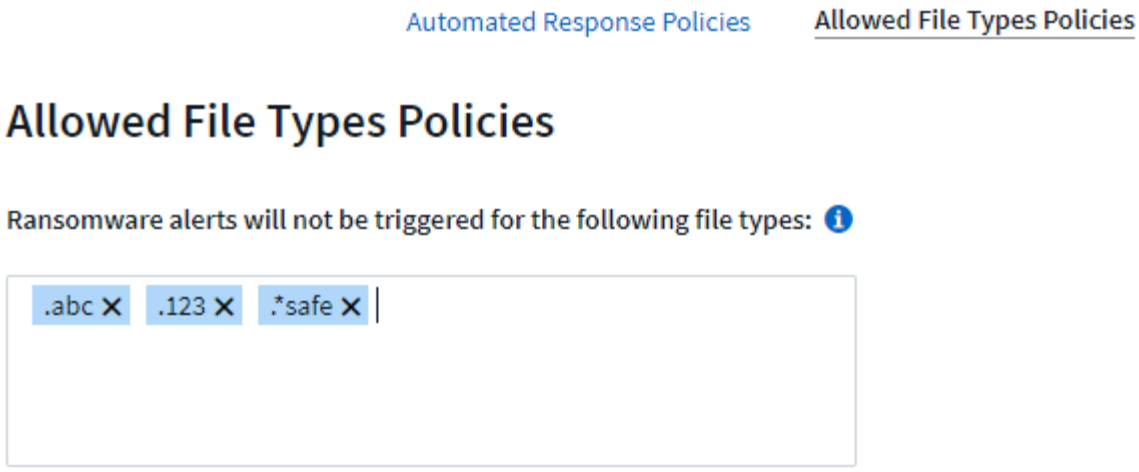
O Workload Security excluirá automaticamente os instantâneos uma vez por dia com base nas configurações de eliminação de instantâneos.




# Políticas de tipos de ficheiros permitidos

Se um ataque de ransomware for detetado para uma extensão de arquivo conhecida e alertas estiverem sendo gerados na tela Alertas, essa extensão de arquivo pode ser adicionada a uma lista *allowed file types* para evitar alertas desnecessários.

Navegue até **Workload Security > Policies** e vá para a guia *allowed File Type Policies*.




Uma vez adicionado à lista *allowed file types*, nenhum alerta de ataque de ransomware será gerado para esse tipo de arquivo permitido. Observe que a política *allowed File Types* só é aplicável para deteção de ransomware.

Por exemplo, se um arquivo chamado *test.txt* for renomeado para *test.txt.abc* e o Workload Security estiver detetando um ataque de ransomware por causa da extensão *.abc*, a extensão *.abc* pode ser adicionada à lista *allowed file types*. Depois de serem adicionados à lista, os ataques de ransomware não serão mais gerados contra arquivos com a extensão *.abc*.

Os tipos de ficheiro 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 do ONTAP

O recurso ONTAP Autonomous ransomware Protection (ARP) usa análise de workload em ambientes nas (NFS e SMB) para detectar e avisar proativamente sobre atividades anormais no arquivo que podem indicar um ataque de ransomware.

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

A segurança do workload se integra ao ONTAP para receber eventos ARP e fornece uma camada adicional de análise e respostas automáticas.

A Segurança da carga de trabalho recebe os eventos ARP do ONTAP e realiza as seguintes ações:

1. Correlaciona os 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 realizem investigações de violação de dados.
    - Identificar 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 ativados por ARP. Detalhes sobre como ativar ARP podem ser "aqui"encontrados . O ARP deve ser ativado via OnCommand System Manager. A Segurança da carga de trabalho não pode ativar o ARP.
3. O coletor de segurança de carga de trabalho deve ser adicionado via IP de cluster.
4. Credenciais de nível de cluster são necessárias para que esse recurso funcione. Em outras palavras, as credenciais no nível do cluster devem ser usadas ao adicionar o SVM.

## Permissões de usuário necessárias

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

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

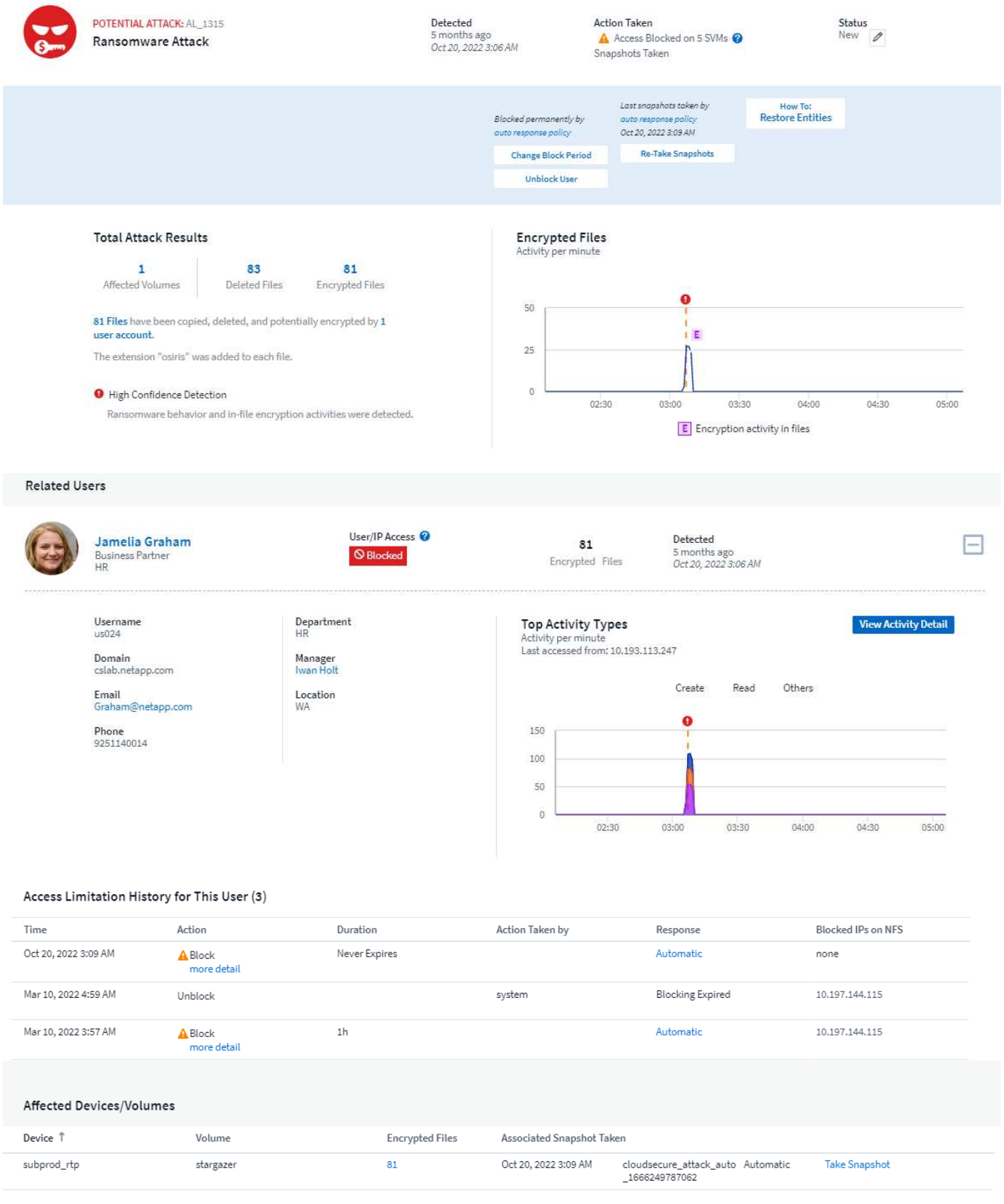
Para *csuser* com credenciais de cluster, faça o seguinte na linha de comando ONTAP:

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

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

## Alerta de amostra

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




Um banner de alta confiança indica que o ataque mostrou comportamento de ransomware, juntamente com atividades de criptografia de arquivos. O gráfico de arquivos criptografados indica o carimbo de data/hora no qual a atividade de criptografia de volume foi detetada pela solução ARP.

### Limitações

No caso de um SVM não ser monitorado pela Segurança de carga de trabalho, mas houver eventos ARP gerados pelo ONTAP, os eventos ainda serão recebidos e exibidos pela Segurança de carga de trabalho. No entanto, as informações forenses relacionadas ao alerta, bem como o mapeamento do usuário, não serão capturadas ou mostradas.

### Solução de problemas

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

| Problema: | Resolução: |
| --- | --- |
| Os alertas por e-mail são recebidos 24 horas após um ataque ser detetado. Na IU, 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 Detected* para a Segurança de carga de trabalho do Insights da infraestrutura de dados (ou seja, Segurança de carga de trabalho), o e-mail é enviado. O evento contém uma lista de ataques e seus carimbos de data/hora. A IU de Segurança do workload exibe o carimbo de data/hora do alerta do primeiro arquivo atacado. O ONTAP envia o evento *ransomware Detected* para informações de infraestrutura de dados quando um certo número de arquivos é codificado. Portanto, pode haver uma diferença entre a hora em que o alerta é exibido na IU e a hora em que o e-mail é enviado. |

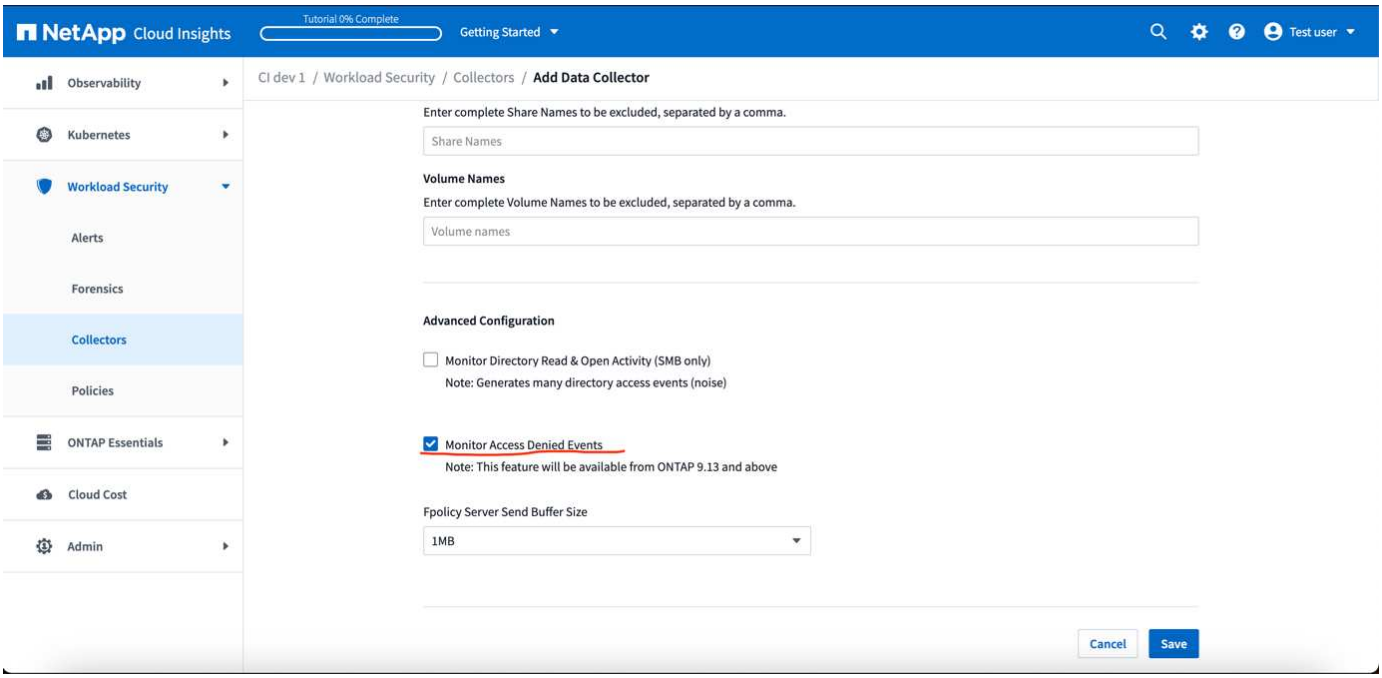
# Integração com o ONTAP Access negada

O recurso Acesso negado do ONTAP usa análise de workload em ambientes nas (NFS e SMB) para detectar e avisar proativamente sobre operações de arquivos com falha (ou seja, um usuário tentando executar uma operação para a qual não tenha permissão). Essas notificações falhadas de operação de arquivos - especialmente em casos de falhas relacionadas à segurança - ajudarão a bloquear ataques internos nos estágios iniciais.

A segurança de workload se integra ao ONTAP para receber eventos de acesso negado e fornecer uma camada de resposta automática e analítica adicional.

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, selecionando a caixa de seleção *Monitor Access Neged Events* em Configuração Avançada.




## Permissões de usuário necessárias

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

Se o Coletor for adicionado usando um usuário personalizado (por exemplo, *csuser*) com permissões dadas ao usuário, siga as etapas abaixo para dar à Segurança da carga de trabalho a permissão necessária para se Registrar para eventos de acesso negado com o ONTAP.

Para csuser com credenciais *cluster*, execute os seguintes comandos a partir da linha de comando ONTAP. Observe que *csrestrole* é função personalizada e *csuser* é usuário personalizado do ONTAP.

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

Para csuser com credenciais *SVM*, execute os seguintes comandos da linha de comando ONTAP:

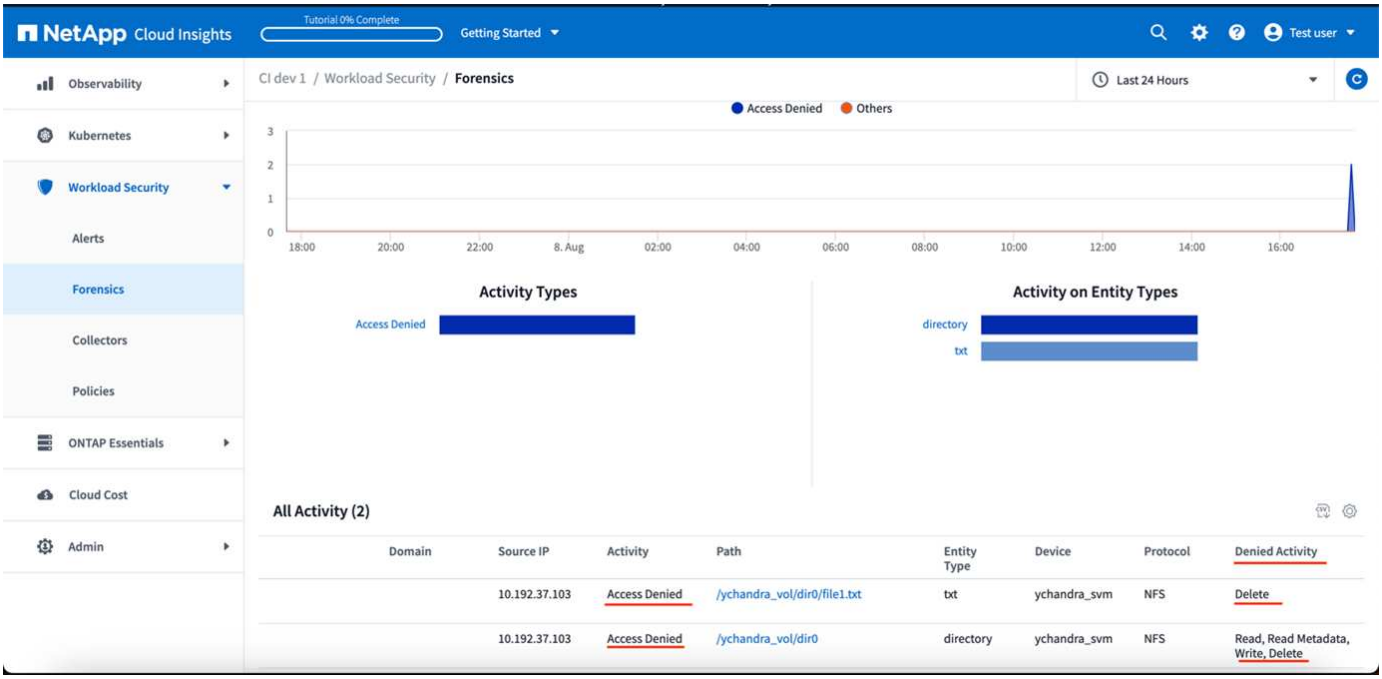
```
 security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <svm_name>
 security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole -vserver <svm_name>
```

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

## Acesso negado eventos

Uma vez que os eventos tenham sido adquiridos do sistema ONTAP, a página Forensics 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 determinada operação adicionando a coluna *atividade desejada* à tabela a partir do ícone de engrenagem.




# Bloquear o acesso do utilizador

Uma vez que um ataque é detetado, o Workload Security pode parar o ataque bloqueando o acesso do usuário ao sistema de arquivos. O acesso pode ser bloqueado automaticamente, usando políticas de resposta automatizadas ou manualmente a partir das páginas de alerta ou detalhes do usuário.

Ao bloquear o acesso do usuário, você deve definir um período de tempo de bloqueio. Após o término do período de tempo selecionado, o acesso do usuário é restaurado automaticamente. O bloqueio de acesso é compatível com protocolos SMB e NFS.

O usuário é bloqueado diretamente para SMB e o endereço IP das máquinas host, fazendo com que o ataque seja bloqueado para NFS. Esses endereços IP da 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 desses SVMs. Se o ataque tiver origem em um dos quatro SVMs, o acesso do usuário será bloqueado em todos os 10 SVMs. O Snapshot ainda é usado na SVM de origem.

Se houver quatro SVMs com um SVM configurado para SMB, um configurado para NFS e os dois restantes configurados 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 de nível de cluster são necessárias para que esse recurso funcione.

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

Se você estiver usando um usuário personalizado (por exemplo, *csuser*) com permissões dadas ao usuário, siga as etapas abaixo para conceder permissões ao Workload Security para bloquear o usuário.

Para csuser com credenciais de cluster, faça o seguinte na linha de comando 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
```

Certifique-se de rever a seção permissões da "Configurando o coletor de dados SVM do ONTAP"página também.

## Como ativar a funcionalidade?

- Em Workload Security, navegue até **Workload Security > Policies > Automated Response Policies**. Escolha * Política de ataque *.
- Selecione (marque) *Bloquear Acesso ao Arquivo de Usuário*.

## Como configurar o bloqueio de acesso automático do usuário?

- 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 verificação "Bloquear acesso ao ficheiro do utilizador". A funcionalidade será ativada quando esta for selecionada.
- Em "período de tempo", selecione o tempo até o qual o bloqueio deve ser aplicado.
- Para testar o bloqueio automático do usuário, você pode simular um ataque por meio de um "script simulado".

## Como saber se existem utilizadores bloqueados no sistema?

- Na página listas de alertas, um banner na parte superior da tela será exibido no caso de qualquer usuário ser bloqueado.
- Clicar no banner irá levá-lo para a página "usuários", onde a lista de usuários bloqueados pode ser vista.
- Na página "usuários", há uma coluna chamada "Usuário/Acesso IP". Nessa coluna, o estado atual de bloqueio do usuário será exibido.

## Restringir e gerenciar o acesso do usuário manualmente

- Pode aceder ao ecrã de detalhes de alerta ou de detalhes do utilizador e, em seguida, bloquear ou restaurar manualmente um utilizador a partir desses ecrãs.

## Histórico de limitação de acesso do utilizador

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

## Como desativar a funcionalidade?

A qualquer momento, você pode desativar o recurso. Se houver usuários restritos no sistema, você deve restaurar o acesso deles primeiro.

- Em Workload Security, navegue até **Workload Security > Policies > Automated Response Policies**. Escolha * Política de ataque *.
- Desmarque (desmarque) *Bloquear acesso ao ficheiro do utilizador*.

O recurso ficará oculto de todas as páginas.

## Restaure manualmente IPs para NFS

Siga as etapas a seguir para restaurar manualmente qualquer IPs do ONTAP se a avaliação de Segurança de carga de trabalho 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 de todas as políticas no SVM que têm "cloudsecure_rule" como correspondência do cliente especificando seu respetivo RuleIndex. Regra de Segurança da carga de trabalho geralmente será em 1.

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

```
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.
```

## Restaure manualmente os usuários para SMB

Siga as etapas a seguir para restaurar manualmente qualquer usuário do ONTAP se a avaliação de Segurança de carga de trabalho expirar ou se o agente/coletor estiver inativo.

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

1. Faça login no cluster do ONTAP (onde você deseja desbloquear usuários) com credenciais *admin* do cluster. (Para o Amazon FSX, faça login com credenciais FSX).
2. Execute o seguinte comando para listar todos os usuários bloqueados pelo Workload Security para SMB em todos os 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. Uma vez que identificamos a posição da 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 | Tente isto |
|---|---|
| Alguns dos usuários não estão ficando restritos, embora haja um ataque. | 1. Certifique-se de que o coletor de dados e o agente das SVMs estejam no estado *Running*. A Segurança da carga de trabalho não poderá enviar comandos se o Coletor de dados e o Agente 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 acontece através do endereço IP do host através do qual o usuário está acessando o armazenamento. Verifique na IU (Detalhes de alerta > Histórico de limitação de acesso para este utilizador > IPs afetados) a lista de endereços IP 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 a partir dos hosts cujos IPs são restritos, o armazenamento não estará acessível. |
| Clicar manualmente em restringir acesso dá "endereços IP deste usuário já foram restritos". | O IP a ser restrito já está sendo restringido de outro usuário. |
| Não foi possível modificar a política. Motivo: Não autorizado para esse comando. | Verifique se usando csuser, as permissões são dadas ao usuário como mencionado acima. |
| O bloqueio de usuário (endereço IP) para NFS funciona, mas para SMB / CIFS, vejo uma mensagem de erro: "SID para transformação DomainName falhou. Tempo limite da razão: O soquete não está estabelecido" | Isso pode acontecer é *csuser* não tem permissão para executar ssh. (Assegure a conexão no nível do cluster e, em seguida, certifique-se de que o usuário pode executar ssh). *csuser* função 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 a partir da linha de comando ONTAP: Security login role create -role csrole -cmddirname "vserver export-policy rule" -access all security login role ONTAP |

| Problema | Tente isto |
| --- | --- |
| Estou recebendo a mensagem de erro *SID translate failed. reason:255:Error: Command failed: Not Authorized for that commandError: "Access-check" não é um comando reconhecido*, quando um usuário deve ter sido bloqueado. | Isso pode acontecer quando *csuser* não tem permissões corretas. Consulte "Pré-requisitos para bloqueio de acesso do usuário" para obter mais informações. Depois de aplicar as permissões, é recomendável reiniciar o coletor de dados do ONTAP e o coletor de dados do diretório do usuário. Os comandos de permissão necessários estão listados abaixo. ---- função de login de segurança criar -role csrole -cmddirname "vserver export-policy rule" -access all security login role create -role csrole -cmddirname set -access all security login role create -rule csrole -csrole -csname -csname -csname- |

# Segurança da carga de trabalho: Simulando um ataque

Você pode usar as instruções nesta página para simular um ataque para testar ou demonstrar o Workload Security usando o script de simulação de ransomware incluído.

## Coisas a observar antes de começar

- O script de simulação de ransomware funciona apenas no Linux.
- O script é fornecido com os arquivos de instalação do agente Workload Security. Ele está disponível em qualquer máquina que tenha um agente Workload Security instalado.
- Você pode executar o script na própria máquina do agente Workload Security; não há necessidade de preparar outra máquina Linux. No entanto, se você preferir executar o script em outro sistema, basta copiar o script e executá-lo lá.

## Tenha pelo menos 1.000 arquivos de amostra

Esse script deve ser executado em uma SVM com uma pasta que tenha arquivos para criptografar. Recomendamos ter pelo menos 1.000 arquivos dentro dessa pasta e quaisquer subpastas. Os ficheiros não podem estar vazios. Não crie os arquivos e criptografe-os usando o mesmo usuário. O Workload Security considera esta uma atividade de baixo risco e, portanto, não gera um alerta (ou seja, o mesmo usuário modifica os arquivos que ele/ela/eles acabaram de criar).

Veja abaixo as instruções para "crie arquivos não vazios programaticamente".

## Diretrizes antes de executar o simulador:

1. Certifique-se de que os ficheiros encriptados não estão vazios.
2. Certifique-se de encriptar > 50 ficheiros. Um pequeno número de arquivos será ignorado.
3. Não execute um ataque com o mesmo usuário várias vezes. Depois de algumas vezes, o Workload Security vai aprender esse comportamento do usuário e assumir que é o comportamento normal do usuário.
4. Não criptografe arquivos que o mesmo usuário acabou de criar. Alterar um arquivo que acabou de ser criado por um usuário não é considerado uma atividade arriscada. Em vez disso, use arquivos criados por outro usuário OU aguarde algumas horas entre a criação dos arquivos e a criptografia.

## Prepare o sistema

Primeiro, monte o volume alvo na máquina. Você pode montar uma montagem NFS ou exportação 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 CIFS no Linux:

```
 mount -t cifs //10.193.77.91/sharedfolderincluster
/root/destinationfolder/ -o username=raisa
Em seguida, configure um Data Collector:
```

1. Configure o agente Workload Security se ainda não tiver sido feito.
2. Configurar o coletor de dados SVM, se ainda não tiver feito.

## Execute o script ransomware Simulator

1. Faça login (ssh) na máquina do agente Workload Security.
2. Navegue para: */opt/NetApp/cloudsecure/Agent/install*
3. Chame o script do simulador sem parâmetros para ver o uso:

```
# pwd
/opt/netapp/cloudsecure/agent/install
# ./ransomware_simulator.sh
Error: Invalid directory  provided.
Usage: ./ransomware_simulator.sh [-e] [-d] [-i <input_directory>]
       -e to encrypt files (default)
       -d to restore files
       -i <input_directory> - Files under the directory to be encrypted
```

```
Encrypt command example: ./ransomware_simulator.sh -e -i
/mnt/audit/reports/
Decrypt command example: ./ransomware_simulator.sh -d -i
/mnt/audit/reports/
```

## Criptografe seus arquivos de teste

Para criptografar os arquivos, execute o seguinte comando:

```
# ./ransomware_simulator.sh -e -i /root/for/
Encryption key is saved in /opt/netapp/cloudsecure/cloudsecure-agent-
1.251.0/install/encryption-key,
which can be used for restoring the files.
Encrypted /root/for/File000.txt
Encrypted /root/for/File001.txt
Encrypted /root/for/File002.txt
...
```

## Restaurar ficheiros

Para descriptografar, execute o seguinte comando:

```
[root@scspa2527575001 install]# ./ransomware_simulator.sh -d -i /root/for/
File /root/for/File000.txt is restored.
File /root/for/File001.txt is restored.
File /root/for/File002.txt is restored.
...
```

## Execute o script várias vezes

Depois de gerar um ataque de ransomware para um usuário, mude para outro usuário para gerar um ataque adicional. O Workload Security aprende o comportamento do usuário e não alerta sobre ataques repetidos de ransomware em um curto período para o mesmo usuário.

## Crie arquivos programaticamente

Antes de criar os arquivos, você deve primeiro parar ou pausar o processamento do coletor de dados. Execute as etapas abaixo antes de adicionar o coletor de dados ao Agente. Se você já adicionou o coletor de dados, basta editar o coletor de dados, inserir uma senha inválida e salvá-la. Isso colocará temporariamente o coletor de dados no estado de erro. Nota: Certifique-se de anotar a palavra-passe original!

A opção recomendada é "pausar o coletor" antes de criar seus arquivos.]

Antes de executar a simulação, você deve primeiro adicionar arquivos para serem criptografados. Você pode copiar manualmente os arquivos a serem criptografados na pasta de destino ou usar um script (veja o exemplo abaixo) para criar programaticamente os arquivos. Qualquer que seja o método utilizado, copie pelo menos 1.000 ficheiros.

Se você optar por criar programaticamente os arquivos, faça o seguinte:

1. Faça login na caixa Agente.
2. Montar uma exportação NFS do SVM do arquivador para a máquina Agent. CD para essa pasta.

3. Nessa pasta, crie um arquivo chamado createfiles.sh
4. Copie as linhas a seguir para esse arquivo.

```
for i in {000..1000}
do
   echo hello > "File${i}.txt"
done
echo 3 > /proc/sys/vm/drop_caches ; sync
```

5. Salve o arquivo.
6. Certifique-se de executar permissão no arquivo:

```
 chmod 777 ./createfiles.sh
. Execute o script:
```

```
./createfiles.sh
```

os ficheiros 1000 serão criados na pasta atual.

7. Reative o coletor de dados

   Se você desativou o coletor de dados na etapa 1, edite o coletor de dados, insira a senha correta e salve. Certifique-se de que o coletor de dados está de volta no estado em execução.

8. Se você fez uma pausa no coletor antes de seguir estas etapas, certifique-se "retomar o coletor"de .

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

Para configurar os destinatários do alerta de segurança do Workload, clique em **Admin > notificações** e insira um endereço de e-mail na(s) seção(s) apropriada(s) para cada destinatário.

## Alertas e avisos de ataque potenciais

Para enviar notificações de alerta *potencial ataque*, insira os endereços de e-mail dos destinatários na seção *Enviar alertas de ataque potencial*. As notificações por e-mail são enviadas para a lista de destinatários de alerta para cada ação no alerta.

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

## Monitoramento de integridade do agente e coletor de dados

Você pode monitorar a integridade de agentes e fontes de dados por meio de notificações.

Para receber notificações no caso de um agente ou coletor de fonte de dados não funcionar, 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 integridade serão enviados somente depois que o agente/coletor parar de informar por pelo menos uma hora.
- Somente uma notificação por e-mail é enviada aos destinatários pretendidos em um determinado período de 24 horas, mesmo que o Agente ou coletor de dados esteja desconetado por uma duração maior.
- Em caso de falha do Agente, um alerta será enviado (não um por coletor). O e-mail incluirá uma lista de todos os SVMs impactados.
- A falha de coleta de diretório ativo é relatada como um aviso; ela não afeta a deteção de ransomware.
- A lista de configuração Introdução agora inclui uma nova fase *Configurar notificações por e-mail*.

### Recebendo notificações de atualização de Agente e Coletor de dados

- Insira o(s) ID(s) de e-mail nos "Alertas de integridade da coleta de dados".
- A caixa de verificação "Ativar notificações de atualização" torna-se ativada.
- As notificações de 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: | Tente isto: |
| --- | --- |
| Os IDs de e-mail estão presentes nos "Alertas de integridade do coletor de dados", no entanto, não estou recebendo notificações. | Os e-mails de notificação são enviados a partir do domínio de informações de infraestrutura de dados da NetApp, ou seja, a partir de [[cloudinsights.NetApp.com_]. Algumas empresas bloqueiam e-mails recebidos se forem de um domínio externo. Certifique-se de que as notificações externas dos domínios do Insights da infraestrutura de dados do NetApp estejam na lista branca. |

# API de segurança de carga de trabalho

A API de segurança de carga de trabalho permite que clientes da NetApp e fornecedores de software independentes (ISVs) integrem a segurança de carga de trabalho com outros aplicativos, como CMDB ou outros sistemas de emissão de tíquetes.

Requisitos para acesso à API:

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

### Documentação da API (Swagger)

As informações mais recentes da API são encontradas efetuando login no Workload Security e navegando até

**Admin > API Access**. Clique no link **Documentação da API**. A Documentação da API é baseada no Swagger, que fornece uma breve descrição e informações de uso para a API e permite que você experimente no seu locatário.

Ao chamar a API de atividade Forensics, use a API cloudsecure_forensics.Activities.**v2** API. Se você estiver fazendo várias chamadas para essa API, verifique se as chamadas ocorrem sequencialmente, não em paralelo. Várias chamadas paralelas podem fazer com que a API termine o tempo limite.

## Tokens de acesso à API

Antes de usar a API Workload Security, 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 para cada token de acesso.

Para criar um token de acesso:

- Clique em **Admin > API Access**
- Clique em * API Access Token*
- Digite **Nome do Token**
- Especifique **validade do token**

Seu token só estará disponível para copiar para a área de transferência e salvar durante o processo de criação. Os tokens não podem ser recuperados depois que são 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 de token.

Você pode desativar, ativar e revogar tokens. Os tokens que estão desativados podem ser ativados.

Os tokens concedem acesso de propósito geral às APIs da perspetiva 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 êxito e 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 que foi 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://<tenant_host_name>/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.
```

Informações detalhadas podem ser encontradas no link *API Documentation* em **Admin > API Access**.

## Script para extrair dados através da API

Os agentes de segurança de carga de trabalho incluem um script de exportação para facilitar chamadas paralelas para a 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 comando de exemplo para invocar o script:

```
python3 data-export.py --tenant_url <tenant
id>.cs01.cloudinsights.netapp.com --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-chave: - `--iteration_interval 12`: Divide o intervalo de tempo solicitado em intervalos de 12 horas. - `--num_workers 3`: Fetches esses intervalos em paralelo usando 3 threads.

## Informações sobre direitos autorais



## Informações sobre marcas comerciais