Forense

Data Infrastructure Insights

NetApp
February 03, 2026

Índice

Forense

Forense - Todas as atividades

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

Examinando todos os dados de atividade

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

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

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

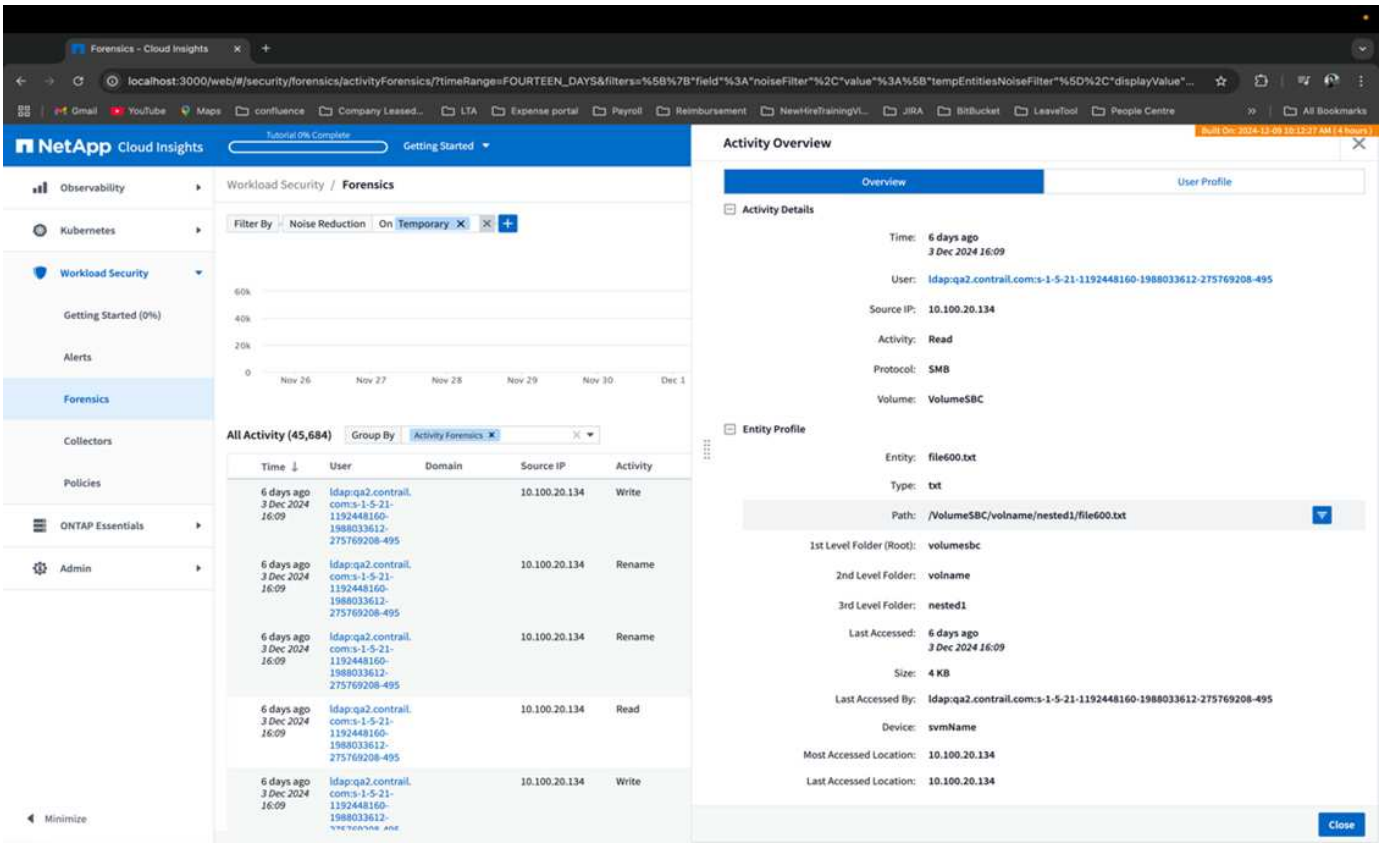
- Uma lista de dados de *Todas as atividades*.
- Um grupo suspenso fornecerá a opção de agrupar a atividade por usuários, pastas, tipo de entidade, etc.
- Um botão de caminho comum estará disponível acima da tabela. Ao clicar nele, podemos obter um painel deslizante com detalhes do caminho da entidade.

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

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

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

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



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

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

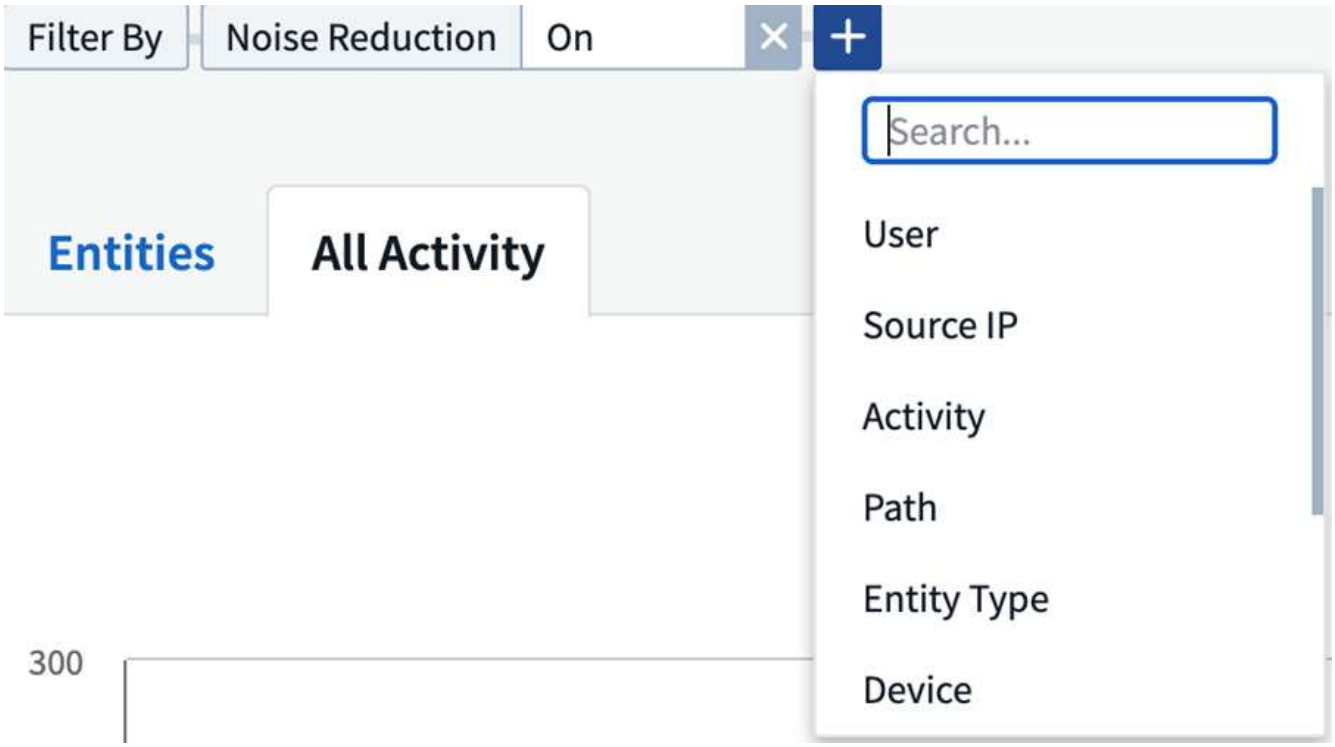
- A contagem de atividades é exibida como um hiperlink; selecionar isso adicionará o agrupamento selecionado como um filtro. A tabela de atividades será atualizada com base nesse filtro.
- Observe que se você alterar o filtro, alterar o intervalo de tempo ou atualizar a tela, não poderá retornar aos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

Filtrando dados do histórico de atividades forenses

Há dois métodos que você pode usar para filtrar dados.

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

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



  Digite o texto de pesquisa

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

Você pode filtrar dados de atividade forense pelos seguintes campos:

- O tipo **Atividade**.
- **Protocolo** para buscar atividades específicas do protocolo.
- **Nome de usuário** do usuário que está realizando a atividade. Você precisa fornecer o nome de usuário

exato para filtrar. Pesquisar com nome de usuário parcial ou nome de usuário parcial prefixado ou sufixado com '*' não funcionará.

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

Os seguintes campos estão sujeitos a regras especiais de filtragem:

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

Os campos anteriores estão sujeitos ao seguinte ao filtrar:

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

contenha 'searchtext'.

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

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

Exemplos de filtros de atividade forense:

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

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

OBSERVAÇÃO:

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

Classificando dados do histórico de atividades forenses

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

Guia do usuário para exportações assíncronas

Visão geral

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

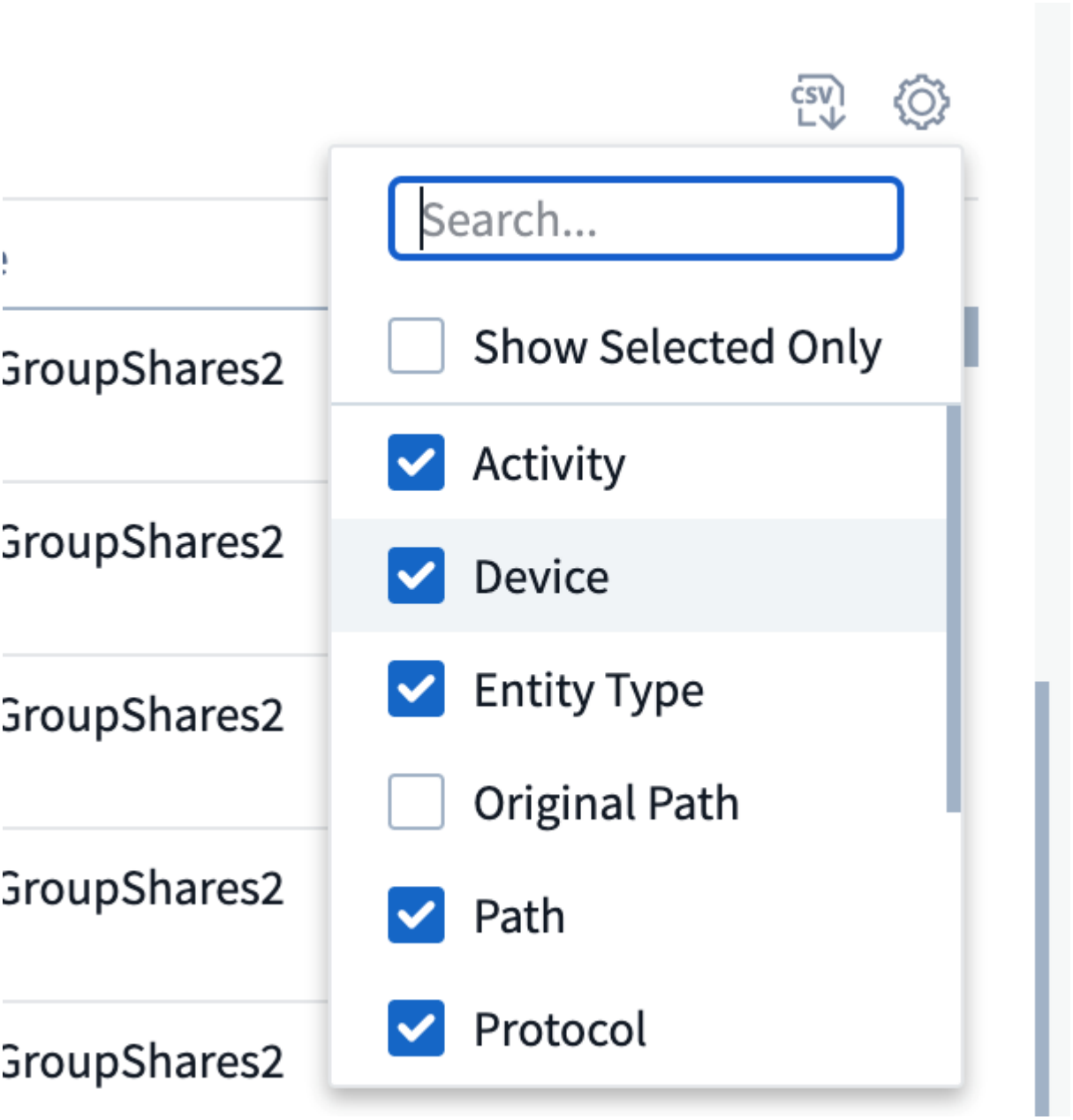
Guia passo a passo: Exportando dados com exportações assíncronas

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

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

Seleção de colunas para todas as atividades

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



Retenção do histórico de atividades

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

Aplicabilidade de Filtros em Perícia Forense

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

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

Busca de Caminho

Os resultados da pesquisa com e sem / serão diferentes

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

Alterações na atividade do usuário raiz SVM local

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

Por exemplo:

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

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

Solução de problemas

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

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

Visão geral do usuário forense

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

Perfil do usuário

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

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

Comportamento do usuário

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

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

Intervalo de atualização

A lista de usuários é atualizada a cada 12 horas.

Política de retenção

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

Informações sobre direitos autorais

Informações sobre marcas comerciais