



## **Forense**

### Data Infrastructure Insights

NetApp  
January 10, 2025

# Índice

- Forense ..... 1
  - Forensics - todas as atividades ..... 1
  - Página de entidades forenses ..... 10
  - Visão geral do utilizador forense ..... 11

# 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 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.

The screenshot displays the NetApp Cloud Insights interface for Forensics. The main view shows a table of activity with columns for Time, User, Domain, Source IP, and Activity. The activity is grouped by 'Activity Forensics'. A detailed view of an activity is shown on the right, including 'Activity Details' and 'Entity Profile'.

Time	User	Domain	Source IP	Activity
6 days ago 3 Dec 2024 16:09	ldap:qa2.contrail.coms-1-5-21-1192448160-1988033612-275769208-495		10.100.20.134	Write
6 days ago 3 Dec 2024 16:09	ldap:qa2.contrail.coms-1-5-21-1192448160-1988033612-275769208-495		10.100.20.134	Rename
6 days ago 3 Dec 2024 16:09	ldap:qa2.contrail.coms-1-5-21-1192448160-1988033612-275769208-495		10.100.20.134	Rename
6 days ago 3 Dec 2024 16:09	ldap:qa2.contrail.coms-1-5-21-1192448160-1988033612-275769208-495		10.100.20.134	Read
6 days ago 3 Dec 2024 16:09	ldap:qa2.contrail.coms-1-5-21-1192448160-1988033612-275769208-495		10.100.20.134	Write

**Activity Details:**

- Time: 6 days ago  
3 Dec 2024 16:09
- User: ldap:qa2.contrail.coms-1-5-21-1192448160-1988033612-275769208-495
- Source IP: 10.100.20.134
- Activity: Read
- Protocol: SMB
- Volume: VolumeSBC

**Entity Profile:**

- Entity: file600.txt
- Type: txt
- Path: /VolumeSBC/volname/nested1/file600.txt
- 1st Level Folder (Root): volumesbc
- 2nd Level Folder: volname
- 3rd Level Folder: nested1
- Last Accessed: 6 days ago  
3 Dec 2024 16:09
- Size: 4 KB
- Last Accessed By: ldap:qa2.contrail.coms-1-5-21-1192448160-1988033612-275769208-495
- Device: svmName
- Most Accessed Location: 10.100.20.134
- Last Accessed Location: 10.100.20.134

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.

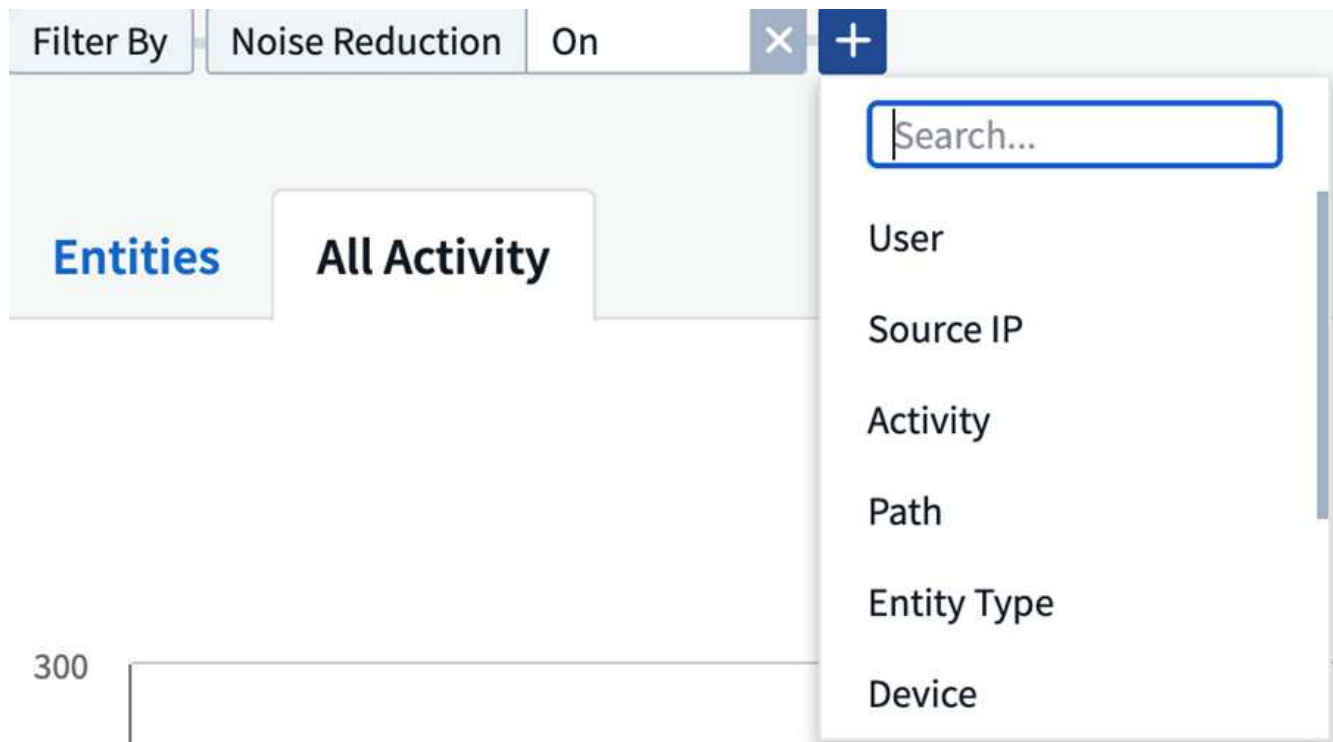
- A contagem de atividades é apresentada como uma hiperligação; selecionar esta opção irá adicionar o agrupamento selecionado como um filtro. A tabela de atividade será atualizada com base nesse filtro.
- Observe que se você alterar o filtro, alterar o intervalo de tempo ou atualizar a tela, não será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

Expressão de filtro aplicada pelo usuário	Resultado esperado	Avaliação de desempenho	Comentário
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.
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.

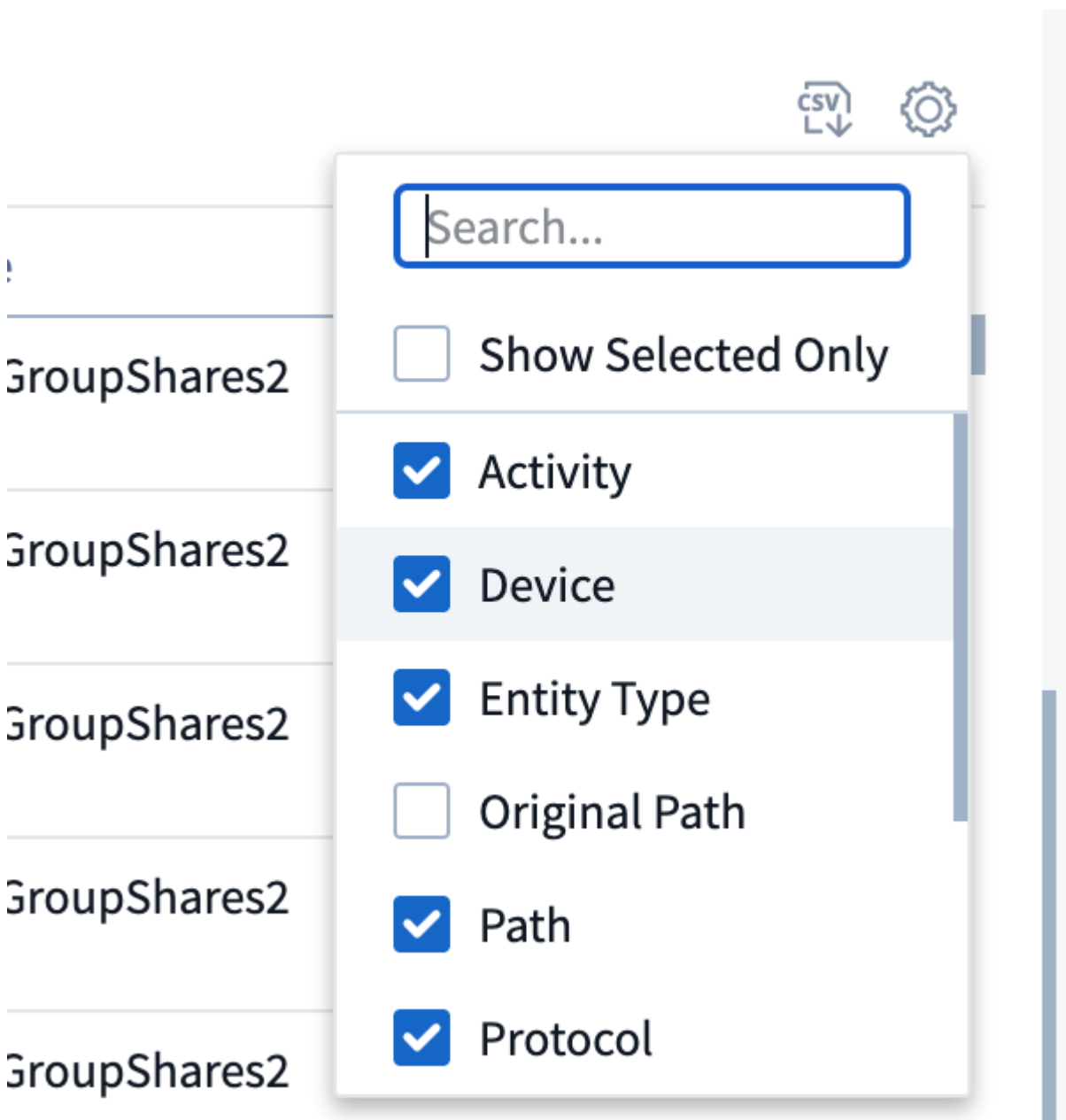
#### 4. Limitações:

- 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.



The image shows a table with five rows, each labeled 'GroupShares2'. To the right of the table is a settings menu. At the top of the menu are icons for 'CSV' (a document with a download arrow) and a gear. Below these is a search bar containing the text 'Search...'. The menu contains a list of columns with checkboxes:

- Show Selected Only
- Activity
- Device
- Entity Type
- Original Path
- Path
- Protocol



## 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 caracteres	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
----------	------------

<p>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"</p>	<p>Possíveis razões podem ser: 1. Ainda não foram configurados coletores de diretório de utilizadores. Para adicionar um, vá para <b>Workload Security &gt; Collectors &gt; User Directory Collectors</b> e clique em * User Directory Collector*. Escolha <i>ative Directory</i> ou <i>LDAP Directory Server</i>. 2. Um Coletor de diretório de usuários foi configurado, no entanto ele parou ou está em estado de erro. Aceda a <b>Collectors &gt; User Directory Collectors</b> e verifique o estado. Consulte "<a href="#">Solução de problemas do User Directory Collector</a>"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.</p>
<p>Alguns eventos NFS não são vistos na IU.</p>	<p>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.</p>
<p>Depois de digitar algumas letras contendo um caractere curinga como asterisco (*) nos filtros nas páginas Forensics <i>All Activity</i> ou <i>entities</i>, as páginas são carregadas muito lentamente.</p>	<p>Um asterisco () <b>na cadeia de pesquisa procura tudo. No entanto, as cadeias de caracteres curinga principais como &lt;searchTerm&gt; ou *&lt;searchTerm&gt;*</b> resultarão em uma consulta lenta. Para obter um melhor desempenho, use strings de prefixo no formato &lt;searchTerm&gt;* (em outras palavras, anexe o asterisco (*) <i>after</i> um termo de pesquisa). Exemplo: Use a string <i>testvolume*</i>, em vez de <i>*testvolume</i> ou <i>*test*volume</i>. Use uma pesquisa de diretório para ver todas as atividades abaixo de uma determinada pasta recursivamente (pesquisa hierárquica). Por exemplo, <i>/path1/path2/path3/</i> listará todas as atividades recursivamente em <i>/path1/path2/path3</i>. Alternativamente, use a opção "Adicionar ao filtro" na guia todas as atividades."</p>
<p>Estou encontrando um erro "solicitação falhou com o código de status 500/503" ao usar um filtro Path.</p>	<p>Tente usar um intervalo de datas menor para filtrar Registros.</p>
<p>A IU forense está carregando dados lentamente ao usar o filtro <i>path</i>.</p>	<p>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 <i>/AAA/BBB/CCC/DDD</i>, tente pesquisar <i>/AAA/BBB/CCC/DDD/</i> para carregar dados mais rapidamente.</p>

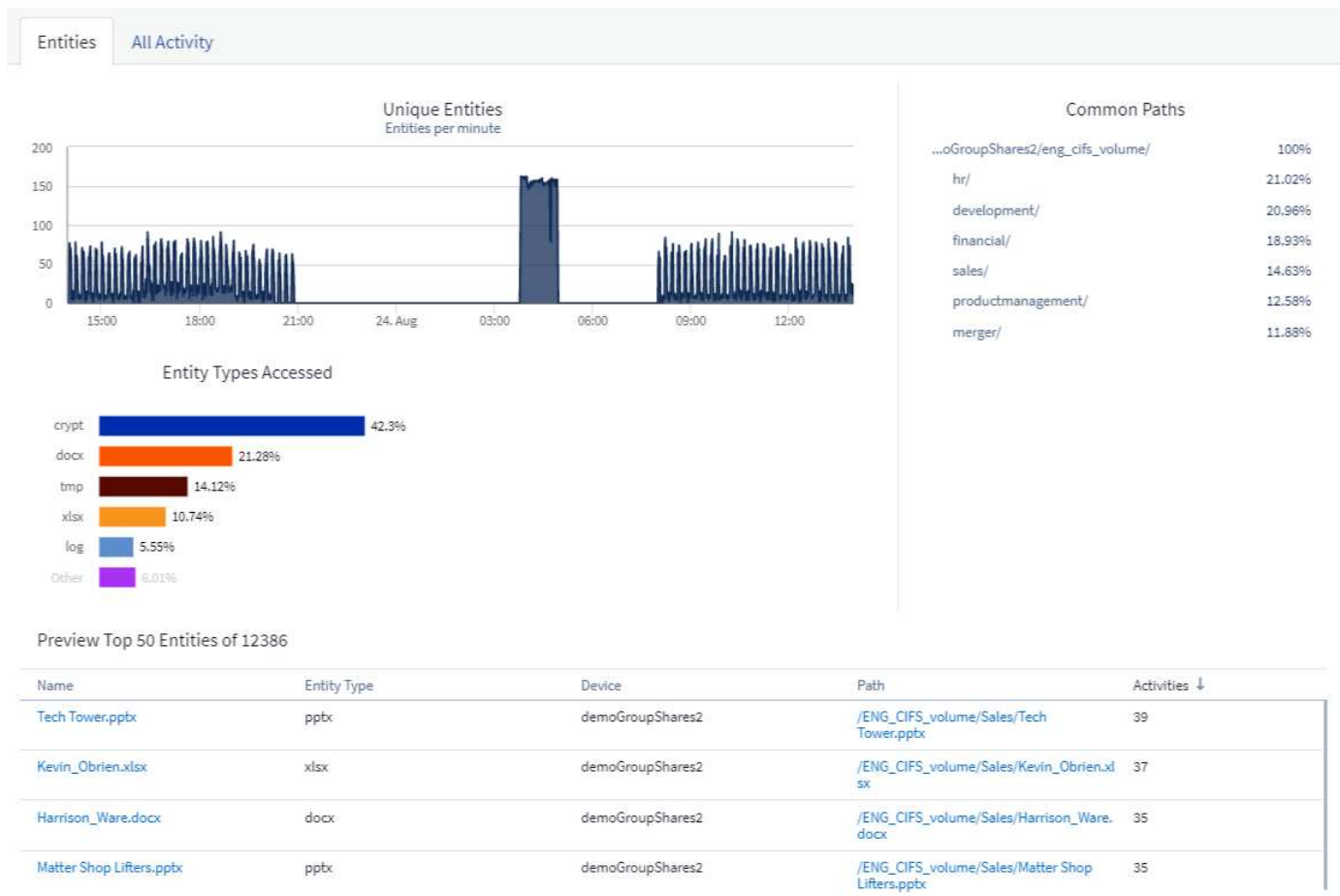
# Página de entidades forenses

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.

## Entity Overview

## Entity Profile

Name Kevin_Obrien.xlsx	Most Accessed Location 10.197.144.115	Size 91 KB
Type xlsx	Device Name demoGroupShares2	Path /ENG_CIFS_volume/Sales/Kevin_Obrien.xlsx

## Entity Behaviour

Recent Activity	Operations (last 7 days)
Last accessed : 12 minutes ago <i>Aug 24, 2020 2:02 PM</i>	Read :89
Last accessed by: <a href="#">Tyrique Ray</a>	Read Metadata :22
Last accessed from : 10.197.144.115	Other Activities :43

## Visão geral do utilizador forense

As 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 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.

## **Informações sobre direitos autorais**

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

## **Informações sobre marcas comerciais**

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.