Auditar eventos nas em SVMs

ONTAP 9

NetApp
January 17, 2025

Índice

Auditar eventos nas em SVMs

Auditoria de SMB e NFS e rastreamento de segurança

Você pode usar os recursos de auditoria de acesso a arquivos disponíveis para os protocolos SMB e NFS com o ONTAP, como auditoria nativa e gerenciamento de políticas de arquivos usando FPolicy.

Você deve projetar e implementar a auditoria de eventos de acesso a arquivos SMB e NFS nas seguintes circunstâncias:

- O acesso básico a arquivos de protocolo SMB e NFS foi configurado.
- Você deseja criar e manter uma configuração de auditoria usando um dos seguintes métodos:
  - Funcionalidade ONTAP nativa
  - Servidores FPolicy externos

Auditar eventos nas em SVMs

A auditoria de eventos nas é uma medida de segurança que permite controlar e Registrar determinados eventos SMB e NFS em máquinas virtuais de storage (SVMs). Isso ajuda você a rastrear possíveis problemas de segurança e fornece evidências de quaisquer violações de segurança. Você também pode organizar e auditar políticas de acesso central do ative Directory para ver qual seria o resultado da implementação delas.

Eventos SMB

Você pode auditar os seguintes eventos:

- Eventos de acesso a arquivos SMB e pastas

  Você pode auditar eventos de acesso a arquivos SMB e pastas em objetos armazenados em volumes FlexVol pertencentes aos SVMs habilitados para auditoria.

- Eventos de logon e logoff SMB

  Você pode auditar eventos de logon e logoff SMB para servidores SMB em SVMs.

- Eventos de preparação da política de acesso central

  Você pode auditar o acesso efetivo de objetos em servidores SMB usando permissões aplicadas por meio de políticas de acesso centrais propostas. A auditoria por meio do preparo de políticas de acesso central permite que você veja quais são os efeitos das políticas de acesso centrais antes que elas sejam implantadas.

  A auditoria do preparo de políticas de acesso central é configurada usando GPOs do active Directory. No entanto, a configuração de auditoria SVM deve ser configurada para auditar eventos de preparação de políticas de acesso central.

  Embora você possa ativar o estadiamento da diretiva de acesso central na configuração de auditoria sem ativar o Controle de Acesso Dinâmico no servidor SMB, os eventos de estadiamento da política de acesso central são gerados somente se o Controle de Acesso Dinâmico estiver ativado. O Dynamic Access Control é ativado através de uma opção de servidor SMB. Ele não está habilitado por padrão.

Eventos NFS

Você pode auditar eventos de arquivo e diretório utilizando NFSv4 ACL em objetos armazenados em SVMs.

Como funciona a auditoria

Conceitos básicos de auditoria

Para entender a auditoria no ONTAP, você deve estar ciente de alguns conceitos básicos de auditoria.

- **Staging arquivos**

  Os arquivos binários intermediários em nós individuais onde os Registros de auditoria são armazenados antes da consolidação e conversão. Os arquivos de estadiamento estão contidos nos volumes de estadiamento.

- * Volume de estadiamento*

  Um volume dedicado criado pelo ONTAP para armazenar arquivos de teste. Há um volume de estadiamento por agregado. Os volumes de preparo são compartilhados por todas as máquinas virtuais de armazenamento (SVMs) habilitadas para auditoria para armazenar Registros de auditoria do acesso a dados para volumes de dados nesse agregado específico. Os Registros de auditoria de cada SVM são armazenados em um diretório separado dentro do volume de teste.

  Os administradores de cluster podem exibir informações sobre volumes de teste, mas a maioria das outras operações de volume não são permitidas. Somente o ONTAP pode criar volumes de estadiamento. O ONTAP atribui automaticamente um nome aos volumes de teste. Todos os nomes de volume de estadiamento começam com `MDV_aud_` seguido pelo UUID do agregado que contém esse volume de estadiamento (por exemplo: `MDV_aud_1d0131843d4811e296fc123478563412` .)

- **Volumes do sistema**

  Um FlexVol volume que contém metadados especiais, como metadados para logs de auditoria de serviços de arquivo. O SVM admin é proprietário de volumes de sistema, que podem ser vistos no cluster. Os volumes de estadiamento são um tipo de volume do sistema.

- **Tarefa de consolidação**

  Uma tarefa que é criada quando a auditoria é ativada. Essa tarefa de longa execução em cada SVM leva os Registros de auditoria de arquivos de teste nos nós membros do SVM. Essa tarefa mescla os Registros de auditoria em ordem cronológica ordenada e os converte em um formato de log de eventos legível pelo usuário especificado na configuração de auditoria — o formato de arquivo EVTX ou XML. Os logs de eventos convertidos são armazenados no diretório de log de eventos de auditoria especificado na configuração de auditoria SVM.

Como funciona o processo de auditoria do ONTAP

O processo de auditoria do ONTAP é diferente do processo de auditoria da Microsoft. Antes de configurar a auditoria, você deve entender como o processo de auditoria do ONTAP funciona.

Os Registros de auditoria são inicialmente armazenados em arquivos de estadiamento binários em nós individuais. Se a auditoria estiver habilitada em uma SVM, cada nó de membro manterá os arquivos de teste para essa SVM. Periodicamente, eles são consolidados e convertidos em logs de eventos legíveis pelo usuário, que são armazenados no diretório de log de eventos de auditoria do SVM.

Processo quando a auditoria é ativada em uma SVM

A auditoria só pode ser ativada em SVMs. Quando o administrador de storage habilita a auditoria na SVM, o subsistema de auditoria verifica se há volumes de teste presentes. Deve existir um volume de preparo para cada agregado que contenha volumes de dados de propriedade da SVM. O subsistema de auditoria cria todos os volumes de teste necessários se eles não existirem.

O subsistema de auditoria também conclui outras tarefas de pré-requisito antes que a auditoria seja ativada:

- O subsistema de auditoria verifica se o caminho do diretório de log está disponível e não contém links simbólicos.

  O diretório de log já deve existir como um caminho dentro do namespace do SVM. Recomenda-se criar um novo volume ou qtree para manter os arquivos de log de auditoria. O subsistema de auditoria não atribui um local de arquivo de log padrão. Se o caminho do diretório de log especificado na configuração de auditoria não for um caminho válido, a criação da configuração de auditoria falhará com o `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name"` erro.

  A criação de configuração falha se o diretório existir, mas contiver links simbólicos.

- A auditoria agenda a tarefa de consolidação.

  Depois que esta tarefa é agendada, a auditoria é ativada. A configuração de auditoria SVM e os arquivos de log persistem em uma reinicialização ou se os servidores NFS ou SMB forem interrompidos ou reiniciados.

Consolidação do log de eventos

A consolidação de log é uma tarefa agendada que é executada de rotina até que a auditoria seja desativada. Quando a auditoria é desativada, a tarefa de consolidação verifica se todos os logs restantes estão consolidados.

Auditoria garantida

Por padrão, a auditoria é garantida. O ONTAP garante que todos os eventos de acesso a arquivos auditáveis (conforme especificado pelas ACLs de diretiva de auditoria configuradas) sejam registrados, mesmo que um nó não esteja disponível. Uma operação de arquivo solicitada não pode ser concluída até que o Registro de auditoria dessa operação seja salvo no volume de espera no armazenamento persistente. Se os Registros de auditoria não puderem ser comprometidos com o disco nos arquivos de teste, seja por causa de espaço insuficiente ou por causa de outros problemas, as operações do cliente serão negadas.

Um administrador ou usuário de conta com acesso em nível de privilégio pode ignorar a operação de log de auditoria de arquivos usando o SDK de gerenciamento do NetApp ou APIs REST. Você pode determinar se alguma ação de arquivo foi realizada usando o SDK de gerenciamento do NetApp ou APIs REST, revisando os logs do histórico de comandos armazenados no `audit.log` arquivo.

Para obter mais informações sobre logs de auditoria do histórico de comandos, consulte a seção "Gerenciando logs de auditoria para atividades de gerenciamento" no "Administração do sistema".

Processo de consolidação quando um nó não está disponível

Se um nó que contenha volumes pertencentes a uma SVM com auditoria habilitada não estiver disponível, o comportamento da tarefa de consolidação de auditoria depende se o parceiro de failover de storage (SFO) do nó (ou o parceiro de HA no caso de um cluster de dois nós) está disponível:

- Se o volume de estadiamento estiver disponível por meio do parceiro SFO, os volumes de estadiamento relatados pela última vez pelo nó serão verificados e a consolidação continuará normalmente.
- Se o parceiro SFO não estiver disponível, a tarefa criará um arquivo de log parcial.

  Quando um nó não é alcançável, a tarefa de consolidação consolida os Registros de auditoria dos outros nós disponíveis desse SVM. Para identificar que não está concluída, a tarefa adiciona o sufixo `.partial` ao nome do arquivo consolidado.

- Depois que o nó indisponível estiver disponível, os Registros de auditoria nesse nó serão consolidados com os Registros de auditoria dos outros nós naquele momento.
- Todos os Registros de auditoria são preservados.

Rotação do registo de eventos

Os arquivos de log de eventos de auditoria são girados quando atingem um tamanho de log de limite configurado ou em uma programação configurada. Quando um arquivo de log de eventos é girado, a tarefa de consolidação agendada primeiro renomeia o arquivo convertido ativo para um arquivo de arquivo com carimbo de tempo e, em seguida, cria um novo arquivo de log de eventos convertido ativo.

Processo quando a auditoria é desativada no SVM

Quando a auditoria é desativada na SVM, a tarefa de consolidação é acionada uma última vez. Todos os Registros de auditoria registrados pendentes são registrados em um formato legível pelo usuário. Os logs de eventos existentes armazenados no diretório de log de eventos não são excluídos quando a auditoria é desativada no SVM e estão disponíveis para visualização.

Depois que todos os arquivos de teste existentes para esse SVM forem consolidados, a tarefa de consolidação será removida da programação. A desativação da configuração de auditoria do SVM não remove a configuração de auditoria. Um administrador de storage pode reativar a auditoria a qualquer momento.

A tarefa de consolidação de auditoria, que é criada quando a auditoria é ativada, monitora a tarefa de consolidação e a cria novamente se a tarefa de consolidação sair devido a um erro. Os usuários não podem excluir o trabalho de consolidação de auditoria.

Requisitos e considerações de auditoria

Antes de configurar e habilitar a auditoria na máquina virtual de storage (SVM), é necessário estar ciente de certos requisitos e considerações.

- O limite combinado para SVMs habilitadas para auditoria NFS e S3 depende da sua versão do ONTAP:

Versão de ONTAP	Máximo
9,8 e anteriores	50
9.9.1 e mais tarde	400

- A auditoria não está vinculada ao licenciamento SMB ou NFS.

  Você pode configurar e ativar a auditoria mesmo que as licenças SMB e NFS não estejam instaladas no cluster.

- A auditoria NFS dá suporte a ACEs de segurança (tipo U).
- Para auditoria NFS, não há mapeamento entre bits de modo e ACEs de auditoria.

  Ao converter ACLs em bits de modo, os ACEs de auditoria são ignorados. Ao converter bits de modo para ACLs, os ACEs de auditoria não são gerados.

- O diretório especificado na configuração de auditoria deve existir.

  Se não existir, o comando para criar a configuração de auditoria falha.

- O diretório especificado na configuração de auditoria deve atender aos seguintes requisitos:
  - O diretório não deve conter links simbólicos.

    Se o diretório especificado na configuração de auditoria contiver links simbólicos, o comando para criar a configuração de auditoria falhará.

  - Você deve especificar o diretório usando um caminho absoluto.

    Você não deve especificar um caminho relativo, por exemplo `/vs1/../`, .

- A auditoria depende de ter espaço disponível nos volumes de teste.

  Você deve estar ciente e ter um plano para garantir que haja espaço suficiente para os volumes de teste em agregados que contenham volumes auditados.

- A auditoria depende de ter espaço disponível no volume que contém o diretório onde os logs de eventos convertidos são armazenados.

  Você deve estar ciente e ter um plano para garantir que há espaço suficiente nos volumes usados para armazenar logs de eventos. Você pode especificar o número de logs de eventos a serem mantidos no diretório de auditoria usando o `-rotate-limit` parâmetro ao criar uma configuração de auditoria, o que pode ajudar a garantir que haja espaço disponível suficiente para os logs de eventos no volume.

- Embora você possa ativar o estadiamento da diretiva de acesso central na configuração de auditoria sem ativar o Controle de Acesso Dinâmico no servidor SMB, o Controle de Acesso Dinâmico deve estar habilitado para gerar eventos de estadiamento da política de acesso central.

O controlo de Acesso Dinâmico não está ativado por predefinição.

Agregue considerações de espaço ao ativar a auditoria

Quando uma configuração de auditoria é criada e a auditoria é ativada em pelo menos uma máquina virtual de storage (SVM) no cluster, o subsistema de auditoria cria volumes de teste em todos os agregados existentes e em todos os novos agregados criados. Você precisa estar ciente de certas considerações de espaço agregado ao habilitar a auditoria no cluster.

A criação de volume de estadiamento pode falhar devido à não disponibilidade de espaço em um agregado. Isso pode acontecer se você criar uma configuração de auditoria e os agregados existentes não tiverem espaço suficiente para conter o volume de preparo.

Você deve garantir que haja espaço suficiente nos agregados existentes para os volumes de teste antes de habilitar a auditoria em um SVM.

Limitações para o tamanho dos Registros de auditoria em arquivos de teste

O tamanho de um Registro de auditoria em um arquivo de teste não pode ser maior que 32 KB.

Quando grandes Registros de auditoria podem ocorrer

Grandes Registros de auditoria podem ocorrer durante a auditoria de gerenciamento em um dos seguintes cenários:

- Adicionar ou excluir usuários de ou para grupos com um grande número de usuários.
- Adicionar ou excluir uma lista de controle de acesso de compartilhamento de arquivos (ACL) em um compartilhamento de arquivos com um grande número de usuários de compartilhamento de arquivos.
- Outros cenários.

Desative a auditoria de gerenciamento para evitar esse problema. Para fazer isso, modifique a configuração de auditoria e remova o seguinte da lista de tipos de eventos de auditoria:

- compartilhamento de arquivos
- conta de utilizador
- grupo de segurança
- autorização-política-alteração

  Após a remoção, eles não serão auditados pelo subsistema de auditoria de serviços de arquivo.

Os efeitos dos registos de auditoria demasiado grandes

- Se o tamanho de um Registro de auditoria for muito grande (mais de 32 KB), o Registro de auditoria não será criado e o subsistema de auditoria gerará uma mensagem do sistema de gerenciamento de eventos (EMS) semelhante à seguinte:

  ```
  File Services Auditing subsystem failed the operation or truncated an audit
  ```

```
record because it was greater than max_audit_record_size value. Vserver
UUID=%s, event_id=%u, size=%u
```

Se a auditoria for garantida, a operação do arquivo falhará porque seu Registro de auditoria não pode ser criado.

- Se o tamanho do registo de auditoria for superior a 9.999 bytes, é apresentada a mesma mensagem EMS acima. Um Registro de auditoria parcial é criado com o valor de chave maior ausente.
- Se o Registro de auditoria exceder 2.000 carateres, a seguinte mensagem de erro será exibida em vez do valor real:

```
The value of this field was too long to display.
```

Quais são os formatos de log de eventos de auditoria suportados

Os formatos de arquivo suportados para os logs de eventos de auditoria convertidos são `EVTX` e `XML` formatos de arquivo.

Você pode especificar o tipo de formato de arquivo ao criar a configuração de auditoria. Por padrão, o ONTAP converte os logs binários para o `EVTX` formato de arquivo.

Ver registos de eventos de auditoria

Você pode usar logs de eventos de auditoria para determinar se você tem segurança de arquivo adequada e se houve tentativas inadequadas de acesso a arquivos e pastas. Pode visualizar e processar registos de eventos de auditoria guardados nos `EVTX` formatos de ficheiro ou `XML`.

- `EVTX` formato do ficheiro

  Você pode abrir os logs de eventos de auditoria convertidos `EVTX` como arquivos salvos usando o Visualizador de Eventos da Microsoft.

  Há duas opções que você pode usar ao visualizar logs de eventos usando o Visualizador de eventos:

  - Vista geral

    As informações comuns a todos os eventos são exibidas para o Registro de eventos. Nesta versão do ONTAP, os dados específicos do evento para o Registro de eventos não são exibidos. Você pode usar a exibição detalhada para exibir dados específicos do evento.

  - Vista detalhada

    Uma vista amigável e uma vista XML estão disponíveis. A visualização amigável e a visualização XML exibem as informações comuns a todos os eventos e os dados específicos do evento para o Registro de eventos.

- `XML` formato do ficheiro

Você pode exibir e processar `XML` logs de eventos de auditoria em aplicativos de terceiros que suportam o `XML` formato de arquivo. As ferramentas de visualização XML podem ser usadas para visualizar os logs de auditoria, desde que você tenha o esquema XML e informações sobre definições para os campos XML. Para obter mais informações sobre o esquema XML e definições, consulte "Referência de Esquema de Auditoria ONTAP" .

Como os logs de auditoria ativos são visualizados usando o Visualizador de Eventos

Se o processo de consolidação de auditoria estiver em execução no cluster, o processo de consolidação anexará novos Registros ao arquivo de log de auditoria ativo para máquinas virtuais de armazenamento (SVMs) habilitadas para auditoria. Este log de auditoria ativo pode ser acessado e aberto por meio de um compartilhamento SMB no Visualizador de Eventos da Microsoft.

Além de exibir Registros de auditoria existentes, o Visualizador de Eventos tem uma opção de atualização que permite atualizar o conteúdo na janela do console. Se os logs recém-anexados são visíveis no Visualizador de Eventos depende se os oplocks estão ativados no compartilhamento usado para acessar o log de auditoria ativo.

Definição de Oplocks na partilha	Comportamento
Ativado	O Visualizador de Eventos abre o log que contém eventos gravados até esse ponto no tempo. A operação de atualização não atualiza o log com novos eventos anexados pelo processo de consolidação.
Desativado	O Visualizador de Eventos abre o log que contém eventos gravados até esse ponto no tempo. A operação de atualização atualiza o log com novos eventos anexados pelo processo de consolidação.

Esta informação é aplicável apenas para `EVTX` registos de eventos. `XML` Os logs de eventos podem ser visualizados através de SMB em um navegador ou através de NFS usando qualquer editor ou visualizador XML.

Eventos SMB que podem ser auditados

Visão geral de eventos SMB que podem ser auditados

O ONTAP pode auditar determinados eventos SMB, incluindo determinados eventos de acesso a arquivos e pastas, determinados eventos de logon e logoff e eventos de preparação de políticas de acesso central. Saber quais eventos de acesso podem ser auditados é útil ao interpretar os resultados dos logs de eventos.

Os seguintes eventos SMB adicionais podem ser auditados no ONTAP 9.2 e posteriores:

ID DO EVENTO (EVT/EVTX)	Evento	Descrição	Categoria

4670	As permissões do objeto foram alteradas	ACESSO A OBJETO: Permissões alteradas.	Acesso a ficheiros
4907	As definições de auditoria de objetos foram alteradas	ACESSO A OBJETO: Definições de auditoria alteradas.	Acesso a ficheiros
4913	A Política de Acesso Central Objeto foi alterada	ACESSO A OBJETO: CAP ALTERADO.	Acesso a ficheiros

Os seguintes eventos SMB podem ser auditados no ONTAP 9.0 e posteriores:

ID DO EVENTO (EVT/EVTX)	Evento	Descrição	Categoria
540/4624	Uma conta foi iniciada com êxito	Logon/LOGOFF: Logon em rede (SMB).	Início de sessão e fim de sessão
529/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: Nome de usuário desconhecido ou senha ruim.	Início de sessão e fim de sessão
530/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: Restrição de tempo de logon da conta.	Início de sessão e fim de sessão
531/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: Conta atualmente desativada.	Início de sessão e fim de sessão
532/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: A conta de usuário expirou.	Início de sessão e fim de sessão
533/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: O usuário não pode fazer logon neste computador.	Início de sessão e fim de sessão
534/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: O usuário não recebeu o tipo de logon aqui.	Início de sessão e fim de sessão
535/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: A senha do usuário expirou.	Início de sessão e fim de sessão
537/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: O logon falhou por motivos diferentes dos acima.	Início de sessão e fim de sessão
539/4625	Não foi possível iniciar sessão numa conta	Logon/LOGOFF: Conta bloqueada.	Início de sessão e fim de sessão
538/4634	Uma conta foi encerrada	Logon/LOGOFF: LOGOFF de usuário local ou de rede.	Início de sessão e fim de sessão

560/4656	Abrir Objeto/criar Objeto	ACESSO A OBJETO: Objeto (arquivo ou diretório) aberto.	Acesso a ficheiros
563/4659	Abra Objeto com a intenção de Excluir	ACESSO A OBJETO: Um identificador para um objeto (arquivo ou diretório) foi solicitado com o intent to Delete.	Acesso a ficheiros
564/4660	Eliminar Objeto	ACESSO A OBJETO: Excluir Objeto (arquivo ou diretório). O ONTAP gera esse evento quando um cliente Windows tenta excluir o objeto (arquivo ou diretório).	Acesso a ficheiros
567/4663	Ler Objeto/escrever Objeto/obter atributos Objeto/Definir atributos Objeto	ACESSO A OBJETO: Tentativa de acesso a objeto (ler, escrever, obter atributo, definir atributo). **Observação:** para este evento, o ONTAP audita apenas a primeira operação de leitura e gravação SMB (sucesso ou falha) em um objeto. Isso impede que o ONTAP crie entradas de log excessivas quando um único cliente abre um objeto e executa muitas operações de leitura ou gravação sucessivas no mesmo objeto.	Acesso a ficheiros
NA/4664	Link físico	ACESSO A OBJETOS: Foi feita uma tentativa de criar um link físico.	Acesso a ficheiros
NA/4818	A política de acesso central proposta não concede as mesmas permissões de acesso que a política de acesso central atual	ACESSO A OBJETOS: Central Access Policy Staging.	Acesso a ficheiros
ID do evento Data ONTAP NA/na 9999	Mudar o nome do objeto	ACESSO A OBJETO: Objeto renomeado. Este é um evento da ONTAP. Atualmente, não é suportado pelo Windows como um único evento.	Acesso a ficheiros
ID do evento Data ONTAP NA/na 9998	Desvincular Objeto	ACESSO A OBJETO: Objeto não vinculado. Este é um evento da ONTAP. Atualmente, não é suportado pelo Windows como um único evento.	Acesso a ficheiros

Informações adicionais sobre o evento 4656

A `HandleID` tag no evento de auditoria `XML` contém o identificador do objeto (arquivo ou diretório) acessado. A `HandleID` tag para o evento EVTX 4656 contém informações diferentes, dependendo se o evento aberto é para criar um novo objeto ou para abrir um objeto existente:

- Se o evento aberto for uma solicitação aberta para criar um novo objeto (arquivo ou diretório), a `HandleID` tag no evento XML de auditoria mostrará um vazio `HandleID` (por exemplo: `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>`).

  O `HandleID` está vazio porque a SOLICITAÇÃO ABERTA (para criar um novo objeto) é auditada antes da criação real do objeto acontecer e antes de existir um identificador. Eventos auditados subsequentes para o mesmo objeto têm o identificador de objeto certo na `HandleID` tag.

- Se o evento aberto for uma solicitação aberta para abrir um objeto existente, o evento de auditoria terá o identificador atribuído desse objeto na `HandleID` tag (por exemplo: `<Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data>`).

Determine qual é o caminho completo para o objeto auditado

O caminho do objeto impresso na `<ObjectName>` tag para um Registro de auditoria contém o nome do volume (entre parênteses) e o caminho relativo da raiz do volume que contém. Se você quiser determinar o caminho completo do objeto auditado, incluindo o caminho de junção, há certas etapas que você deve seguir.

Passos

1. Determine qual é o nome do volume e o caminho relativo para o objeto auditado olhando para a `<ObjectName>` tag no evento de auditoria.

   Neste exemplo, o nome do volume é "ATA1" e o caminho relativo para o arquivo é `/dir1/file.txt`:

   `<Data Name="ObjectName"> (data1);/dir1/file.txt </Data>`

2. Usando o nome do volume determinado na etapa anterior, determine qual é o caminho de junção para o volume que contém o objeto auditado:

   Neste exemplo, o nome do volume é "ATA1" e o caminho de junção para o volume que contém o objeto auditado é `/data/data1`:

   `volume show -junction -volume data1`

   ```
                                  Junction                       Junction
   Vserver   Volume       Language Active    Junction Path      Path Source
   --------- ------------ -------- --------  ------------------ -----------
   vs1       data1        en_US.UTF-8
                                  true      /data/data1        RW_volume
   ```

3. Determine o caminho completo para o objeto auditado anexando o caminho relativo encontrado na `<ObjectName>` tag para o caminho de junção para o volume.

Neste exemplo, o caminho de junção para o volume:

`/data/data1/dir1/file.text`

Considerações ao auditar links simbólicos e links duros

Há certas considerações que você deve ter em mente ao auditar links simbólicos e links duros.

Um Registro de auditoria contém informações sobre o objeto que está sendo auditado, incluindo o caminho para o objeto auditado, que é identificado na `ObjectName` tag. Você deve estar ciente de como caminhos para links simbólicos e links rígidos são gravados na `ObjectName` tag.

Links simbólicos

Um link simbólico é um arquivo com um inode separado que contém um ponteiro para a localização de um objeto de destino, conhecido como alvo. Ao acessar um objeto por meio de um link simbólico, o ONTAP interpreta automaticamente o link simbólico e segue o caminho agnóstico do protocolo canônico real para o objeto de destino no volume.

Na saída de exemplo a seguir, há dois links simbólicos, ambos apontando para um arquivo `target.txt` chamado . Um dos links simbólicos é um link simbólico relativo e um é um link simbólico absoluto. Se qualquer um dos links simbólicos for auditado, a `ObjectName` tag no evento de auditoria conterá o caminho para o arquivo `target.txt`:

```
[root@host1 audit]# ls -l
total 0
lrwxrwxrwx 1 user1 group1 37 Apr  2 10:09 softlink_fullpath.txt ->
/data/audit/target.txt
lrwxrwxrwx 1 user1 group1 10 Apr  2 09:54 softlink.txt -> target.txt
-rwxrwxrwx 1 user1 group1 16 Apr  2 10:05 target.txt
```

Links físicos

Um link físico é uma entrada de diretório que associa um nome a um arquivo existente em um sistema de arquivos. O link físico aponta para a localização do inode do arquivo original. Semelhante a como o ONTAP interpreta links simbólicos, o ONTAP interpreta o link físico e segue o caminho canônico real para o objeto alvo no volume. Quando o acesso a um objeto de link físico é auditado, o evento de auditoria Registra esse caminho canônico absoluto na `ObjectName` tag em vez do caminho do link físico.

Considerações ao auditar fluxos de dados NTFS alternativos

Há certas considerações que você deve ter em mente ao auditar arquivos com fluxos de dados alternativos NTFS.

A localização de um objeto que está sendo auditado é registrada em um Registro de evento usando duas tags, a `ObjectName` tag (o caminho) e a `HandleID` tag (o identificador). Para identificar corretamente quais solicitações de fluxo estão sendo registradas, você deve estar ciente de quais Registros do ONTAP nesses campos para fluxos de dados alternativos do NTFS:

- ID EVTX: 4656 eventos (abrir e criar eventos de auditoria)
  - O caminho do fluxo de dados alternativo é gravado na `ObjectName` tag.
  - O identificador do fluxo de dados alternativo é gravado na `HandleID` tag.
- ID EVTX: 4663 eventos (todos os outros eventos de auditoria, como leitura, escrita, getattr, e assim por diante)
  - O caminho do arquivo base, não o fluxo de dados alternativo, é gravado na `ObjectName` tag.
  - O identificador do fluxo de dados alternativo é gravado na `HandleID` tag.

Exemplo

O exemplo a seguir ilustra como identificar o ID EVTX: 4663 eventos para fluxos de dados alternativos usando a `HandleID` tag. Mesmo que a `ObjectName` tag (caminho) registrada no evento de auditoria de leitura seja para o caminho do arquivo base, a `HandleID` tag pode ser usada para identificar o evento como um Registro de auditoria para o fluxo de dados alternativo.

Os nomes dos arquivos de stream assumem o formulário `base_file_name:stream_name`. Neste exemplo, o `dir1` diretório contém um arquivo base com um fluxo de dados alternativo com os seguintes caminhos:

```
/dir1/file1.txt
/dir1/file1.txt:stream1
```

A saída no exemplo de evento a seguir é truncada como indicado; a saída não exibe todas as tags de saída disponíveis para os eventos.

Para um EVTX ID 4656 (evento de auditoria aberto), a saída do Registro de auditoria para o fluxo de dados alternativo Registra o nome do fluxo de dados alternativo na `ObjectName` tag:

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4656</EventID>
  <EventName>Open Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt:stream1</Data\>
**
  [...]
  </EventData>
  </Event>
- <Event>
```

Para um EVTX ID 4663 (evento de auditoria de leitura), a saída do Registro de auditoria para o mesmo fluxo de dados alternativo Registra o nome do arquivo base na `ObjectName` tag; no entanto, o identificador na `HandleID` tag é o identificador do fluxo de dados alternativo e pode ser usado para correlacionar esse evento com o fluxo de dados alternativo:

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt</Data\> **
  [...]
  </EventData>
  </Event>
- <Event>
```

Eventos de acesso a arquivos e diretórios NFS que podem ser auditados

O ONTAP pode auditar determinados eventos de acesso a arquivos NFS e diretórios. Saber quais eventos de acesso podem ser auditados é útil ao interpretar os resultados dos logs de eventos de auditoria convertidos.

Você pode auditar os seguintes eventos de acesso a arquivos NFS e diretórios:

- LEIA
- ABRIR
- FECHAR
- READDIR
- ESCREVA
- SETATTR
- CRIAR
- LINK
- OPENATTR
- RETIRE
- GETATTR
- VERIFIQUE

- NVERIFY
- MUDAR O NOME

Para auditar de forma confiável os eventos DE RENOMEAÇÃO do NFS, você deve definir ACEs de auditoria em diretórios em vez de arquivos porque as permissões de arquivo não são verificadas para uma operação DE RENOMEAÇÃO se as permissões de diretório forem suficientes.

Planejar a configuração de auditoria

Antes de configurar a auditoria em máquinas virtuais de armazenamento (SVMs), você deve entender quais opções de configuração estão disponíveis e Planejar os valores que deseja definir para cada opção. Essas informações podem ajudá-lo a configurar a configuração de auditoria que atende às necessidades da sua empresa.

Existem certos parâmetros de configuração que são comuns a todas as configurações de auditoria.

Além disso, existem certos parâmetros que você pode usar para especificar quais métodos são usados ao girar os logs de auditoria consolidados e convertidos. Você pode especificar um dos três métodos a seguir ao configurar a auditoria:

- Rode registos com base no tamanho do registo

  Este é o método padrão usado para girar logs.

- Gire os logs com base em um agendamento
- Rodar registos com base no tamanho e na programação do registo (qualquer que seja o evento que ocorrer primeiro)

Pelo menos um dos métodos de rotação de log deve ser sempre definido.

Parâmetros comuns a todas as configurações de auditoria

Há dois parâmetros necessários que você deve especificar ao criar a configuração de auditoria. Há também três parâmetros opcionais que você pode especificar:

Tipo de informação	Opção	Obrigatório	Incluir	Seus valores
Nome da SVM Nome do SVM no qual você pode criar a configuração de auditoria. O SVM já deve existir.	`-vserver vserver_name`	Sim	Sim	

Log Destination path Especifica o diretório onde os logs de auditoria convertidos são armazenados, normalmente um volume ou qtree dedicado. O caminho já deve existir no namespace SVM. O caminho pode ter até 864 carateres de comprimento e deve ter permissões de leitura e gravação. Se o caminho não for válido, o comando de configuração de auditoria falhará. Se o SVM for uma fonte de recuperação de desastres do SVM, o caminho de destino do log não poderá estar no volume raiz. Isso ocorre porque o conteúdo do volume raiz não é replicado para o destino de recuperação de desastres. Não é possível usar um volume FlexCache como destino de log (ONTAP 9.7 e posterior).	`-destination text`	Sim	Sim	

Categorias de eventos a auditar Especifica as categorias de eventos a auditar. As seguintes categorias de eventos podem ser auditadas: • Eventos de acesso a arquivos (SMB e NFSv4) • Eventos de logon e logoff SMB • Eventos de preparação da política de acesso central Os eventos de preparação da política de acesso central estão disponíveis a partir dos domínios do ative Directory do Windows 2012. • Eliminação assíncrona • Eventos de categoria de compartilhamento de arquivos • Auditoria de eventos de mudança de política • Eventos de gerenciamento de contas de usuário local • Eventos de gerenciamento de grupo de segurança • Eventos de alteração da política de autorização O padrão é auditar o acesso a arquivos e eventos de logon e logoff SMB. **Observação:** antes de poder especificar `cap-staging` como categoria de evento, um servidor SMB deve existir na SVM. Embora você possa ativar o estadiamento da diretiva de acesso central na configuração de auditoria sem ativar o Controle de Acesso Dinâmico no servidor SMB, os eventos de estadiamento da política de acesso central são gerados somente se o Controle de Acesso Dinâmico estiver ativado. O Dynamic Access Control é ativado através de uma opção de servidor SMB. Ele não está habilitado por padrão.	`-events {file-ops`	`cifs-logon-logoff`	`cap-staging`	`file-share`

audit-policy-change	user-account	security-group	authorization-policy-change	`async-delete`Selecione
Não			*Formato de saída do ficheiro de registo* Determina o formato de saída dos logs de auditoria. O formato de saída pode ser um formato de log específico do ONTAP XML ou do Microsoft Windows EVTX. Por padrão, o formato de saída é EVTX.	-format {xml

`evtx`Selecione	Não			*Limite de rotação de arquivos de log* Determina quantos arquivos de log de auditoria devem ser mantidos antes de girar o arquivo de log mais antigo. Por exemplo, se você inserir um valor de `5`, os últimos cinco arquivos de log serão retidos. Um valor de `0` indica que todos os arquivos de log são mantidos. O valor padrão é 0.

Parâmetros usados para determinar quando girar logs de eventos de auditoria

Rotate logs com base no tamanho do log

O padrão é girar os logs de auditoria com base no tamanho.

- O tamanho padrão do log é de 100 MB
- Se você quiser usar o método de rotação de log padrão e o tamanho padrão do log, não será necessário configurar nenhum parâmetro específico para a rotação de log.
- Se você quiser girar os logs de auditoria somente com base em um tamanho de log, use o seguinte comando para desdefinir o `-rotate-schedule-minute` parâmetro: `vserver audit modify -vserver vs0 -destination / -rotate-schedule-minute -`

Se você não quiser usar o tamanho padrão do log, você pode configurar o `-rotate-size` parâmetro para especificar um tamanho de log personalizado:

Tipo de informação	Opção	Obrigatório	Incluir	Seus valores
Limite de tamanho do ficheiro de registo Determina o limite de tamanho do arquivo de log de auditoria.	`-rotate-size` {`integer`[KB	MB	GB	TB

Rotate logs com base em uma programação

Se você optar por girar os logs de auditoria com base em um agendamento, poderá agendar a rotação de logs usando os parâmetros de rotação baseados em tempo em qualquer combinação.

- Se utilizar rotação baseada no tempo, o `-rotate-schedule-minute` parâmetro é obrigatório.
- Todos os outros parâmetros de rotação baseados no tempo são opcionais.
- O programa de rotação é calculado utilizando todos os valores relacionados com o tempo.

  Por exemplo, se você especificar apenas o `-rotate-schedule-minute` parâmetro, os arquivos de log de auditoria serão girados com base nos minutos especificados em todos os dias da semana, durante todas as horas em todos os meses do ano.

- Se você especificar apenas um ou dois parâmetros de rotação baseados no tempo (por exemplo, `-rotate-schedule-month` e `-rotate-schedule-minutes`), os arquivos de log serão girados com base nos valores de minuto especificados em todos os dias da semana, durante todas as horas, mas somente durante os meses especificados.

  Por exemplo, você pode especificar que o log de auditoria deve ser girado durante os meses de janeiro, março e agosto em todas as segundas, quartas e sábados às 10:30 da manhã

- Se você especificar valores para ambos `-rotate-schedule-dayofweek` e `-rotate-schedule-day`, eles serão considerados independentemente.

  Por exemplo, se você especificar `-rotate-schedule-dayofweek` como sexta-feira e `-rotate -schedule-day` como 13, os logs de auditoria serão girados em todas as sextas-feiras e no dia 13th do mês especificado, não apenas em todas as sextas-feiras, dia 13th.

- Se você quiser girar os logs de auditoria somente com base em uma programação, use o seguinte comando para desdefinir o `-rotate-size` parâmetro: `vserver audit modify -vserver vs0 -destination / -rotate-size -`

Você pode usar a seguinte lista de parâmetros de auditoria disponíveis para determinar quais valores usar para configurar uma programação para rotações de log de eventos de auditoria:

Tipo de informação	Opção	Obrigatório	Incluir	Seus valores
Calendário de rotação de Registro: Mês Determina a programação mensal para os logs de auditoria rotativos. Os valores válidos `January` são através de `December`, e `all`. Por exemplo, você pode especificar que o log de auditoria deve ser girado durante os meses de janeiro, março e agosto.	`-rotate-schedule-month chron_month`	Não		
Calendário de rotação de Registro: Dia da semana Determina o cronograma diário (dia da semana) para logs de auditoria rotativos. Os valores válidos `Sunday` são através de `Saturday`, e `all`. Por exemplo, você pode especificar que o log de auditoria deve ser girado às terças e sextas-feiras, ou durante todos os dias de uma semana.	`-rotate-schedule -dayofweek chron_dayofweek`	Não		
Calendário de rotação de Registro: Dia Determina o dia do calendário do mês para a rotação do log de auditoria. Os valores válidos variam de `1` até `31`. Por exemplo, você pode especificar que o log de auditoria deve ser girado nos 10th e 20th dias de um mês ou em todos os dias de um mês.	`-rotate-schedule-day chron_dayofmonth`	Não		
Calendário de rotação de Registro: Hora Determina a programação horária para girar o log de auditoria. Os valores válidos variam de `0` (meia-noite) a `23` (11:00 p.m.). `all`Especificar gira os logs de auditoria a cada hora. Por exemplo, você pode especificar que o log de auditoria deve ser girado às 6 (6 a.m.) e 18 (6 p.m.).	`-rotate-schedule-hour chron_hour`	Não		

Calendário de rotação de Registro: Minuto Determina o cronograma de minutos para girar o log de auditoria. Os valores válidos variam de `0` a `59`. Por exemplo, você pode especificar que o log de auditoria deve ser girado aos 30th minutos.	`-rotate-schedule-minute chron_minute`	Sim, se configurar a rotação de log baseada em programação; caso contrário, não		

Rotate logs com base no tamanho e horário do log

Você pode optar por girar os arquivos de log com base no tamanho do log e em uma programação, definindo o `-rotate-size` parâmetro e os parâmetros de rotação baseados no tempo em qualquer combinação. Por exemplo: Se `-rotate-size` estiver definido para 10 MB e `-rotate-schedule-minute` estiver definido para 15, os arquivos de log rodam quando o tamanho do arquivo de log atinge 10 MB ou nos 15th minutos de cada hora (o que ocorrer primeiro).

Crie uma configuração de auditoria de arquivos e diretórios em SVMs

Crie a configuração de auditoria

A criação de uma configuração de auditoria de arquivos e diretórios na máquina virtual de storage (SVM) inclui compreender as opções de configuração disponíveis, Planejar a configuração e, em seguida, configurar e ativar a configuração. Em seguida, você pode exibir informações sobre a configuração de auditoria para confirmar se a configuração resultante é a configuração desejada.

Antes de iniciar a auditoria de eventos de arquivo e diretório, crie uma configuração de auditoria na máquina virtual de storage (SVM).

Antes de começar

Se você planeja criar uma configuração de auditoria para o preparo de políticas de acesso central, um servidor SMB deve existir no SVM.

- Embora você possa ativar o estadiamento da diretiva de acesso central na configuração de auditoria sem ativar o Controle de Acesso Dinâmico no servidor SMB, os eventos de estadiamento da política de acesso central são gerados somente se o Controle de Acesso Dinâmico estiver ativado.

  O Dynamic Access Control é ativado através de uma opção de servidor SMB. Ele não está habilitado por padrão.

- Se os argumentos de um campo em um comando forem inválidos, por exemplo, entradas inválidas para campos, entradas duplicadas e entradas inexistentes, o comando falhará antes da fase de auditoria.

  Tais falhas não geram um Registro de auditoria.

Sobre esta tarefa

Se o SVM for uma fonte de recuperação de desastres do SVM, o caminho de destino não poderá estar no volume raiz.

Passo

1. Usando as informações na Planilha de Planejamento, crie a configuração de auditoria para girar os logs de auditoria com base no tamanho do log ou em uma programação:

Se você quiser girar logs de auditoria…	Digite…
Tamanho do registo	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging
file-share	authorization-policy-change
user-account	security-group
authorization-policy-change}] [-format {xml	evtx}] [-rotate-limit integer] [-rotate-size {integer[KB
MB	GB
TB	PB]}]`
Uma programação	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging}] [-format {xml

Exemplos

O exemplo a seguir cria uma configuração de auditoria que audita operações de arquivo e eventos de logon e logoff SMB (o padrão) usando rotação baseada em tamanho. O formato de log é `EVTX` (o padrão). Os logs são armazenados no `/audit_log` diretório. O limite de tamanho do ficheiro de registo é `200 MB`. Os logs são girados quando atingem 200 MB de tamanho:

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-size 200MB
```

O exemplo a seguir cria uma configuração de auditoria que audita operações de arquivo e eventos de logon e logoff SMB (o padrão) usando rotação baseada em tamanho. O formato de log é `EVTX` (o padrão). Os logs são armazenados no `/cifs_event_logs` diretório. O limite de tamanho do arquivo de log é `100 MB` (o padrão) e o limite de rotação do log é `5`:

```
cluster1::> vserver audit create -vserver vs1 -destination
/cifs_event_logs -rotate-limit 5
```

O exemplo a seguir cria uma configuração de auditoria que audita operações de arquivo, eventos de logon e logoff CIFS e eventos de preparação de políticas de acesso central usando rotação baseada em tempo. O formato de log é `EVTX` (o padrão). Os logs de auditoria são girados mensalmente, às 12:30 horas em todos os dias da semana. O limite de rotação do registo é `5`de :

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-events file-ops,cifs-logon-logoff,file-share,audit-policy-change,user-
account,security-group,authorization-policy-change,cap-staging -rotate
-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour
12 -rotate-schedule-minute 30 -rotate-limit 5
```

Informações relacionadas

- "Habilite a auditoria no SVM"
- "Verifique a configuração de auditoria"

Habilite a auditoria no SVM

Depois de concluir a configuração de auditoria, será necessário habilitar a auditoria na máquina virtual de storage (SVM).

Antes de começar

A configuração de auditoria da SVM já deve existir.

Sobre esta tarefa

Quando uma configuração de descarte de ID de recuperação de desastres da SVM é iniciada pela primeira vez (após a inicialização do SnapMirror ser concluída) e o SVM tiver uma configuração de auditoria, o ONTAP desativa automaticamente a configuração de auditoria. A auditoria é desativada no SVM somente leitura para evitar que os volumes de preparo sejam preenchidos. Você pode ativar a auditoria somente depois que a relação do SnapMirror for interrompida e o SVM for leitura-gravação.

Passos

1. Habilite a auditoria no SVM:

   ```
   vserver audit enable -vserver vserver_name
   ```

```
vserver audit enable -vserver vs1
```

Informações relacionadas

- "Crie a configuração de auditoria"
- "Verifique a configuração de auditoria"

Verifique a configuração de auditoria

Depois de concluir a configuração de auditoria, você deve verificar se a auditoria está configurada corretamente e está habilitada.

Passos

1. Verifique a configuração de auditoria:

   ```
   vserver audit show -instance -vserver vserver_name
   ```

   O comando a seguir exibe em lista todas as informações de configuração de auditoria da máquina virtual de armazenamento (SVM) VS1:

   ```
   vserver audit show -instance -vserver vs1
   ```

   ```
                               Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops
                           Log Format: evtx
                  Log File Size Limit: 200MB
        Log Rotation Schedule: Month: -
   Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
             Log Files Rotation Limit: 0
   ```

Informações relacionadas

- "Crie a configuração de auditoria"
- "Habilite a auditoria no SVM"

Configurar políticas de auditoria de arquivos e pastas

Configurar políticas de auditoria de arquivos e pastas

Implementar auditoria em eventos de acesso a arquivos e pastas é um processo de duas etapas. Primeiro, você deve criar e habilitar uma configuração de auditoria em máquinas virtuais de storage (SVMs). Em segundo lugar, você deve configurar políticas de

auditoria nos arquivos e pastas que deseja monitorar. Você pode configurar políticas de auditoria para monitorar tentativas de acesso bem-sucedidas e com falha.

Você pode configurar políticas de auditoria SMB e NFS. As políticas de auditoria SMB e NFS têm requisitos de configuração e funcionalidades de auditoria diferentes.

Se as políticas de auditoria apropriadas estiverem configuradas, o ONTAP monitora eventos de acesso SMB e NFS conforme especificado nas políticas de auditoria somente se os servidores SMB ou NFS estiverem em execução.

Configurar políticas de auditoria em arquivos e diretórios de estilo de segurança NTFS

Antes de poder auditar operações de arquivo e diretório, você deve configurar políticas de auditoria nos arquivos e diretórios para os quais deseja coletar informações de auditoria. Isso é além de configurar e ativar a configuração de auditoria. Você pode configurar políticas de auditoria NTFS usando a guia Segurança do Windows ou usando a CLI do ONTAP.

Configurando diretivas de auditoria NTFS usando a guia Segurança do Windows

Você pode configurar políticas de auditoria NTFS em arquivos e diretórios usando a guia **Segurança do Windows** na janela Propriedades do Windows. Este é o mesmo método usado ao configurar políticas de auditoria em dados residentes em um cliente Windows, que permite que você use a mesma interface GUI que você está acostumado a usar.

Antes de começar

A auditoria deve ser configurada na máquina virtual de storage (SVM) que contém os dados aos quais você está aplicando as listas de controle de acesso do sistema (SACLs).

Sobre esta tarefa

A configuração de diretivas de auditoria NTFS é feita adicionando entradas a SACLs NTFS que estão associadas a um descritor de segurança NTFS. O descritor de segurança é então aplicado a arquivos e diretórios NTFS. Essas tarefas são tratadas automaticamente pela GUI do Windows. O descritor de segurança pode conter listas de controle de acesso discricionárias (DACLs) para aplicar permissões de acesso a arquivos e pastas, SACLs para auditoria de arquivos e pastas ou SACLs e DACLs.

Para definir políticas de auditoria NTFS usando a guia Segurança do Windows, execute as seguintes etapas em um host do Windows:

Passos

1. No menu **Ferramentas** no Windows Explorer, selecione **Mapear unidade de rede**.
2. Preencha a caixa **Map Network Drive**:

    a. Selecione uma letra **Drive**.

    b. Na caixa **pasta**, digite o nome do servidor SMB que contém o compartilhamento, mantendo os dados que deseja auditar e o nome do compartilhamento.

    Você pode especificar o endereço IP da interface de dados para o servidor SMB em vez do nome do servidor SMB.

    Se o nome do servidor SMB for ""SMB_SERVER"" e o compartilhamento for chamado "hare1", você

deverá inserir `\\SMB_SERVER\share1`.

c. Clique em **Finish**.

A unidade selecionada está montada e pronta com a janela do Windows Explorer exibindo arquivos e pastas contidos no compartilhamento.

3. Selecione o ficheiro ou diretório para o qual pretende ativar o acesso de auditoria.
4. Clique com o botão direito do rato no ficheiro ou diretório e selecione **Propriedades**.
5. Selecione a guia **Segurança**.
6. Clique em **Avançado**.
7. Selecione a guia **Auditoria**.
8. Execute as ações desejadas:

Se você quiser	Faça o seguinte
Configure a auditoria para um novo usuário ou grupo	a. Clique em **Add**. b. Na caixa Digite o nome do objeto a ser selecionado, digite o nome do usuário ou grupo que deseja adicionar. c. Clique em **OK**.
Remova a auditoria de um usuário ou grupo	a. Na caixa Digite o nome do objeto a ser selecionado, selecione o usuário ou grupo que deseja remover. b. Clique em **Remover**. c. Clique em **OK**. d. Ignore o resto deste procedimento.
Alterar a auditoria para um usuário ou grupo	a. Na caixa Digite o nome do objeto a ser selecionado, selecione o usuário ou grupo que deseja alterar. b. Clique em **Editar**. c. Clique em **OK**.

Se você estiver configurando a auditoria em um usuário ou grupo ou alterando a auditoria em um usuário ou grupo existente, a caixa Entrada de Auditoria para <object> será aberta.

9. Na caixa **aplicar a**, selecione como você deseja aplicar essa entrada de auditoria.

Pode selecionar uma das seguintes opções:

- **Esta pasta, subpastas e ficheiros**
- **Esta pasta e subpastas**
- **Somente esta pasta**
- **Esta pasta e ficheiros**
- **Somente subpastas e arquivos**
- **Somente subpastas**

- **Somente arquivos** se você estiver configurando a auditoria em um único arquivo, a caixa **aplicar a** não estará ativa. A configuração da caixa **Apply to** é padrão para **this object only**.

> Como a auditoria exige recursos da SVM, selecione apenas o nível mínimo que forneça os eventos de auditoria que atendam aos seus requisitos de segurança.

10. Na caixa **Access**, selecione o que deseja auditado e se deseja auditar eventos bem-sucedidos, eventos de falha ou ambos.
    - Para auditar eventos bem-sucedidos, selecione a caixa sucesso.
    - Para auditar eventos de falha, selecione a caixa Falha.

      Selecione apenas as ações que você precisa monitorar para atender aos requisitos de segurança. Para obter mais informações sobre esses eventos auditáveis, consulte a documentação do Windows. Você pode auditar os seguintes eventos:

    - * Controle total*
    - * Traverse pasta / executar arquivo *
    - **Lista de pastas / dados de leitura**
    - **Leia atributos**
    - **Leia atributos estendidos**
    - * Criar arquivos / escrever dados *
    - * Criar pastas / anexar dados*
    - * Escrever atributos*
    - **Escreva atributos estendidos**
    - **Excluir subpastas e arquivos**
    - **Excluir**
    - **Permissões de leitura**
    - **Alterar permissões**
    - **Assuma a propriedade**
11. Se você não quiser que a configuração de auditoria se propague para arquivos e pastas subsequentes do contentor original, marque a caixa **aplicar essas entradas de auditoria a objetos e/ou contentores dentro desse contentor somente**.
12. Clique em **aplicar**.
13. Depois de terminar de adicionar, remover ou editar entradas de auditoria, clique em **OK**.

    A caixa Entrada Auditoria para <object> fecha.

14. Na caixa **Auditoria**, selecione as configurações de herança para esta pasta.

    Selecione apenas o nível mínimo que fornece os eventos de auditoria que atendem aos seus requisitos de segurança. Você pode escolher uma das seguintes opções:

    - Selecione a caixa incluir entradas de auditoria herdáveis na caixa pai deste objeto.
    - Selecione a caixa Substituir todas as entradas de auditoria herdáveis existentes em todos os descendentes por entradas de auditoria herdáveis deste objeto.

- Selecione ambas as caixas.
- Selecione nenhuma das caixas. Se você estiver configurando SACLs em um único arquivo, a caixa Substituir todas as entradas de auditoria herdáveis existentes em todos os descendentes por entradas de auditoria herdáveis deste objeto não estará presente na caixa Auditoria.

15. Clique em **OK**.

    A caixa Auditoria fecha.

Configurar políticas de auditoria NTFS usando a CLI do ONTAP

Você pode configurar políticas de auditoria em arquivos e pastas usando a CLI do ONTAP. Isso permite configurar políticas de auditoria NTFS sem a necessidade de se conetar aos dados usando um compartilhamento SMB em um cliente Windows.

Você pode configurar políticas de auditoria NTFS usando a `vserver security file-directory` família de comandos.

Você só pode configurar SACLs NTFS usando a CLI. A configuração de SACLs NFSv4 não é suportada com esta família de comandos ONTAP. Consulte as páginas de manual para obter mais informações sobre como usar esses comandos para configurar e adicionar SACLs NTFS a arquivos e pastas.

Configurar auditoria para arquivos e diretórios de estilo de segurança UNIX

Você configura a auditoria de arquivos e diretórios de estilo de segurança UNIX adicionando ACEs de auditoria a ACLs NFSv4.x. Isso permite que você monitore determinados eventos de acesso a arquivos NFS e diretórios para fins de segurança.

Sobre esta tarefa

Para NFSv4.x, os ACEs discricionários e do sistema são armazenados na mesma ACL. Eles não são armazenados em DACLs e SACLs separados. Portanto, você deve ter cuidado ao adicionar ACEs de auditoria a uma ACL existente para evitar sobrescrever e perder uma ACL existente. A ordem em que você adiciona os ACEs de auditoria a uma ACL existente não importa.

Passos

1. Recupere a ACL existente para o arquivo ou diretório usando o `nfs4_getfacl` comando ou equivalente.

   Para obter mais informações sobre como manipular ACLs, consulte as páginas de manual do seu cliente NFS.

2. Anexe os ACEs de auditoria desejados.
3. Aplique a ACL atualizada ao arquivo ou diretório usando o `nfs4_setfacl` comando ou equivalente.

Exibir informações sobre políticas de auditoria aplicadas a arquivos e diretórios

Exiba informações sobre políticas de auditoria usando a guia Segurança do Windows

Você pode exibir informações sobre políticas de auditoria que foram aplicadas a arquivos

e diretórios usando a guia Segurança na janela Propriedades do Windows. Este é o mesmo método usado para dados que residem em um servidor Windows, que permite que os clientes usem a mesma interface GUI que estão acostumados a usar.

Sobre esta tarefa

A exibição de informações sobre políticas de auditoria aplicadas a arquivos e diretórios permite verificar se você tem as listas de controle de acesso do sistema (SACLs) apropriadas definidas em arquivos e pastas especificados.

Para exibir informações sobre SACLs que foram aplicadas a arquivos e pastas NTFS, execute as etapas a seguir em um host do Windows.

Passos

1. No menu **Ferramentas** no Windows Explorer, selecione **Mapear unidade de rede**.
2. Preencha a caixa de diálogo **Map Network Drive**:

   a. Selecione uma letra **Drive**.

   b. Na caixa **pasta**, digite o endereço IP ou o nome do servidor SMB da máquina virtual de armazenamento (SVM) que contém o compartilhamento que contém os dados que deseja auditar e o nome do compartilhamento.

      Se o nome do servidor SMB for ""SMB_SERVER"" e o compartilhamento for chamado "hare1", você deverá inserir `\\SMB_SERVER\share1`.

      Você pode especificar o endereço IP da interface de dados para o servidor SMB em vez do nome do servidor SMB.

   c. Clique em **Finish**.

   A unidade selecionada está montada e pronta com a janela do Windows Explorer exibindo arquivos e pastas contidos no compartilhamento.

3. Selecione o arquivo ou diretório para o qual você exibe informações de auditoria.
4. Clique com o botão direito do rato no ficheiro ou diretório e selecione **Propriedades**.
5. Selecione a guia **Segurança**.
6. Clique em **Avançado**.
7. Selecione a guia **Auditoria**.
8. Clique em **continuar**.

   Abre-se a caixa Auditoria. A caixa **Auditoria de entradas** exibe um resumo de usuários e grupos que têm SACLs aplicados a eles.

9. Na caixa **Auditoria de entradas**, selecione o usuário ou grupo cujas entradas SACL você deseja exibir.
10. Clique em **Editar**.

    A caixa Entrada Auditoria para <object> será aberta.

11. Na caixa **Access**, exiba os SACLs atuais aplicados ao objeto selecionado.
12. Clique em **Cancelar** para fechar a caixa **Entrada de Auditoria para <object>**.

13. Clique em **Cancelar** para fechar a caixa **Auditoria**.

Exibir informações sobre políticas de auditoria NTFS em volumes FlexVol usando a CLI

Você pode exibir informações sobre políticas de auditoria NTFS no FlexVol volumes, incluindo quais são os estilos de segurança e estilos de segurança eficazes, quais permissões são aplicadas e informações sobre listas de controle de acesso do sistema. Você pode usar as informações para validar sua configuração de segurança ou para solucionar problemas de auditoria.

Sobre esta tarefa

A exibição de informações sobre políticas de auditoria aplicadas a arquivos e diretórios permite verificar se você tem as listas de controle de acesso do sistema (SACLs) apropriadas definidas em arquivos e pastas especificados.

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os arquivos ou pastas cujas informações de auditoria você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

- Os volumes e qtrees de estilo de segurança NTFS usam apenas as listas de controle de acesso do sistema NTFS (SACLs) para políticas de auditoria.
- Arquivos e pastas em um volume misto de estilo de segurança com segurança efetiva NTFS podem ter políticas de auditoria NTFS aplicadas a eles.

  Volumes mistos de estilo de segurança e qtrees podem conter alguns arquivos e diretórios que usam permissões de arquivo UNIX, bits de modo ou ACLs NFSv4 e alguns arquivos e diretórios que usam permissões de arquivo NTFS.

- O nível superior de um volume de estilo de segurança misto pode ter segurança efetiva UNIX ou NTFS e pode ou não conter SACLs NTFS.
- Como a segurança do Storage-Level Access Guard pode ser configurada em um volume ou qtree misto de estilo de segurança, mesmo que o estilo de segurança efetivo da raiz de volume ou qtree seja UNIX, a saída para um caminho de volume ou qtree em que o Storage-Level Access Guard está configurado pode exibir tanto o arquivo normal quanto a pasta NFSv4 SACLs e o Storage-Level Access Guard NTFS SACLs.
- Se o caminho inserido no comando for para dados com segurança efetiva NTFS, a saída também exibirá informações sobre ACEs de Controle de Acesso Dinâmico se o Controle de Acesso Dinâmico estiver configurado para o caminho do arquivo ou diretório fornecido.
- Ao exibir informações de segurança sobre arquivos e pastas com segurança efetiva NTFS, os campos de saída relacionados ao UNIX contêm informações de permissão de arquivo UNIX somente para exibição.

  Arquivos e pastas de estilo de segurança NTFS usam apenas permissões de arquivo NTFS e usuários e grupos do Windows ao determinar direitos de acesso a arquivos.

- A saída ACL é exibida apenas para arquivos e pastas com segurança NTFS ou NFSv4.

  Este campo está vazio para arquivos e pastas que usam segurança UNIX que têm apenas permissões de bits de modo aplicadas (sem ACLs NFSv4).

- Os campos de saída do proprietário e do grupo na saída da ACL aplicam-se apenas no caso de

descritores de segurança NTFS.

Passo

1. Exiba as configurações de diretiva de auditoria de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações…	Digite o seguinte comando…
Em forma de resumo	`vserver security file-directory show -vserver vserver_name -path path`
Como uma lista detalhada	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Exemplos

O exemplo a seguir exibe as informações da política de auditoria do caminho `/corp` no SVM VS1. O caminho tem segurança eficaz NTFS. O descritor de segurança NTFS contém uma entrada SACL DE sucesso e uma entrada de sucesso/FALHA.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

O exemplo a seguir exibe as informações da política de auditoria do caminho `/datavol1` no SVM VS1. O caminho contém SACLs de arquivo e pasta regulares e SACLs de proteção de acesso em nível de

armazenamento.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Maneiras de exibir informações sobre segurança de arquivos e diretivas de auditoria

Você pode usar o caractere curinga (*) para exibir informações sobre segurança de arquivos e políticas de auditoria de todos os arquivos e diretórios em um determinado caminho ou volume raiz.

O caractere curinga (*) pode ser usado como o último subcomponente de um determinado caminho de diretório abaixo do qual você deseja exibir informações de todos os arquivos e diretórios.

Se você quiser exibir informações de um arquivo ou diretório específico chamado "*", então você precisa fornecer o caminho completo dentro de aspas duplas (" ").

Exemplo

O comando a seguir com o caractere curinga exibe as informações sobre todos os arquivos e diretórios abaixo do caminho `/1/` do SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

O comando a seguir exibe as informações de um arquivo chamado "*" no caminho `/vol1/a` do SVM VS1. O caminho está entre aspas duplas (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                Vserver: vs1
              File Path: "/vol1/a/*"
      Security Style: mixed
     Effective Style: unix
      DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
         Unix User Id: 1002
        Unix Group Id: 65533
       Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                 ACLs: NFSV4 Security Descriptor
                       Control:0x8014
                       SACL - ACEs
                         AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                       DACL - ACEs
                         ALLOW-EVERYONE@-0x1f00a9-FI|DI
                         ALLOW-OWNER@-0x1f01ff-FI|DI
                         ALLOW-GROUP@-0x1200a9-IG
```

Eventos de mudança de CLI que podem ser auditados

CLI alterar eventos que podem ser auditados visão geral

O ONTAP pode auditar certos eventos de mudança de CLI, incluindo certos eventos de compartilhamento de SMB, certos eventos de política de auditoria, determinados eventos de grupo de segurança local, eventos de grupo de usuários locais e eventos de política de autorização. Entender quais eventos de mudança podem ser auditados é útil ao interpretar os resultados dos logs de eventos.

Você pode gerenciar eventos de alteração da CLI de auditoria de máquina virtual de storage (SVM) girando manualmente os logs de auditoria, habilitando ou desativando a auditoria, exibindo informações sobre auditoria de eventos de alterações, modificando eventos de auditoria de alterações e excluindo eventos de alteração de auditoria.

Como administrador, se você executar qualquer comando para alterar a configuração relacionada aos eventos SMB-share, grupo de usuários local, grupo de segurança local, política de autorização e política de auditoria, um Registro será gerado e o evento correspondente será auditado:

Categoria Auditoria	Eventos	IDs de eventos	Execute este comando…
Auditoria Mhost	mudança de política	[4719] Configuração de auditoria alterada	`vserver audit disable

enable	modify`	compartilhamento de arquivos	[5142] a partilha de rede foi adicionada
`vserver cifs share create`	[5143] a partilha de rede foi modificada	`vserver cifs share modify` `vserver cifs share create`	modify
delete` `vserver cifs share add	remove`	[5144] partilha de rede eliminada	`vserver cifs share delete`
Auditoria	conta de utilizador	[4720] usuário local criado	`vserver cifs users-and-groups local-user create` `vserver services name-service unix-user create`
[4722] utilizador local ativado	`vserver cifs users-and-groups local-user create	modify`	[4724] Reposição da palavra-passe do utilizador local
`vserver cifs users-and-groups local-user set-password`	[4725] Utilizador local desativado	`vserver cifs users-and-groups local-user create	modify`
[4726] utilizador local eliminado	`vserver cifs users-and-groups local-user delete` `vserver services name-service unix-user delete`	[4738] alteração do utilizador local	`vserver cifs users-and-groups local-user modify` `vserver services name-service unix-user modify`
[4781] Renomear utilizador local	`vserver cifs users-and-groups local-user rename`	grupo de segurança	[4731] Grupo de Segurança local criado
`vserver cifs users-and-groups local-group create` `vserver services name-service unix-group create`	[4734] Grupo de Segurança local eliminado	`vserver cifs users-and-groups local-group delete` `vserver services name-service unix-group delete`	[4735] Grupo de Segurança local modificado

`vserver cifs users-and-groups local-group rename	modify` `vserver services name-service unix-group modify`	[4732] Usuário adicionado ao Grupo local	`vserver cifs users-and-groups local-group add-members vserver services name-service unix-group adduser`
[4733] Usuário removido do Grupo local	`vserver cifs users-and-groups local-group remove-members vserver services name-service unix-group deluser`	autorização-política-alteração	[4704] Direitos de Usuário atribuídos
`vserver cifs users-and-groups privilege add-privilege`	[4705] Direitos de usuário removidos	`vserver cifs users-and-groups privilege remove-privilege`	reset-privilege`

Gerenciar evento de compartilhamento de arquivos

Quando um evento de compartilhamento de arquivos é configurado para uma máquina virtual de storage (SVM) e uma auditoria é ativada, os eventos de auditoria são gerados. Os eventos de compartilhamento de arquivos são gerados quando o compartilhamento de rede SMB é modificado usando `vserver cifs share` comandos relacionados.

Os eventos de compartilhamento de arquivos com as ids de eventos 5142, 5143 e 5144 são gerados quando um compartilhamento de rede SMB é adicionado, modificado ou excluído para o SVM. A configuração de compartilhamento de rede SMB é modificada usando os `cifs share access control create|modify|delete` comandos.

O exemplo a seguir exibe um evento de compartilhamento de arquivos com a ID 5143 é gerado, quando um objeto de compartilhamento chamado 'audit_dest' é criado:

```
netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 5142
   EventName Share Object Added
   ...
   ...
  ShareName audit_dest
  SharePath /audit_dest
  ShareProperties oplocks;browsable;changenotify;show-previous-versions;
  SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;FA;;;WD)
```

Gerenciar evento de mudança de política de auditoria

Quando um evento de alteração de política de auditoria é configurado para uma máquina virtual de storage (SVM) e uma auditoria é ativada, os eventos de auditoria são gerados. Os eventos de alteração de política de auditoria são gerados quando uma diretiva de auditoria é modificada usando `vserver audit` comandos relacionados.

O evento de alteração de política de auditoria com o ID de evento 4719 é gerado sempre que uma política de auditoria é desativada, ativada ou modificada e ajuda a identificar quando um usuário tenta desativar a auditoria para cobrir os trajetos. Ele é configurado por padrão e requer privilégio de diagnóstico para ser desativado.

O exemplo a seguir exibe um evento de mudança de diretiva de auditoria com a ID 4719 gerada, quando uma auditoria é desativada:

```
netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4719
   EventName Audit Disabled
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
```

Gerenciar evento de conta de usuário

Quando um evento de conta de usuário é configurado para uma máquina virtual de storage (SVM) e uma auditoria é ativada, os eventos de auditoria são gerados.

Os eventos da conta de usuário com ids de eventos 4720, 4722, 4724, 4725, 4726, 4738 e 4781 são gerados quando um usuário SMB ou NFS local é criado ou excluído do sistema, a conta de usuário local é ativada, desativada ou modificada e a senha de usuário SMB local é redefinida ou alterada. Os eventos de conta de usuário são gerados quando uma conta de usuário é modificada usando `vserver cifs users-and-groups <local user>` comandos e `vserver services name-service <unix user>`.

O exemplo a seguir exibe um evento de conta de usuário com a ID 4720 gerada, quando um usuário SMB local é criado:

```
netapp-clus1::*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4720
   EventName Local Cifs User Created
   ...
   ...
  TargetUserName testuser
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
  TargetType CIFS
  DisplayName testuser
  PasswordLastSet 1472662216
  AccountExpires NO
  PrimaryGroupId 513
  UserAccountControl %%0200
  SidHistory ~
  PrivilegeList ~
```

O exemplo a seguir exibe um evento de conta de usuário com a ID 4781 gerada, quando o usuário local SMB criado no exemplo anterior é renomeado:

```
 netapp-clus1::*> vserver cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4781
   EventName Local Cifs User Renamed
   ...
   ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~
```

Gerenciar evento do grupo de segurança

Quando um evento de grupo de segurança é configurado para uma máquina virtual de storage (SVM) e uma auditoria é ativada, os eventos de auditoria são gerados.

Os eventos de grupo de segurança com ids de eventos 4731, 4732, 4733, 4734 e 4735 são gerados quando um grupo SMB ou NFS local é criado ou excluído do sistema e o usuário local é adicionado ou removido do grupo. Os eventos de grupo de segurança são gerados quando uma conta de usuário é modificada usando `vserver cifs users-and-groups <local-group>` comandos e `vserver services name-service <unix-group>`.

O exemplo a seguir exibe um evento de grupo de segurança com a ID 4731 gerada, quando um grupo de segurança UNIX local é criado:

```
netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4731
   EventName Local Unix Security Group Created
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~
```

Gerenciar evento de alteração de política de autorização

Quando o evento de alteração de política de autorização é configurado para uma máquina virtual de storage (SVM) e uma auditoria é ativada, os eventos de auditoria são gerados.

Os eventos autorização-política-mudança com os ids de evento 4704 e 4705 são gerados sempre que os direitos de autorização são concedidos ou revogados para um usuário SMB e grupo SMB. Os eventos autorização-política-mudança são gerados quando os direitos de autorização são atribuídos ou revogados usando `vserver cifs users-and-groups privilege` comandos relacionados.

O exemplo a seguir exibe um evento de política de autorização com a ID 4704 gerada, quando os direitos de autorização para um grupo de usuários SMB são atribuídos:

```
netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4704
   EventName User Right Assigned
   ...
   ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS
```

Gerenciar configurações de auditoria

Rode manualmente os registos de eventos de auditoria

Antes de poder visualizar os registos de eventos de auditoria, os registos têm de ser convertidos para formatos legíveis pelo utilizador. Se você quiser exibir os logs de eventos de uma máquina virtual de storage específica (SVM) antes que o ONTAP gire automaticamente o log, você pode girar manualmente os logs de eventos de auditoria em uma SVM.

Passo

1. Gire os logs de eventos de auditoria usando o `vserver audit rotate-log` comando.

   ```
   vserver audit rotate-log -vserver vs1
   ```

   O log de eventos de auditoria é salvo no diretório de log de eventos de auditoria SVM com o formato especificado pela configuração de auditoria (`XML`ou `EVTX`) e pode ser visualizado usando o aplicativo apropriado.

Ativar e desativar a auditoria em SVMs

Você pode ativar ou desativar a auditoria em máquinas virtuais de armazenamento (SVMs). Talvez você queira interromper temporariamente a auditoria de arquivos e diretórios desativando a auditoria. Você pode ativar a auditoria a qualquer momento (se houver uma configuração de auditoria).

O que você vai precisar

Antes de habilitar a auditoria na SVM, a configuração de auditoria da SVM já deve existir.

"Crie a configuração de auditoria"

Sobre esta tarefa

A desativação da auditoria não exclui a configuração de auditoria.

Passos

1. Execute o comando apropriado:

Se você quer que a auditoria seja…	Digite o comando…
Ativado	`vserver audit enable -vserver vserver_name`
Desativado	`vserver audit disable -vserver vserver_name`

2. Verifique se a auditoria está no estado desejado:

   `vserver audit show -vserver vserver_name`

Exemplos

O exemplo a seguir permite a auditoria do SVM VS1:

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

                               Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
      Categories of Events to Audit: file-ops, cifs-logon-logoff
                          Log Format: evtx
                 Log File Size Limit: 100MB
       Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
         Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 10
```

O exemplo a seguir desativa a auditoria para SVM VS1:

```
cluster1::> vserver audit disable -vserver vs1

                              Vserver: vs1
                      Auditing state: false
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops, cifs-logon-logoff
                          Log Format: evtx
                 Log File Size Limit: 100MB
         Log Rotation Schedule: Month: -
   Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
             Log Files Rotation Limit: 10
```

Exibir informações sobre configurações de auditoria

Você pode exibir informações sobre configurações de auditoria. As informações podem ajudá-lo a determinar se a configuração é o que você deseja em vigor para cada SVM. As informações exibidas também permitem verificar se uma configuração de auditoria está ativada.

Sobre esta tarefa

Você pode exibir informações detalhadas sobre configurações de auditoria em todos os SVMs ou pode personalizar quais informações são exibidas na saída especificando parâmetros opcionais. Se não especificar nenhum dos parâmetros opcionais, é apresentado o seguinte:

- Nome do SVM ao qual a configuração de auditoria se aplica
- O estado de auditoria, que pode ser `true` ou `false`

  Se o estado de auditoria for `true`, a auditoria será ativada. Se o estado de auditoria for `false`, a auditoria será desativada.

- As categorias de eventos a auditar
- O formato do log de auditoria
- O diretório de destino onde o subsistema de auditoria armazena logs de auditoria consolidados e convertidos

Passo

1. Exiba informações sobre a configuração de auditoria usando o `vserver audit show` comando.

   Para obter mais informações sobre como usar o comando, consulte as páginas de manual.

Exemplos

O exemplo a seguir exibe um resumo da configuração de auditoria de todos os SVMs:

```
cluster1::> vserver audit show

 Vserver     State  Event Types Log Format Target Directory
 ----------- ------ ----------- ---------- --------------------
 vs1         false  file-ops    evtx       /audit_log
```

O exemplo a seguir exibe, em forma de lista, todas as informações de configuração de auditoria para todos os SVMs:

```
cluster1::> vserver audit show -instance

                            Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops
                         Log Format: evtx
                  Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 0
```

Comandos para modificar configurações de auditoria

Se você quiser alterar uma configuração de auditoria, você pode modificar a configuração atual a qualquer momento, incluindo modificar o destino do caminho de log e o formato de log, modificar as categorias de eventos a auditar, como salvar automaticamente arquivos de log e especificar o número máximo de arquivos de log a serem salvos.

Se você quiser…	Use este comando…
Modifique o caminho de destino do log	`vserver audit modify` com o `-destination` parâmetro

Modifique a categoria de eventos para auditoria	`vserver audit modify` com o `-events` parâmetro Para auditar eventos de preparação de políticas de acesso central, a opção servidor SMB de controle de acesso dinâmico (DAC) deve estar ativada na máquina virtual de armazenamento (SVM).
Modifique o formato do log	`vserver audit modify` com o `-format` parâmetro
Ativar gravações automáticas com base no tamanho do ficheiro de registo interno	`vserver audit modify` com o `-rotate-size` parâmetro
Ativar as gravações automáticas com base num intervalo de tempo	`vserver audit modify` com os `-rotate -schedule-month` parâmetros , `-rotate -schedule-dayofweek`, `-rotate-schedule-day`, `-rotate-schedule-hour` e `-rotate -schedule-minute`
Especificar o número máximo de ficheiros de registo guardados	`vserver audit modify` com o `-rotate-limit` parâmetro

Excluir uma configuração de auditoria

Se você não quiser mais auditar eventos de arquivo e diretório na máquina virtual de storage (SVM) e não quiser manter uma configuração de auditoria na SVM, é possível excluir a configuração de auditoria.

Passos

1. Desative a configuração de auditoria:

```
vserver audit disable -vserver vserver_name

vserver audit disable -vserver vs1
```

2. Excluir a configuração de auditoria:

```
vserver audit delete -vserver vserver_name

vserver audit delete -vserver vs1
```

Entenda as implicações de reverter o cluster

Se você pretende reverter o cluster, deve estar ciente do processo de reversão que o ONTAP segue quando houver máquinas virtuais de storage (SVMs) habilitadas para

auditoria no cluster. Você deve tomar certas ações antes de reverter.

Revertendo para uma versão do ONTAP que não suporte a auditoria de eventos de logon e logoff SMB e eventos de preparação de políticas de acesso central

O suporte para auditoria de eventos de logon e logoff SMB e para eventos de preparação de políticas de acesso central começa com o Clustered Data ONTAP 8.3. Se você estiver revertendo para uma versão do ONTAP que não ofereça suporte a esses tipos de eventos e tiver configurações de auditoria que monitorem esses tipos de eventos, será necessário alterar a configuração de auditoria desses SVMs habilitados para auditoria antes de reverter. Você deve modificar a configuração para que apenas eventos de arquivo operacional sejam auditados.

Solucionar problemas de volume de auditoria e preparação

Problemas podem surgir quando não houver espaço suficiente nos volumes de teste ou no volume que contém os logs de eventos de auditoria. Se não houver espaço suficiente, novos Registros de auditoria não podem ser criados, o que impede que os clientes acessem dados e as solicitações de acesso falhem. Você deve saber como solucionar e resolver esses problemas de espaço de volume.

Solucionar problemas de espaço relacionados aos volumes de log de eventos

Se os volumes contendo arquivos de log de eventos ficarem sem espaço, a auditoria não poderá converter Registros de log em arquivos de log. Isso resulta em falhas de acesso do cliente. Você deve saber como solucionar problemas de espaço relacionados aos volumes de log de eventos.

- Os administradores de cluster e máquina virtual de storage (SVM) podem determinar se há espaço de volume insuficiente exibindo informações sobre o volume e o uso e a configuração agregados.
- Se houver espaço insuficiente nos volumes que contêm logs de eventos, os administradores de SVM e cluster poderão resolver os problemas de espaço removendo alguns dos arquivos de log de eventos ou aumentando o tamanho do volume.

> Se o agregado que contém o volume do log de eventos estiver cheio, o tamanho do agregado deve ser aumentado antes que você possa aumentar o tamanho do volume. Somente um administrador de cluster pode aumentar o tamanho de um agregado.

- O caminho de destino para os arquivos de log de eventos pode ser alterado para um diretório em outro volume, modificando a configuração de auditoria.

> O acesso aos dados é negado nos seguintes casos:
>
> - O diretório de destino é excluído.
> - O limite de arquivo em um volume, que hospeda o diretório de destino, atinge seu nível máximo.

Saiba mais sobre:

- "Como visualizar informações sobre volumes e aumentar o tamanho do volume".
- "Como visualizar informações sobre agregados e gerenciar agregados".

Solucionar problemas de espaço relacionados aos volumes de teste

Se algum dos volumes que contém arquivos de teste para a máquina virtual de armazenamento (SVM) ficar sem espaço, a auditoria não poderá gravar Registros de log em arquivos de teste. Isso resulta em falhas de acesso do cliente. Para solucionar esse problema, você precisa determinar se algum dos volumes de teste usados no SVM está cheio exibindo informações sobre o uso de volume.

Se o volume que contém os arquivos de log de eventos consolidados tiver espaço suficiente, mas ainda houver falhas de acesso do cliente devido a espaço insuficiente, os volumes de teste podem estar fora do espaço. O administrador do SVM deve entrar em Contato com você para determinar se os volumes de teste que contêm arquivos de teste para o SVM têm espaço insuficiente. O subsistema de auditoria gera um evento EMS se os eventos de auditoria não puderem ser gerados devido a espaço insuficiente em um volume de teste. É apresentada a seguinte mensagem: `No space left on device`. Somente você pode exibir informações sobre volumes de teste; os administradores do SVM não podem.

Todos os nomes de volume de estadiamento começam com `MDV_aud_` seguido pelo UUID do agregado que contém esse volume de estadiamento. O exemplo a seguir mostra quatro volumes de sistema no SVM admin, que foram criados automaticamente quando uma configuração de auditoria de serviços de arquivo foi criada para um data SVM no cluster:

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
                       aggr0        online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          5GB     4.75GB
5%
4 entries were displayed.
```

Se não houver espaço suficiente nos volumes de teste, você poderá resolver os problemas de espaço aumentando o tamanho do volume.

> Se o agregado que contém o volume de estadiamento estiver cheio, o tamanho do agregado deverá ser aumentado antes de poder aumentar o tamanho do volume. Somente você pode aumentar o tamanho de um agregado. Os administradores de SVM não podem.

Se um ou mais agregados tiverem um espaço disponível inferior a 2GB TB (no ONTAP 9.14,1 e anterior) ou 5GB TB (começando com o ONTAP 9.15,1), a criação da auditoria SVM falhará. Quando a criação da auditoria SVM falhar, os volumes de teste criados são excluídos.

Informações sobre direitos autorais

Informações sobre marcas comerciais