Como funciona a auditoria

ONTAP 9

NetApp
January 17, 2025

Índice

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.

Informações sobre direitos autorais

Informações sobre marcas comerciais