Configurar políticas de auditoria de arquivos e pastas

ONTAP 9

NetApp
January 17, 2025

Índice

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.

Informações sobre direitos autorais

Informações sobre marcas comerciais