



Proteja o acesso aos arquivos usando permissões de arquivo

ONTAP 9

NetApp
January 17, 2025

Índice

- Proteja o acesso aos arquivos usando permissões de arquivo 1
 - Configure permissões avançadas de arquivos NTFS usando a guia Segurança do Windows 1
 - Configurar permissões de arquivos NTFS usando a CLI do ONTAP 4
 - Como as permissões de arquivo UNIX fornecem controle de acesso ao acessar arquivos por SMB 4

Proteja o acesso aos arquivos usando permissões de arquivo

Configure permissões avançadas de arquivos NTFS usando a guia **Segurança do Windows**

Você pode configurar permissões de arquivo NTFS padrão em arquivos e pastas usando a guia **Segurança do Windows** na janela Propriedades do Windows.

Antes de começar

O administrador que executa esta tarefa deve ter permissões NTFS suficientes para alterar permissões nos objetos selecionados.

Sobre esta tarefa

A configuração de permissões de arquivos NTFS é feita em um host do Windows adicionando entradas a listas de controle de acesso discricionárias (DACLS) NTFS 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.

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 nome do servidor CIFS que contém o compartilhamento que contém os dados aos quais você deseja aplicar permissões e o nome do compartilhamento.

Se o nome do servidor CIFS for "CIFS_SERVER" e o compartilhamento for chamado "hare1", você deverá digitar \\CIFS_SERVER\share1.



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

- 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 deseja definir permissões de arquivo NTFS.
4. Clique com o botão direito do rato no ficheiro ou diretório e selecione **Propriedades**.
5. Selecione a guia **Segurança**.

A guia **Segurança** exibe a lista de usuários e grupos para os quais a permissão NTFS está definida. A caixa **Permissions for** exibe uma lista de permissões de permissão e negação em vigor para cada usuário ou grupo selecionado.

6. Clique em **Avançado**.

A janela Propriedades do Windows exibe informações sobre permissões de arquivo existentes atribuídas a

usuários e grupos.

7. Clique em **alterar permissões**.

A janela permissões é aberta.

8. Execute as ações desejadas:

Se você quiser...	Faça o seguinte...
Configurar permissões NTFS avançadas para um novo utilizador ou grupo	<ol style="list-style-type: none">Clique em Add.Na caixa Digite o nome do objeto a ser selecionado, digite o nome do usuário ou grupo que deseja adicionar.Clique em OK.
Alterar permissões NTFS avançadas de um usuário ou grupo	<ol style="list-style-type: none">Na caixa entradas de permissões:, selecione o usuário ou grupo cujas permissões avançadas você deseja alterar.Clique em Editar.
Remover permissões NTFS avançadas para um usuário ou grupo	<ol style="list-style-type: none">Na caixa entradas de permissões:, selecione o usuário ou grupo que deseja remover.Clique em Remover.Avance para o passo 13.

Se você estiver adicionando permissões NTFS avançadas em um novo usuário ou grupo ou alterando permissões avançadas NTFS em um usuário ou grupo existente, a caixa Entrada de permissão para <Object> será aberta.

9. Na caixa **Apply to**, selecione como você deseja aplicar esta entrada de permissão de arquivo NTFS.

Se você estiver configurando permissões de arquivo NTFS em um único arquivo, a caixa **Apply to** não estará ativa. A configuração **apply to** é padrão para **this object only**.

10. Na caixa **Permissions**, selecione as caixas **allow** ou **deny** para as permissões avançadas que você deseja definir neste objeto.

- Para permitir o acesso especificado, selecione a caixa **permitir**.
- Para não permitir o acesso especificado, selecione a caixa **Negar**. Você pode definir permissões nos seguintes direitos avançados:
- * Controle total*

Se você escolher esse direito avançado, todos os outros direitos avançados serão escolhidos automaticamente (permitir ou negar direitos).

- * 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**



Se qualquer uma das caixas de permissão avançada não for selecionável, é porque as permissões são herdadas do objeto pai.

11. Se você quiser que subpastas e arquivos desse objeto herdem essas permissões, marque a caixa **aplicar essas permissões a objetos e/ou contentores dentro desse contentor somente**.
12. Clique em **OK**.
13. Depois de terminar de adicionar, remover ou editar permissões NTFS, especifique a configuração de herança para este objeto:

- Selecione a caixa **incluir permissões herdadas a partir da caixa pai** deste objeto.

Este é o padrão.

- Selecione a caixa **Substituir todas as permissões de objeto filho por permissões herdadas deste objeto**.

Esta configuração não está presente na caixa permissões se você estiver definindo permissões de arquivo NTFS em um único arquivo.



Tenha cuidado ao selecionar esta definição. Esta configuração remove todas as permissões existentes em todos os objetos filho e as substitui pelas configurações de permissão deste objeto. Você pode remover inadvertidamente as permissões que você não queria que fossem removidas. É especialmente importante ao definir permissões em um volume ou qtree misto de estilo de segurança. Se objetos filho tiverem um estilo de segurança eficaz UNIX, propagar permissões NTFS para esses objetos filho resulta na alteração do ONTAP desses objetos do estilo de segurança UNIX para o estilo de segurança NTFS e todas as permissões UNIX nesses objetos filho serão substituídas por permissões NTFS.

- Selecione ambas as caixas.
- Selecione nenhuma das caixas.

14. Clique em **OK** para fechar a caixa **permissões**.
15. Clique em **OK** para fechar a caixa **Configurações avançadas de segurança para o <Object>**.

Para obter mais informações sobre como definir permissões NTFS avançadas, consulte a documentação do Windows.

Informações relacionadas

[Configure e aplique segurança de arquivos em arquivos e pastas NTFS usando a CLI](#)

[Exibindo informações sobre segurança de arquivos em volumes de estilo de segurança NTFS](#)

[Exibindo informações sobre segurança de arquivos em volumes mistos de estilo de segurança](#)

[Exibindo informações sobre segurança de arquivos em volumes estilo de segurança UNIX](#)

Configurar permissões de arquivos NTFS usando a CLI do ONTAP

Você pode configurar permissões de arquivos NTFS em arquivos e diretórios usando a CLI do ONTAP. Isso permite configurar permissões de arquivos NTFS sem precisar se conectar aos dados usando um compartilhamento SMB em um cliente Windows.

Você pode configurar permissões de arquivo NTFS adicionando entradas a listas de controle de acesso discricionário NTFS (DACLS) associadas a um descritor de segurança NTFS. O descritor de segurança é então aplicado a arquivos e diretórios NTFS.

Você só pode configurar permissões de arquivo NTFS usando a linha de comando. Você não pode configurar ACLs NFSv4 usando a CLI.

Passos

1. Crie um descritor de segurança NTFS.

```
vserver security file-directory ntfs create -vserver svm_name -ntfs-sd  
ntfs_security_descriptor_name -owner owner_name -group primary_group_name  
-control-flags-raw raw_control_flags
```

2. Adicione DACLS ao descritor de segurança NTFS.

```
vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd  
ntfs_security_descriptor_name -access-type {deny|allow} -account account_name  
-rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to  
{this-folder|sub-folders|files}
```

3. Crie uma política de segurança de arquivo/diretório.

```
vserver security file-directory policy create -vserver svm_name -policy-name  
policy_name
```

Como as permissões de arquivo UNIX fornecem controle de acesso ao acessar arquivos por SMB

Um FlexVol volume pode ter um dos três tipos de estilo de segurança: NTFS, UNIX ou misto. Você pode acessar dados sobre SMB independentemente do estilo de segurança; no entanto, permissões de arquivo UNIX apropriadas são necessárias para acessar dados com segurança efetiva UNIX.

Quando os dados são acessados por SMB, há vários controles de acesso usados para determinar se um usuário está autorizado a executar uma ação solicitada:

- Permissões de exportação

Configurar permissões de exportação para o acesso SMB é opcional.

- Permissões de compartilhamento
- Permissões de arquivo

Os seguintes tipos de permissões de arquivo podem ser aplicados aos dados nos quais o usuário deseja executar uma ação:

- NTFS
- ACLs do UNIX NFSv4
- Bits do modo UNIX

Para dados com ACLs NFSv4 ou bits de modo UNIX definidos, as permissões de estilo UNIX são usadas para determinar os direitos de acesso aos dados. O administrador do SVM precisa definir a permissão de arquivo apropriada para garantir que os usuários tenham os direitos para executar a ação desejada.



Os dados em um volume misto de estilo de segurança podem ter um estilo de segurança eficaz NTFS ou UNIX. Se os dados tiverem um estilo de segurança eficaz UNIX, as permissões NFSv4 ou os bits de modo UNIX serão usados ao determinar os direitos de acesso aos dados.

Informações sobre direitos autorais

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

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

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

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

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

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

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

Informações sobre marcas comerciais

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