



# **Configurar o acesso de cliente SMB ao armazenamento compartilhado**

ONTAP 9

NetApp  
January 17, 2025

# Índice

- Configurar o acesso de cliente SMB ao armazenamento compartilhado ..... 1
  - Configurar o acesso de cliente SMB ao armazenamento compartilhado ..... 1
  - Crie um volume ou um contêiner de storage de qtree ..... 1
  - Requisitos e considerações para criar um compartilhamento SMB ..... 4
  - Crie um compartilhamento SMB ..... 5
  - Verifique o acesso do cliente SMB ..... 6
  - Criar listas de controle de acesso de compartilhamento SMB ..... 7
  - Configurar permissões de arquivo NTFS em um compartilhamento ..... 9
  - Verifique o acesso do usuário ..... 10

# Configurar o acesso de cliente SMB ao armazenamento compartilhado

## Configurar o acesso de cliente SMB ao armazenamento compartilhado

Para fornecer acesso de cliente SMB ao storage compartilhado em uma SVM, você precisa criar um volume ou qtree para fornecer um contêiner de storage e, em seguida, criar ou modificar um compartilhamento para esse contêiner. Em seguida, você pode configurar permissões de compartilhamento e arquivo e testar o acesso a partir de sistemas cliente.

### Antes de começar

- O SMB deve estar completamente configurado no SVM.
- Todas as atualizações da configuração dos serviços de nome devem estar concluídas.
- Quaisquer adições ou modificações a um domínio do Active Directory ou configuração de grupo de trabalho devem estar concluídas.

## Crie um volume ou um contêiner de storage de qtree

### Crie um volume

Você pode criar um volume e especificar seu ponto de junção e outras propriedades usando o `volume create` comando.

### Sobre esta tarefa

Um volume deve incluir um *caminho de junção* para que seus dados sejam disponibilizados aos clientes. Você pode especificar o caminho de junção ao criar um novo volume. Se você criar um volume sem especificar um caminho de junção, será necessário *montar* o volume no namespace SVM usando o `volume mount` comando.

### Antes de começar

- O SMB deve ser configurado e executado.
- O estilo de segurança da SVM deve ser NTFS.
- A partir do ONTAP 9.13.1, você pode criar volumes com análise de capacidade e acompanhamento de atividades habilitados. Para ativar o acompanhamento de capacidade ou atividade, emita o `volume create` comando com `-analytics-state` ou `-activity-tracking-state` defina como `on`.

Para saber mais sobre análise de capacidade e acompanhamento de atividades, ["Ative a análise do sistema de arquivos"](#) consulte .

### Passos

1. Crie o volume com um ponto de junção: 

```
volume create -vserver svm_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style ntfs -junction-path junction_path
```

As opções para `-junction-path` são as seguintes:

- Diretamente sob a raiz, por exemplo, `/new_vol`

Você pode criar um novo volume e especificar que ele seja montado diretamente no volume raiz da SVM.

- Em um diretório existente, por exemplo, `/existing_dir/new_vol`

Você pode criar um novo volume e especificar que ele seja montado em um volume existente (em uma hierarquia existente), expresso como um diretório.

Se você quiser criar um volume em um novo diretório (em uma nova hierarquia em um novo volume), por exemplo, `/new_dir/new_vol` será necessário criar primeiro um novo volume pai que seja juntado ao volume raiz SVM. Em seguida, você criaria o novo volume filho no caminho de junção do novo volume pai (novo diretório).

2. Verifique se o volume foi criado com o ponto de junção desejado: `volume show -vserver svm_name -volume volume_name -junction`

### Exemplos

O comando a seguir cria um novo volume chamado `users1` no SVM `vs1.example.com` e no agregado `aggr1`. O novo volume é disponibilizado em `/users`. O volume tem 750 GB de tamanho e sua garantia de volume é do tipo `volume` (por padrão).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
```

Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1.example.com	users1	true	/users	RW_volume

O comando a seguir cria um novo volume chamado `"home4"` na SVM `vs1.example.com` e o agregado `"aggr1"`. O diretório `/eng/` já existe no namespace para o VS1 SVM, e o novo volume é disponibilizado no `/eng/home`, que se torna o diretório `home` do `/eng/` namespace. O volume é de 750 GB de tamanho e sua garantia de volume é do tipo `volume` (por padrão).

```

cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction

```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	home4	true	/eng/home	RW_volume

## Crie uma qtree

Você pode criar uma qtree para conter seus dados e especificar suas propriedades usando o `volume qtree create` comando.

### Antes de começar

- O SVM e o volume que conterá a nova qtree já devem existir.
- O estilo de segurança da SVM deve ser NTFS e o SMB deve ser configurado e executado.

### Passos

1. Crie a qtree: `volume qtree create -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path } -security-style ntfs`

Você pode especificar o volume e a qtree como argumentos separados ou especificar o argumento de caminho de qtree no formato `/vol/volume_name/_qtree_name`.

2. Verifique se a qtree foi criada com o caminho de junção desejado: `volume qtree show -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path }`

### Exemplo

O exemplo a seguir cria uma qtree chamada qt01 localizada no SVM vs1.example.com que tem um caminho de junção `/vol/data1`:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style ntfs
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01
```

```
          Vserver Name: vs1.example.com
          Volume Name: data1
          Qtree Name: qt01
Actual (Non-Junction) Qtree Path: /vol/data1/qt01
          Security Style: ntfs
          Oplock Mode: enable
          Unix Permissions: ---rwxr-xr-x
          Qtree Id: 2
          Qtree Status: normal
          Export Policy: default
Is Export Policy Inherited: true
```

## Requisitos e considerações para criar um compartilhamento SMB

Antes de criar um compartilhamento SMB, você deve entender os requisitos para caminhos de compartilhamento e propriedades de compartilhamento, especialmente para diretórios base.

Criar um compartilhamento SMB implica especificar uma estrutura de caminho de diretório (usando a `-path` opção no `vserver cifs share create` comando) que os clientes acessarão. O caminho do diretório corresponde ao caminho de junção de um volume ou `qtree` que você criou no namespace SVM. O caminho do diretório e o caminho de junção correspondente devem existir antes de criar seu compartilhamento.

Os caminhos de compartilhamento têm os seguintes requisitos:

- Um nome de caminho de diretório pode ter até 255 caracteres.
- Se houver um espaço no nome do caminho, toda a cadeia de caracteres deve ser colocada em aspas (por exemplo, `"/new volume/mount here"`).
- Se o caminho UNC (`\\servername\sharename\filepath`) do compartilhamento contiver mais de 256 caracteres (excluindo o `""` inicial no caminho UNC), a guia **Segurança** na caixa Propriedades do Windows não estará disponível.

Este é um problema de cliente do Windows em vez de um problema de ONTAP. Para evitar esse problema, não crie compartilhamentos com caminhos UNC com mais de 256 caracteres.

Os padrões de propriedade de compartilhamento podem ser alterados:

- As propriedades iniciais padrão para todos os compartilhamentos são `oplocks`, `browsable`,

`changenotify` e `show-previous-versions`.

- É opcional especificar propriedades de compartilhamento quando você cria um compartilhamento.

No entanto, se você especificar propriedades de compartilhamento ao criar o compartilhamento, os padrões não serão usados. Se você usar o `-share-properties` parâmetro ao criar um compartilhamento, especifique todas as propriedades de compartilhamento que deseja aplicar ao compartilhamento usando uma lista delimitada por vírgulas.

- Para designar um compartilhamento de diretório base, use a `homedirectory` propriedade.

Este recurso permite configurar um compartilhamento que mapeia para diferentes diretórios com base no usuário que se conecta a ele e um conjunto de variáveis. Em vez de ter que criar compartilhamentos separados para cada usuário, você pode configurar um único compartilhamento com alguns parâmetros do diretório base para definir a relação de um usuário entre um ponto de entrada (o compartilhamento) e seu diretório inicial (um diretório no SVM).



Não é possível adicionar ou remover esta propriedade depois de criar a partilha.

Os compartilhamentos do diretório base têm os seguintes requisitos:

- Antes de criar diretórios home do SMB, você deve adicionar pelo menos um caminho de pesquisa do diretório home usando o `vserver cifs home-directory search-path add` comando.
- Os compartilhamentos do diretório base especificados pelo valor de `homedirectory` no `-share-properties` parâmetro devem incluir a `%w` variável dinâmica (nome de usuário do Windows) no nome do compartilhamento.

O nome do compartilhamento pode também conter a `%d` variável dinâmica (nome de domínio) (por exemplo, `%d/%w`) ou uma parte estática no nome do compartilhamento (por exemplo, `home1_%w`).

- Se o compartilhamento for usado por administradores ou usuários para se conectar a diretórios home de outros usuários (usando opções para o `vserver cifs home-directory modify` comando), o padrão de nome de compartilhamento dinâmico deve ser precedido por um til (~).

"Gerenciamento de SMB" e `vserver cifs share` as páginas de manual têm informações adicionais.

## Crie um compartilhamento SMB

Você deve criar um compartilhamento SMB antes de compartilhar dados de um servidor SMB com clientes SMB. Ao criar um compartilhamento, você pode definir propriedades de compartilhamento, como designar o compartilhamento como um diretório inicial. Você também pode personalizar o compartilhamento configurando configurações opcionais.

### Antes de começar

O caminho do diretório para o volume ou `qtree` deve existir no namespace SVM antes de criar o compartilhamento.

### Sobre esta tarefa

Quando você cria um compartilhamento, a ACL de compartilhamento padrão (permissões de compartilhamento padrão) é `Everyone / Full Control`. Depois de testar o acesso ao compartilhamento, você deve remover a ACL de compartilhamento padrão e substituí-la por uma alternativa mais segura.

## Passos

1. Se necessário, crie a estrutura do caminho do diretório para o compartilhamento.

O `vserver cifs share create` comando verifica o caminho especificado na `-path` opção durante a criação de compartilhamento. Se o caminho especificado não existir, o comando falhará.

2. Crie um compartilhamento SMB associado ao SVM especificado: `vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [other_attributes] [-comment text]`
3. Verifique se o compartilhamento foi criado: `vserver cifs share show -share-name share_name`

## Exemplos

O comando a seguir cria um compartilhamento SMB chamado "SHARE1" no SVM `vs1.example.com`. Seu caminho de diretório é `/users`, e é criado com propriedades padrão.

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name SHARE1 -path /users
```

```
cluster1::> vserver cifs share show -share-name SHARE1
```

Vserver	Share	Path	Properties	Comment	ACL
vs1.example.com	SHARE1	/users	oplocks browsable changenotify show-previous-versions	-	Everyone / Full Control

## Verifique o acesso do cliente SMB

Você deve verificar se configurou o SMB corretamente acessando e gravando dados no compartilhamento. Você deve testar o acesso usando o nome do servidor SMB e quaisquer aliases NetBIOS.

### Passos

1. Faça login em um cliente Windows.
2. Teste o acesso usando o nome do servidor SMB:
  - a. No Explorador do Windows, mapeie uma unidade para a partilha no seguinte formato: `\\SMB_Server_Name\Share_Name`

Se o mapeamento não for bem-sucedido, é possível que o mapeamento DNS ainda não tenha se propagado pela rede. Você deve testar o acesso usando o nome do servidor SMB posteriormente.

Se o servidor SMB tiver o nome `vs1.example.com` e o compartilhamento tiver o nome `SHARE1`, você deverá inserir o seguinte: `\\vs0.example.com\SHARE1`



b. Na unidade recém-criada, crie um arquivo de teste e exclua o arquivo.

Você verificou o acesso de gravação ao compartilhamento usando o nome do servidor SMB.

3. Repita a Etapa 2 para qualquer alias NetBIOS.

## Criar listas de controle de acesso de compartilhamento SMB

A configuração de permissões de compartilhamento criando listas de controle de acesso (ACLs) para compartilhamentos SMB permite controlar o nível de acesso a um compartilhamento para usuários e grupos.

### Antes de começar

Você deve ter decidido quais usuários ou grupos terão acesso ao compartilhamento.

### Sobre esta tarefa

Você pode configurar ACLs de nível de compartilhamento usando nomes de usuário ou grupo do Windows locais ou de domínio.

Antes de criar uma nova ACL, você deve excluir a ACL de compartilhamento padrão `Everyone / Full Control`, que representa um risco de segurança.

No modo de grupo de trabalho, o nome de domínio local é o nome do servidor SMB.

### Passos

1. Excluir a ACL de compartilhamento padrão:

```
vserver cifs share access-control delete -vserver vserver_name -share share_name -user-or-group everyone
```
2. Configure a nova ACL:

Se você quiser configurar ACLs usando um...	Digite o comando...
Usuário do Windows	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name\\user_name -permission access_right</pre>
Grupo Windows	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_group_name -permission access_right</pre>

3. Verifique se a ACL aplicada ao compartilhamento está correta usando o `vserver cifs share access-control show` comando.

### Exemplo

O comando a seguir Change dá permissões ao grupo Windows "equipe de vendas" para o compartilhamento "vendas" no vs1.example.com`"SVM:

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vserver cifs share access-control show

Vserver      Share      User/Group      User/Group  Access
Permission   Name       Name            Type
-----
vs1.example.com  c$        BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales     DOMAIN\"Sales Team"    windows    Change
```

Os comandos a seguir Change dão permissão ao grupo local do Windows chamado "Tiger Team" e Full\_Control permissão ao usuário local do Windows chamado "Sue Chang" para o compartilhamento "d.atavol5" no "VS1" SVM:

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1

Vserver      Share      User/Group      User/Group  Access
Permission   Name       Name            Type
-----
vs1          c$        BUILTIN\Administrators  windows
Full_Control
vs1          datavol5  DOMAIN\"Tiger Team"    windows    Change
vs1          datavol5  DOMAIN\"Sue Chang"    windows
```

# Configurar permissões de arquivo NTFS em um compartilhamento

Para habilitar o acesso a arquivos aos usuários ou grupos que têm acesso a um compartilhamento, você deve configurar permissões de arquivo NTFS em arquivos e diretórios nesse compartilhamento a partir de um cliente Windows.

## Antes de começar

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

## Sobre esta tarefa

"[Gerenciamento de SMB](#)" E a documentação do Windows contém informações sobre como definir permissões NTFS padrão e avançadas.

## Passos

1. Inicie sessão num cliente Windows como administrador.
2. No menu **Ferramentas** no Windows Explorer, selecione **Mapear unidade de rede**.
3. 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 que contém os dados aos quais você deseja aplicar permissões e o nome do compartilhamento.

Se o nome do servidor SMB for SMB\_SERVER01 e o compartilhamento for chamado "SHARE1", você digitaria \\SMB\_SERVER01\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.

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

A guia Segurança exibe a lista de usuários e grupos para os quais a permissão NTFS está definida. A caixa permissões para <Object> exibe uma lista de permissões de permissão e negação em vigor para o usuário ou grupo selecionado.

7. Clique em **Editar**.

A caixa permissões para <Object> será aberta.

8. Execute as ações desejadas:

Se você quiser	Faça o seguinte...
Defina permissões NTFS padrão para um novo usuário ou grupo	<p>a. Clique em <b>Add</b>.</p> <p>A janela Selecionar usuário, computadores, contas de serviço ou grupos será exibida.</p> <p>b. Na caixa <b>Digite os nomes de objeto a selecionar</b>, digite o nome do usuário ou grupo no qual você deseja adicionar permissão NTFS.</p> <p>c. Clique em <b>OK</b>.</p>
Alterar ou remover permissões NTFS padrão de um usuário ou grupo	Na caixa <b>Group (Grupo) ou User Names (nomes de usuário)</b> , selecione o usuário ou grupo que deseja alterar ou remover.

9. Execute as ações desejadas:

Se você quiser...	Faça o seguinte
Defina permissões NTFS padrão para um usuário ou grupo novo ou existente	Na caixa <b>Permissions for &lt;Object&gt;</b> , selecione as caixas <b>allow</b> ou <b>deny</b> para o tipo de acesso que você deseja permitir ou não permitir para o usuário ou grupo selecionado.
Remover um usuário ou grupo	Clique em <b>Remover</b> .



Se algumas ou todas as caixas de permissão padrão não forem selecionáveis, é porque as permissões são herdadas do objeto pai. A caixa **Special Permissions** não é selecionável. Se estiver selecionado, significa que um ou mais direitos avançados granulares foram definidos para o usuário ou grupo selecionado.

10. Depois de terminar de adicionar, remover ou editar permissões NTFS nesse objeto, clique em **OK**.

## Verifique o acesso do usuário

Você deve testar se os usuários configurados podem acessar o compartilhamento SMB e os arquivos nele contidos.

### Passos

1. Em um cliente Windows, faça login como um dos usuários que agora tem acesso ao compartilhamento.
2. No menu **Ferramentas** no Windows Explorer, selecione **Mapear unidade de rede**.
3. Preencha a caixa **Map Network Drive**:
  - a. Selecione uma letra **Drive**.
  - b. Na caixa **pasta**, digite o nome do compartilhamento que você fornecerá aos usuários.

Se o nome do servidor SMB for SMB\_SERVER01 e o compartilhamento for chamado "SHARE1",

você digitaria \\SMB\_SERVER01\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.

4. Crie um arquivo de teste, verifique se ele existe, escreva texto nele e remova o arquivo de teste.

## 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.