



Implante serviços baseados em servidor SMB

ONTAP 9

NetApp
January 17, 2025

Índice

Implante serviços baseados em servidor SMB	1
Gerenciar diretórios base	1
Configurar o acesso de cliente SMB a links simbólicos UNIX	14
Use BranchCache para armazenar em cache conteúdo de compartilhamento SMB em uma filial	23
Melhorar o desempenho de cópia remota da Microsoft	55
Melhore o tempo de resposta do cliente fornecendo referências de nó automáticas SMB com localização automática	61
Forneça segurança de pastas em compartilhamentos com enumeração baseada em acesso	68

Implante serviços baseados em servidor SMB

Gerenciar diretórios base

Como o ONTAP ativa diretórios base dinâmicos

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

Um usuário que está conectado como um usuário convidado não tem um diretório home e não pode acessar os diretórios home de outros usuários. Existem quatro variáveis que determinam como um usuário é mapeado para um diretório:

- **Nome da partilha**

Este é o nome do compartilhamento que você cria ao qual o usuário se conecta. Você deve definir a propriedade do diretório base para esse compartilhamento.

O nome do compartilhamento pode usar os seguintes nomes dinâmicos:

- `%w` (O nome de utilizador do Windows do utilizador)
- `%d` (O nome de domínio do Windows do utilizador)
- `%u` (O nome de usuário UNIX mapeado do usuário) para tornar o nome de compartilhamento exclusivo em todos os diretórios base, o nome de compartilhamento deve conter `a/%w` variável ou `%u`. O nome do compartilhamento pode conter tanto a `%d` e `a/%w` variável (por exemplo, `%d/%w`), ou o nome do compartilhamento pode conter uma porção estática e uma porção variável (por exemplo, `Home_/%w`).

- **Caminho de compartilhamento**

Este é o caminho relativo, que é definido pelo compartilhamento e, portanto, está associado a um dos nomes de compartilhamento, que é anexado a cada caminho de pesquisa para gerar o caminho do diretório home inteiro do usuário a partir da raiz do SVM. Pode ser estático (por exemplo, `home`), dinâmico (por exemplo, `%w`) ou uma combinação dos dois (por exemplo, `eng/%w`).

- **Pesquisar caminhos**

Esse é o conjunto de caminhos absolutos da raiz do SVM que você especifica que direciona a busca do ONTAP por diretórios base. Você pode especificar um ou mais caminhos de pesquisa usando o `vserver cifs home-directory search-path add` comando. Se você especificar vários caminhos de pesquisa, o ONTAP os tentará na ordem especificada até encontrar um caminho válido.

- **Diretório**

Este é o diretório home do usuário que você cria para o usuário. O nome do diretório é geralmente o nome do usuário. Você deve criar o diretório home em um dos diretórios que são definidos pelos caminhos de pesquisa.

Como exemplo, considere a seguinte configuração:

- Usuário: John Smith
- Domínio de usuário: acme
- Nome de usuário: jsmith
- Nome do SVM: VS1
- Nome de compartilhamento de diretório base nº 1: Home_ %w - caminho de compartilhamento: %w
- Nome de compartilhamento do diretório base nº 2: %w - Caminho de compartilhamento: %d/%w
- Caminho de pesquisa nº 1: /vol0home/home
- Caminho de pesquisa nº 2: /vol1home/home
- Caminho de pesquisa nº 3: /vol2home/home
- Diretório base: /vol1home/home/jsmith

Cenário 1: O usuário se conecta `\\vs1\home_jsmith` ao . Isso corresponde ao primeiro nome de compartilhamento do diretório inicial e gera o caminho `jsmith`relativo` . O ONTAP procura agora um diretório nomeado ``jsmith` verificando cada caminho de pesquisa em ordem:

- `/vol0home/home/jsmith` não existe; passando para o caminho de pesquisa nº 2.
- `/vol1home/home/jsmith` existe; portanto, o caminho de pesquisa nº 3 não está marcado; o usuário agora está conectado ao seu diretório inicial.

Cenário 2: O usuário se conecta `\\vs1\jsmith` ao . Isso corresponde ao segundo nome de compartilhamento do diretório inicial e gera o caminho `acme/jsmith`relativo` . O ONTAP procura agora um diretório nomeado ``acme/jsmith` verificando cada caminho de pesquisa em ordem:

- `/vol0home/home/acme/jsmith` não existe; passando para o caminho de pesquisa nº 2.
- `/vol1home/home/acme/jsmith` não existe; passando para o caminho de pesquisa nº 3.
- `/vol2home/home/acme/jsmith` não existe; o diretório home não existe; portanto, a conexão falha.

Compartilhamentos de diretório base

Adicione um compartilhamento de diretório base

Se você quiser usar o recurso diretório base SMB, você deve adicionar pelo menos um compartilhamento com a propriedade diretório base incluída nas propriedades de compartilhamento.

Sobre esta tarefa

Você pode criar um compartilhamento de diretório inicial no momento em que você cria o compartilhamento usando o `vserver cifs share create` comando, ou você pode alterar um compartilhamento existente em um compartilhamento de diretório inicial a qualquer momento usando o `vserver cifs share modify` comando.

Para criar um compartilhamento de diretório inicial, você deve incluir o `homedirectory` valor na `-share -properties` opção quando criar ou modificar um compartilhamento. Você pode especificar o nome do compartilhamento e o caminho do compartilhamento usando variáveis que são expandidas dinamicamente

quando os usuários se conectam a seus diretórios base. As variáveis disponíveis que você pode usar no caminho são `%w`, `%d` e `%u`, correspondentes ao nome de usuário, domínio e nome de usuário UNIX mapeado do Windows, respectivamente.

Passos

1. Adicionar um diretório de casa compartilhado `vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties homedirectory[,...]`

`-vserver vserver` Especifica a máquina virtual de storage (SVM) habilitada para CIFS na qual adicionar o caminho de pesquisa.

`-share-name share_name` especifica o nome de compartilhamento do diretório base.

Além de conter uma das variáveis necessárias, se o nome do compartilhamento contiver uma das strings literais `%w`, `%u`, ou `%d`, você deve preceder a string literal com um caractere `%` (percentual) para impedir que o ONTAP trate a string literal como uma variável (por exemplo, `%%w`).

- O nome do compartilhamento deve conter a `%w` variável ou `%u`.
- O nome do compartilhamento também pode conter a `%d` variável (por exemplo, `%d/%w`) ou uma parte estática no nome do compartilhamento (por exemplo, `home1_/%w`).
- Se o compartilhamento for usado pelos administradores para se conectar aos diretórios home de outros usuários ou para permitir que os usuários se conectem aos diretórios home de outros usuários, o padrão de nome de compartilhamento dinâmico deve ser precedido por um til (`.`).

```
`vserver cifs home-directory modify`O é utilizado para ativar este acesso definindo `-is-home-dirs-access-for-admin-enabled` a opção como `true`) ou definindo a opção avançada `-is-home-dirs-access-for-public-enabled` como `true`.
```

`-path path` especifica o caminho relativo para o diretório home.

`-share-properties homedirectory[,...]` especifica as propriedades de compartilhamento para esse compartilhamento. Você deve especificar o `homedirectory` valor. Você pode especificar propriedades de compartilhamento adicionais usando uma lista delimitada por vírgulas.

1. Verifique se você adicionou com êxito o compartilhamento do diretório home usando o `vserver cifs share show` comando.

Exemplo

O comando a seguir cria um compartilhamento de diretório base `%w` chamado `.`. As `oplocks` propriedades, `browsable`, e `changenotify` compartilhar são definidas além de definir a `homedirectory` propriedade compartilhar.



Este exemplo não exibe a saída de todos os compartilhamentos no SVM. A saída é truncada.

```
cluster1::> vsserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory
```

```
vs1::> vsserver cifs share show -vserver vs1
```

Vserver	Share	Path	Properties	Comment	ACL
vs1	%w	%w	oplocks	-	Everyone / Full
Control			browsable changenotify homedirectory		

Informações relacionadas

[Adicionando um caminho de pesquisa de diretório base](#)

[Requisitos e diretrizes para o uso de referências automáticas de nós](#)

[Gerenciando a acessibilidade aos diretórios home dos usuários](#)

Compartilhamentos de diretório inicial exigem nomes de usuário exclusivos

Tenha cuidado para atribuir nomes de usuário exclusivos ao criar compartilhamentos de diretório inicial usando as %w variáveis (nome de usuário do Windows) ou %u (nome de usuário UNIX) para gerar compartilhamentos dinamicamente. O nome da partilha é mapeado para o seu nome de utilizador.

Podem ocorrer dois problemas quando o nome de uma partilha estática e o nome de um utilizador são os mesmos:

- Quando o usuário lista os compartilhamentos em um cluster usando o `net view` comando, dois compartilhamentos com o mesmo nome de usuário são exibidos.
- Quando o usuário se conecta a esse nome de compartilhamento, o usuário está sempre conectado ao compartilhamento estático e não pode acessar o compartilhamento do diretório inicial com o mesmo nome.

Por exemplo, há um compartilhamento chamado "administrador" e você tem um nome de usuário do Windows. Se você criar um compartilhamento de diretório base e se conectar a esse compartilhamento, você será conectado ao compartilhamento estático "administrador", não ao compartilhamento de diretório principal "administrador".

Você pode resolver o problema com nomes de compartilhamento duplicados seguindo qualquer uma destas etapas:

- Renomear o compartilhamento estático para que ele não fique em conflito com o compartilhamento do diretório home do usuário.
- Dando ao usuário um novo nome de usuário para que ele não fique em conflito com o nome de compartilhamento estático.
- Criando um compartilhamento de diretório home CIFS com um nome estático, como "home", em vez de

usar o `%w` parâmetro para evitar conflitos com os nomes de compartilhamento.

O que acontece com nomes estáticos de compartilhamento de diretório base após a atualização

Os nomes de compartilhamento de diretório base devem conter a `%w` variável dinâmica ou `%u`. Você deve estar ciente do que acontece com nomes de compartilhamento de diretório home estático existentes após atualizar para uma versão do ONTAP com o novo requisito.

Se a configuração do diretório base contiver nomes de compartilhamento estáticos e você atualizar para o ONTAP, os nomes de compartilhamento do diretório base estático não serão alterados e ainda serão válidos. No entanto, você não pode criar novos compartilhamentos de diretório base que não contenham a `%w` variável ou `%u`.

Exigir que uma dessas variáveis seja incluída no nome de compartilhamento do diretório home do usuário garante que cada nome de compartilhamento seja exclusivo em toda a configuração do diretório home. Se desejar, você pode alterar os nomes estáticos de compartilhamento do diretório base para nomes que contêm a `%w` variável ou `%u`.

Adicione um caminho de pesquisa de diretório base

Se você quiser usar diretórios home do ONTAP SMB, você deve adicionar pelo menos um caminho de pesquisa de diretório base.

Sobre esta tarefa

Você pode adicionar um caminho de pesquisa de diretório base usando o `vserver cifs home-directory search-path add` comando.

O `vserver cifs home-directory search-path add` comando verifica o caminho especificado na `-path` opção durante a execução do comando. Se o caminho especificado não existir, o comando gera uma mensagem solicitando se deseja continuar. Você escolhe `y` ou `n`. Se você optar `y` por continuar, o ONTAP criará o caminho de pesquisa. No entanto, você deve criar a estrutura do diretório antes de usar o caminho de pesquisa na configuração do diretório base. Se você optar por não continuar, o comando falhará; o caminho de pesquisa não será criado. Em seguida, você pode criar a estrutura de diretório de caminho e executar novamente o `vserver cifs home-directory search-path add` comando.

Passos

1. Adicionar um caminho de pesquisa de diretório base: `vserver cifs home-directory search-path add -vserver vserver -path path`
2. Verifique se você adicionou com êxito o caminho de pesquisa usando o `vserver cifs home-directory search-path show` comando.

Exemplo

O exemplo a seguir adiciona o caminho `/home1` à configuração do diretório base no SVM VS1.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

vs1::> vserver cifs home-directory search-path show
Vserver      Position Path
-----
vs1          1      /home1
```

O exemplo a seguir tenta adicionar o caminho `/home2` à configuração do diretório base no SVM VS1. O caminho não existe. A escolha é feita para não continuar.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home2
Warning: The specified path "/home2" does not exist in the namespace
        belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

Informações relacionadas

[Adicionando um compartilhamento de diretório inicial](#)

Crie uma configuração de diretório base usando as variáveis `%W` e `%d`

Você pode criar uma configuração de diretório base usando as `%w` variáveis e `%d`. Os usuários podem então se conectar ao compartilhamento doméstico usando compartilhamentos criados dinamicamente.

Passos

1. Crie uma `qtree` para conter os diretórios iniciais do usuário: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Verifique se a `qtree` está usando o estilo de segurança correto: `volume qtree show`
3. Se a `qtree` não estiver usando o estilo de segurança desejado, altere o estilo de segurança usando o `volume qtree security` comando.
4. Adicionar uma partilha de diretório base: `vserver cifs share create -vserver vserver -share-name %w -path %d/%w -share-properties homedirectory\[,...\]`

`-vserver vserver` Especifica a máquina virtual de storage (SVM) habilitada para CIFS na qual adicionar o caminho de pesquisa.

`-share-name %w` especifica o nome de compartilhamento do diretório base. O ONTAP cria dinamicamente o nome do compartilhamento à medida que cada usuário se conecta ao seu diretório inicial. O nome da partilha será do formulário `Windows_user_name`.

`-path %d/%w` especifica o caminho relativo para o diretório home. O caminho relativo é criado dinamicamente à medida que cada usuário se conecta ao seu diretório inicial e será do formulário `domain/Windows_user_name`.

`-share-properties homedirectory[,...]` especifica as propriedades de compartilhamento para esse compartilhamento. Você deve especificar o `homedirectory` valor. Você pode especificar propriedades de compartilhamento adicionais usando uma lista delimitada por vírgulas.

5. Verifique se o compartilhamento tem a configuração desejada usando o `vserver cifs share show` comando.
6. Adicionar um caminho de pesquisa de diretório base: `vserver cifs home-directory search-path add -vserver vserver -path path`

`-vserver vserver-name` Especifica o SVM habilitado para CIFS no qual adicionar o caminho de pesquisa.

`-path path` especifica o caminho absoluto do diretório para o caminho de pesquisa.

7. Verifique se você adicionou com êxito o caminho de pesquisa usando o `vserver cifs home-directory search-path show` comando.
8. Para usuários com um diretório home, crie um diretório correspondente na `qtree` ou volume designado para conter diretórios home.

Por exemplo, se você criou uma `qtree` com o caminho `/vol/vol1/users` e o nome de usuário cujo diretório você deseja criar é `mydomain.user1`, você criará um diretório com o seguinte caminho: `/vol/vol1/users/mydomain/user1`.

Se você criou um volume chamado "home1" montado no `/home1`, você criará um diretório com o seguinte caminho: `/home1/mydomain/user1`.

9. Verifique se um usuário pode se conectar com êxito ao compartilhamento doméstico mapeando uma unidade ou conectando-se usando o caminho UNC.

Por exemplo, se o usuário `mydomain/user1` quiser se conectar ao diretório criado na Etapa 8 que está localizado na SVM `VS1`, o `user1` se conectaria usando o caminho UNC `\\vs1\user1`.

Exemplo

Os comandos no exemplo a seguir criam uma configuração de diretório base com as seguintes configurações:

- O nome da partilha é `%w`.
- O caminho do diretório home relativo é `%d/%w`.
- O caminho de pesquisa usado para conter os diretórios base `/home1`, é um volume configurado com estilo de segurança NTFS.
- A configuração é criada no SVM `VS1`.

Você pode usar esse tipo de configuração de diretório base quando os usuários acessam seus diretórios base a partir de hosts do Windows. Você também pode usar esse tipo de configuração quando os usuários acessam seus diretórios base a partir de hosts Windows e UNIX e o administrador do sistema de arquivos usa usuários e grupos baseados no Windows para controlar o acesso ao sistema de arquivos.

```

cluster::> vserver cifs share create -vserver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %w

                Vserver: vs1
                Share: %w
CIFS Server NetBIOS Name: VS1
                Path: %d/%w
    Share Properties: oplocks
                    browsable
                    changenotify
                    homedirectory
    Symlink Properties: enable
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
            Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
        Volume Name: -
        Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show
Vserver      Position Path
-----
vs1          1      /home1

```

Informações relacionadas

[Configurando diretórios base usando a variável %u](#)

[Configurações adicionais do diretório base](#)

[Exibindo informações sobre o caminho do diretório inicial de um usuário SMB](#)

Configure diretórios base usando a variável %u

Você pode criar uma configuração de diretório inicial onde você designar o nome de compartilhamento usando a %w variável, mas você usa a %u variável para designar o caminho relativo para o compartilhamento de diretório inicial. Em seguida, os usuários podem se conectar ao compartilhamento doméstico usando compartilhamentos criados dinamicamente usando o nome de usuário do Windows sem estar ciente do nome ou caminho real do diretório inicial.

Passos

1. Crie uma qtree para conter os diretórios iniciais do usuário: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Verifique se a qtree está usando o estilo de segurança correto: `volume qtree show`
3. Se a qtree não estiver usando o estilo de segurança desejado, altere o estilo de segurança usando o `volume qtree security` comando.
4. Adicionar uma partilha de diretório base: `vserver cifs share create -vserver vserver -share-name %w -path %u -share-properties homedirectory ,...]`

`-vserver vserver` Especifica a máquina virtual de storage (SVM) habilitada para CIFS na qual adicionar o caminho de pesquisa.

`-share-name %w` especifica o nome de compartilhamento do diretório base. O nome do compartilhamento é criado dinamicamente à medida que cada usuário se conecta ao seu diretório inicial e é do formulário `Windows_user_name`.



Você também pode usar a `%u` variável para a `-share-name` opção. Isso cria um caminho de compartilhamento relativo que usa o nome de usuário UNIX mapeado.

`-path %u` especifica o caminho relativo para o diretório home. O caminho relativo é criado dinamicamente à medida que cada usuário se conecta ao seu diretório inicial e é do formulário `mapeado_UNIX_user_name`.



O valor para esta opção também pode conter elementos estáticos. Por exemplo, `eng/%u`.

`-share-properties homedirectory\[,... \]` especifica as propriedades de compartilhamento para esse compartilhamento. Você deve especificar o `homedirectory` valor. Você pode especificar propriedades de compartilhamento adicionais usando uma lista delimitada por vírgulas.

5. Verifique se o compartilhamento tem a configuração desejada usando o `vserver cifs share show` comando.
6. Adicionar um caminho de pesquisa de diretório base: `vserver cifs home-directory search-path add -vserver vserver -path path`

`-vserver vserver` Especifica o SVM habilitado para CIFS no qual adicionar o caminho de pesquisa.

`-path path` especifica o caminho absoluto do diretório para o caminho de pesquisa.

7. Verifique se você adicionou com êxito o caminho de pesquisa usando o `vserver cifs home-directory search-path show` comando.
8. Se o usuário UNIX não existir, crie o usuário UNIX usando o `vserver services unix-user create` comando.



O nome de usuário UNIX para o qual você mapeia o nome de usuário do Windows deve existir antes de mapear o usuário.

9. Crie um mapeamento de nomes para o usuário do Windows para o usuário UNIX usando o seguinte comando: `vserver name-mapping create -vserver vserver_name -direction win-unix`

```
-priority integer -pattern windows_user_name -replacement unix_user_name
```



Se já existirem mapeamentos de nomes que mapeiem os usuários do Windows para usuários UNIX, você não precisará executar a etapa de mapeamento.

O nome de usuário do Windows é mapeado para o nome de usuário UNIX correspondente. Quando o usuário do Windows se conecta ao compartilhamento do diretório inicial, ele se conecta a um diretório inicial criado dinamicamente com um nome de compartilhamento que corresponde ao nome de usuário do Windows sem saber que o nome do diretório corresponde ao nome de usuário do UNIX.

10. Para usuários com um diretório home, crie um diretório correspondente na qtree ou volume designado para conter diretórios home.

Por exemplo, se você criou uma qtree com o caminho `/vol/vol1/users` e o nome de usuário UNIX mapeado do usuário cujo diretório você deseja criar é `""unixuser1""`, você criará um diretório com o seguinte caminho: `/vol/vol1/users/unixuser1`.

Se você criou um volume chamado `""home1""` montado no `/home1`, você criará um diretório com o seguinte caminho: `/home1/unixuser1`.

11. Verifique se um usuário pode se conectar com êxito ao compartilhamento doméstico mapeando uma unidade ou conectando-se usando o caminho UNC.

Por exemplo, se o usuário `mydomain/user1` mapeia para o usuário UNIX `unixuser1` e quiser se conectar ao diretório criado na Etapa 10 que está localizado na SVM VS1, o `user1` se conectaria usando o caminho UNC `\\vs1\user1`.

Exemplo

Os comandos no exemplo a seguir criam uma configuração de diretório base com as seguintes configurações:

- O nome da partilha é `%w`.
- O caminho relativo do diretório base é `%u`.
- O caminho de pesquisa usado para conter os diretórios base `/home1`, é um volume configurado com estilo de segurança UNIX.
- A configuração é criada no SVM VS1.

Você pode usar esse tipo de configuração de diretório base quando os usuários acessam seus diretórios base de hosts do Windows ou hosts do Windows e UNIX e o administrador do sistema de arquivos usa usuários e grupos baseados em UNIX para controlar o acesso ao sistema de arquivos.

```

cluster::> vsriver cifs share create -vsriver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vsriver cifs share show -vsriver vs1 -share-name %u

                Vserver: vs1
                Share: %w
CIFS Server NetBIOS Name: VS1
                Path: %u
    Share Properties: oplocks
                    browsable
                    changenotify
                    homedirectory
    Symlink Properties: enable
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
            Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vsriver cifs home-directory search-path add -vsriver vs1 -path
/home1

cluster::> vsriver cifs home-directory search-path show -vsriver vs1
Vserver      Position Path
-----
vs1          1        /home1

cluster::> vsriver name-mapping create -vsriver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1

cluster::> vsriver name-mapping show -pattern user1
Vserver      Direction Position
-----
vs1          win-unix  5        Pattern: user1
                    Replacement: unixuser1

```

Informações relacionadas

[Criando uma configuração de diretório base usando as variáveis %W e %d](#)

[Configurações adicionais do diretório base](#)

[Exibindo informações sobre o caminho do diretório inicial de um usuário SMB](#)

Configurações adicionais do diretório base

Você pode criar configurações adicionais do diretório base usando as %w variáveis , %d, e %u , que permitem personalizar a configuração do diretório base para atender às suas necessidades.

Você pode criar uma série de configurações de diretório inicial usando uma combinação de variáveis e strings estáticas nos nomes de compartilhamento e caminhos de pesquisa. A tabela a seguir fornece alguns exemplos ilustrando como criar diferentes configurações de diretório base:

Caminhos criados quando /vol1/user contém diretórios base...	Compartilhar comando...
Para criar um caminho de compartilhamento \\vs1\~win_username que direcione o usuário /vol1/user/win_username	<pre>vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changefnotify,homedirectory</pre>
Para criar um caminho de compartilhamento \\vs1\win_username que direcione o usuário /vol1/user/domain/win_username	<pre>vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changefnotify,homedirectory</pre>
Para criar um caminho de compartilhamento \\vs1\win_username que direcione o usuário /vol1/user/unix_username	<pre>vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changefnotify,homedirectory</pre>
Para criar um caminho de compartilhamento \\vs1\unix_username que direcione o usuário /vol1/user/unix_username	<pre>vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changefnotify,homedirectory</pre>

Comandos para gerenciar caminhos de pesquisa

Existem comandos ONTAP específicos para gerenciar caminhos de pesquisa para configurações de diretório base SMB. Por exemplo, existem comandos para adicionar, remover e exibir informações sobre caminhos de pesquisa. Há também um comando para alterar a ordem do caminho de pesquisa.

Se você quiser...	Use este comando...
Adicionar um caminho de pesquisa	<pre>vserver cifs home-directory search-path add</pre>
Exibir caminhos de pesquisa	<pre>vserver cifs home-directory search-path show</pre>

Se você quiser...	Use este comando...
Altere a ordem do caminho de pesquisa	<code>vserver cifs home-directory search-path reorder</code>
Remova um caminho de pesquisa	<code>vserver cifs home-directory search-path remove</code>

Consulte a página de manual de cada comando para obter mais informações.

Exiba informações sobre o caminho do diretório inicial de um usuário SMB

Você pode exibir o caminho do diretório inicial de um usuário SMB na máquina virtual de armazenamento (SVM), que pode ser usado se você tiver vários caminhos de diretório inicial CIFS configurados e quiser ver qual caminho contém o diretório inicial do usuário.

Passo

1. Exiba o caminho do diretório base usando o `vserver cifs home-directory show-user` comando.

```
vserver cifs home-directory show-user -vserver vs1 -username user1
```

Vserver	User	Home Dir Path
vs1	user1	/home/user1

Informações relacionadas

[Gerenciando a acessibilidade aos diretórios home dos usuários](#)

Gerencie a acessibilidade aos diretórios home dos usuários

Por padrão, o diretório home de um usuário só pode ser acessado por esse usuário. Para compartilhamentos em que o nome dinâmico do compartilhamento é precedido por um til ("til"), você pode habilitar ou desabilitar o acesso aos diretórios iniciais dos usuários por administradores do Windows ou por qualquer outro usuário (acesso público).

Antes de começar

Os compartilhamentos de diretório inicial na máquina virtual de armazenamento (SVM) devem ser configurados com nomes de compartilhamento dinâmicos que são precedidos por um til ("tilde"). Os seguintes casos ilustram os requisitos de nomeação de compartilhamento:

Nome de compartilhamento do diretório base	Exemplo de comando para se conectar ao compartilhamento
clique no botão "ok"	<code>net use * \\IPAddress\~domain~user/u:credentials</code>

Nome de compartilhamento do diretório base	Exemplo de comando para se conectar ao compartilhamento
clique no botão "ok"	<code>net use * \\IPAddress\~user/u:credentials</code>
clique no botão "ok"	<code>net use * \\IPAddress\abc~user/u:credentials</code>

Passo

1. Execute a ação apropriada:

Se você quiser ativar ou desativar o acesso aos diretórios home dos usuários para...	Digite o seguinte...
Administradores do Windows	<code>vserver cifs home-directory modify -vserver vserver_name -is-home-dirs -access-for-admin-enabled {true false}</code> A predefinição é <code>true</code> .
Qualquer utilizador (acesso público)	<ol style="list-style-type: none"> a. Defina o nível de privilégio como avançado <code>set -privilege advanced</code> b. Ativar ou desativar o acesso: <code>`vserver cifs home-directory modify -vserver vserver_name -is-home-dirs-access-for-public-enabled {true</code>

O exemplo a seguir permite o acesso público aos diretórios home dos usuários `set -privilege advanced vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public-enabled true set -privilege admin`

Informações relacionadas

[Exibindo informações sobre o caminho do diretório inicial de um usuário SMB](#)

Configurar o acesso de cliente SMB a links simbólicos UNIX

Como o ONTAP permite que você forneça acesso de cliente SMB a links simbólicos UNIX

Um link simbólico é um arquivo criado em um ambiente UNIX que contém uma referência a outro arquivo ou diretório. Se um cliente acessar um link simbólico, o cliente será redirecionado para o arquivo de destino ou diretório ao qual o link simbólico se refere. O ONTAP suporta links simbólicos relativos e absolutos, incluindo widelinks (links absolutos com alvos fora do sistema de arquivos local).

O ONTAP fornece aos clientes SMB a capacidade de seguir links simbólicos UNIX configurados no SVM. Este recurso é opcional, e você pode configurá-lo por compartilhamento, usando a `-symlink-properties` opção `vserver cifs share create` do comando, com uma das seguintes configurações:

- Habilitado com acesso de leitura/gravação
- Habilitado com acesso somente leitura
- Desabilitado ocultando links simbólicos de clientes SMB
- Desativado sem acesso a links simbólicos de clientes SMB

Se você habilitar links simbólicos em um compartilhamento, links simbólicos relativos funcionam sem configuração adicional.

Se você habilitar links simbólicos em um compartilhamento, links simbólicos absolutos não funcionam imediatamente. Você deve primeiro criar um mapeamento entre o caminho UNIX do link simbólico para o caminho SMB de destino. Ao criar mapeamentos de links simbólicos absolutos, você pode especificar se é um link local ou um *widelink*; *widelinks* podem ser links para sistemas de arquivos em outros dispositivos de armazenamento ou links para sistemas de arquivos hospedados em SVMs separadas no mesmo sistema ONTAP. Quando você cria um *widelink*, ele deve incluir as informações para o cliente seguir; ou seja, você cria um ponto de reparação para o cliente descobrir o ponto de junção do diretório. Se você criar um link simbólico absoluto para um arquivo ou diretório fora do compartilhamento local, mas definir a localidade como local, o ONTAP não permite o acesso ao destino.



Se um cliente tentar excluir um link simbólico local (absoluto ou relativo), apenas o link simbólico é excluído, não o arquivo ou diretório de destino. No entanto, se um cliente tentar excluir um *widelink*, ele pode excluir o arquivo ou diretório de destino real ao qual o *widelink* se refere. O ONTAP não tem controle sobre isso porque o cliente pode abrir explicitamente o arquivo ou diretório de destino fora do SVM e excluí-lo.

• Reparse Points e serviços de sistema de arquivos ONTAP

Um *ponto de reparação* é um objeto de sistema de arquivos NTFS que pode ser opcionalmente armazenado em volumes junto com um arquivo. Os pontos Reparse fornecem aos clientes SMB a capacidade de receber serviços de sistema de arquivos aprimorados ou estendidos ao trabalhar com volumes de estilo NTFS. Os pontos Reparse consistem em tags padrão que identificam o tipo de ponto de reparação e o conteúdo do ponto de reparação que pode ser recuperado por clientes SMB para processamento posterior pelo cliente. Dos tipos de objeto disponíveis para a funcionalidade estendida do sistema de arquivos, o ONTAP implementa suporte para links simbólicos NTFS e pontos de junção de diretório usando tags de ponto de reparação. Os clientes SMB que não conseguem entender o conteúdo de um ponto de reparação simplesmente ignoram e não fornecem o serviço de sistema de arquivos estendido que o ponto de reparação pode habilitar.

- * Diretório de pontos de junção e suporte ONTAP para links simbólicos*

Os pontos de junção de diretório são locais dentro de uma estrutura de diretórios do sistema de arquivos que podem se referir a locais alternativos onde os arquivos são armazenados, seja em um caminho diferente (links simbólicos) ou em um dispositivo de armazenamento separado (*widelinks*). Os servidores SMB do ONTAP expõem pontos de junção de diretório para clientes Windows como pontos de reparação, permitindo que clientes capazes obtenham conteúdos de pontos de reparação do ONTAP quando um ponto de junção de diretório é atravessado. Eles podem, assim, navegar e se conectar a diferentes caminhos ou dispositivos de armazenamento como se fossem parte do mesmo sistema de arquivos.

- * Habilitando o suporte de *widelink* usando opções de ponto de reparação*

A `-is-use-junctions-as-reparse-points-enabled` opção está ativada por predefinição no ONTAP 9. Nem todos os clientes SMB suportam *widelinks*, portanto, a opção de ativar as informações é configurável com base na versão por protocolo, permitindo que os administradores acomodem clientes SMB com suporte e não suporte. No ONTAP 9.2 e versões posteriores, você deve habilitar a opção

-widelink-as-reparse-point-versions para cada protocolo cliente que acessa o compartilhamento usando widelinks; o padrão é SMB1. Em versões anteriores, apenas os widelinks acessados usando o SMB1 padrão foram relatados e os sistemas que usam SMB2 ou SMB3 não conseguiram acessar os widelinks.

Informações relacionadas

- ["Aplicativos de backup do Windows e links simbólicos em estilo Unix"](#)
- ["Documentação da Microsoft: Pontos de reanálise"](#)

Limites ao configurar links simbólicos UNIX para acesso SMB

Você precisa estar ciente de certos limites ao configurar links simbólicos UNIX para acesso SMB.

Limite	Descrição
45	<p>Comprimento máximo do nome do servidor CIFS que você pode especificar ao usar um FQDN para o nome do servidor CIFS.</p> <p> Você pode, alternativamente, especificar o nome do servidor CIFS como um nome NetBIOS, que é limitado a 15 caracteres.</p>
80	Comprimento máximo do nome da partilha.
256	Comprimento máximo do caminho UNIX que você pode especificar ao criar um link simbólico ou ao modificar o caminho UNIX de um link simbólico existente. O caminho UNIX deve começar com um "/" (slash) and end with a "/". As barras de início e fim contam como parte do limite de 256 caracteres.
256	Comprimento máximo do caminho CIFS que você pode especificar ao criar um link simbólico ou ao modificar o caminho CIFS de um link simbólico existente. O caminho CIFS deve começar com um "/" (slash) and end with a "/". As barras de início e fim contam como parte do limite de 256 caracteres.

Informações relacionadas

[Criando mapeamentos de links simbólicos para compartilhamentos SMB](#)

Controle anúncios DFS automáticos no ONTAP com uma opção de servidor CIFS

Uma opção de servidor CIFS controla como os recursos do DFS são anunciados para

clientes SMB ao se conectar a compartilhamentos. Como o ONTAP usa referências DFS quando os clientes acessam links simbólicos sobre o SMB, você deve estar ciente do impactos ao desativar ou ativar essa opção.

Uma opção de servidor CIFS determina se os servidores CIFS anunciam automaticamente que são capazes de DFS para clientes SMB. Por padrão, essa opção está ativada e o servidor CIFS sempre anuncia que é capaz de DFS para clientes SMB (mesmo quando se conecta a compartilhamentos onde o acesso a links simbólicos está desativado). Se você quiser que o servidor CIFS anuncie que ele é capaz de clientes somente quando eles estão se conectando a compartilhamentos onde o acesso a links simbólicos está ativado, você pode desativar essa opção.

Você deve estar ciente do que acontece quando essa opção está desativada:

- As configurações de compartilhamento para links simbólicos não são alteradas.
- Se o parâmetro share estiver definido para permitir acesso a links simbólicos (acesso de leitura e gravação ou acesso somente leitura), o servidor CIFS anuncia recursos DFS aos clientes que se conectam a esse compartilhamento.

As conexões do cliente e o acesso a links simbólicos continuam sem interrupção.

- Se o parâmetro share estiver definido para não permitir acesso a links simbólicos (desabilitando o acesso ou se o valor do parâmetro share for nulo), o servidor CIFS não anunciará recursos DFS aos clientes que se conectam a esse compartilhamento.

Como os clientes têm informações em cache que o servidor CIFS é capaz de DFS e não está mais anunciando que são, os clientes que estão conectados a compartilhamentos onde o acesso a links simbólicos está desativado podem não ser capazes de acessar esses compartilhamentos depois que a opção do servidor CIFS é desativada. Depois que a opção estiver desativada, talvez seja necessário reinicializar os clientes que estão conectados a esses compartilhamentos, limpando assim as informações em cache.

Essas alterações não se aplicam às conexões SMB 1,0.

Configurar o suporte a links simbólicos UNIX em compartilhamentos SMB

Você pode configurar o suporte a links simbólicos UNIX em compartilhamentos SMB especificando uma configuração de propriedade de compartilhamento de link simbólico ao criar compartilhamentos SMB ou a qualquer momento modificando compartilhamentos SMB existentes. O suporte a links simbólicos UNIX está habilitado por padrão. Você também pode desativar o suporte a links simbólicos UNIX em um compartilhamento.

Sobre esta tarefa

Ao configurar o suporte a links simbólicos UNIX para compartilhamentos SMB, você pode escolher uma das seguintes configurações:

Definição	Descrição
<code>enable</code> (OBSOLETO*)	Especifica que links simbólicos estão habilitados para acesso de leitura e gravação.

Definição	Descrição
<code>read_only</code> (OBSOLETO*)	Especifica que os links simbólicos estão ativados para acesso somente leitura. Esta definição não se aplica a widelinks. O acesso à Widelink é sempre leitura-escrita.
<code>hide</code> (OBSOLETO*)	Especifica que os clientes SMB são impedidos de ver links simbólicos.
<code>no-strict-security</code>	Especifica que os clientes seguem links simbólicos fora dos limites de compartilhamento.
<code>symlinks</code>	Especifica que os links simbólicos são ativados localmente para acesso de leitura e gravação. Os anúncios DFS não são gerados mesmo que a opção CIFS <code>is-advertise-dfs-enabled</code> esteja definida como <code>true</code> . Esta é a configuração padrão.
<code>symlinks-and-widelinks</code>	Especifica que os links simbólicos locais e os widelinks para acesso de leitura e gravação. Os anúncios DFS são gerados para links simbólicos locais e widelinks, mesmo que a opção CIFS <code>is-advertise-dfs-enabled</code> esteja definida como <code>false</code> .
<code>disable</code>	Especifica que links simbólicos e widelinks estão desativados. Os anúncios DFS não são gerados mesmo que a opção CIFS <code>is-advertise-dfs-enabled</code> esteja definida como <code>true</code> .
<code>""</code> (nulo, não definido)	Desativa links simbólicos no compartilhamento.
<code>-</code> (não definido)	Desativa links simbólicos no compartilhamento.



*Os parâmetros *enable*, *hide* e *read-only* são obsoletos e podem ser removidos em uma versão futura do ONTAP.

Passos

1. Configure ou desative o suporte a links simbólicos:

Se for...	Digite...
Um novo compartilhamento SMB	<code>`+vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink -properties {enable</code>
<code>hide</code>	<code>read-only</code>

Se for...	Digite...
""	-
symlinks	symlinks-and-widelinks
disable},...]+`	Um compartilhamento SMB existente
`+vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable	hide
read-only	""
-	symlinks
symlinks-and-widelinks	disable},...]+`

2. Verifique se a configuração do compartilhamento SMB está correta: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Exemplo

O comando a seguir cria um compartilhamento SMB chamado "d.ATA1" com a configuração de link simbólico UNIX definida como `enable`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                Vserver: vs1
                Share: data1
CIFS Server NetBIOS Name: VS1
                Path: /data1
                Share Properties: oplocks
                                browsable
                                changenotify
                Symlink Properties: enable
                File Mode Creation Mask: -
                Directory Mode Creation Mask: -
                Share Comment: -
                Share ACL: Everyone / Full Control
                File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: manual
                Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
                UNIX Group for File Create: -
```

Informações relacionadas

[Criando mapeamentos de links simbólicos para compartilhamentos SMB](#)

Crie mapeamentos de links simbólicos para compartilhamentos SMB

Você pode criar mapeamentos de links simbólicos UNIX para compartilhamentos SMB. Você pode criar um link simbólico relativo, que se refere ao arquivo ou pasta relativa à sua pasta pai, ou você pode criar um link simbólico absoluto, que se refere ao arquivo ou pasta usando um caminho absoluto.

Sobre esta tarefa

Os Winelinks não são acessíveis a partir de clientes Mac os X se você usar SMB 2.x. Quando um usuário tenta se conectar a um compartilhamento usando widelinks de um cliente Mac os X, a tentativa falha. No entanto, você pode usar widelinks com clientes Mac os X se você usar SMB 1.

Passos

1. Para criar mapeamentos de links simbólicos para compartilhamentos SMB: `vserver cifs symlink create -vserver virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-directory {true|false}]`
 - `-vserver virtual_server_name` Especifica o nome da máquina virtual de storage (SVM).
 - `-unix-path path` Especifica o caminho UNIX. O caminho UNIX deve começar com uma barra (/) e deve terminar com uma barra (/).
 - `-share-name share_name` Especifica o nome do compartilhamento SMB para mapear.
 - `-cifs-path path` Especifica o caminho CIFS. O caminho CIFS deve começar com uma barra (/) e deve terminar com uma barra (/).
 - `-cifs-server server_name` Especifica o nome do servidor CIFS. O nome do servidor CIFS pode ser especificado como um nome DNS (por exemplo, mynetwork.cifs.server.com), endereço IP ou nome NetBIOS. O nome NetBIOS pode ser determinado usando o `vserver cifs show` comando. Se este parâmetro opcional não for especificado, o valor padrão será o nome NetBIOS do servidor CIFS local.
 - `-locality local|free|widelink` especifica se deseja criar um link local, um link gratuito ou um link simbólico amplo. Um link simbólico local mapeia para o compartilhamento SMB local. Um link simbólico gratuito pode mapear qualquer lugar no servidor SMB local. Um link simbólico amplo mapeia para qualquer compartilhamento SMB na rede. Se não especificar este parâmetro opcional, o valor predefinido é `local`.
 - `-home-directory true|false` especifica se o compartilhamento de destino é um diretório home. Mesmo que esse parâmetro seja opcional, você deve definir esse parâmetro para `true` quando o compartilhamento de destino for configurado como um diretório inicial. A predefinição é `false`.

Exemplo

O comando a seguir cria um mapeamento de link simbólico no SVM chamado VS1. Ele tem o caminho UNIX `/src/`, o nome de compartilhamento SMB `"SOURCE"`, o caminho CIFS `/mycompany/source/` e o

endereço IP do servidor CIFS 123.123.123.123, e é um widelink.

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/  
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server  
123.123.123.123 -locality widelink
```

Informações relacionadas

[Configurando o suporte a links simbólicos UNIX em compartilhamentos SMB](#)

Comandos para gerenciar mapeamentos de links simbólicos

Existem comandos ONTAP específicos para gerenciar mapeamentos de links simbólicos.

Se você quiser...	Use este comando...
Crie um mapeamento de link simbólico	<code>vserver cifs symlink create</code>
Exibir informações sobre mapeamentos de links simbólicos	<code>vserver cifs symlink show</code>
Modifique um mapeamento de link simbólico	<code>vserver cifs symlink modify</code>
Excluir um mapeamento de link simbólico	<code>vserver cifs symlink delete</code>

Consulte a página de manual de cada comando para obter mais informações.

Aplicativos de backup do Windows e links simbólicos em estilo Unix

Quando um aplicativo de backup executado no Windows encontra um link simbólico (link simbólico) estilo Unix, o link é seguido e os dados são copiados. Começando com ONTAP 9.15,1, você tem a opção de fazer backup dos links simbólicos em vez dos dados. Esse recurso é totalmente compatível com FlexGroups e FlexVols da ONTAP.

Visão geral

Antes de alterar a forma como o ONTAP lida com links simbólicos durante uma operação de backup do Windows, você deve estar familiarizado com os benefícios, os principais conceitos e as opções de configuração.

Benefícios

Quando esse recurso está desativado ou indisponível, cada link simbólico é percorrido e os dados aos quais ele se vincula são copiados. Por causa disso, dados desnecessários podem às vezes ser copiados e, em certas situações, o aplicativo pode acabar em um loop. Ao invés disso, fazer backup dos links simbólicos evita esses problemas. E como os arquivos de link simbólico são muito pequenos em comparação com os dados na maioria dos casos, os backups levam menos tempo para serem concluídos. O desempenho geral do cluster também pode melhorar devido à redução das operações de e/S.

Ambiente de servidor Windows

Este recurso é compatível com aplicativos de backup executados no Windows. Você deve entender os aspectos técnicos relevantes do ambiente antes de usá-lo.

Atributos estendidos

O Windows suporta atributos estendidos (EA) que formam coletivamente metadados adicionais associados opcionalmente aos arquivos. Esses atributos são usados por vários aplicativos, como o subsistema do Windows para Linux, conforme descrito em "[Permissões de arquivo para WSL](#)". Os aplicativos podem solicitar atributos estendidos para cada arquivo ao ler dados do ONTAP.

Os links simbólicos são retornados nos atributos estendidos quando o recurso é ativado. Portanto, um aplicativo de backup deve fornecer suporte padrão EA, que é usado para armazenar os metadados. Alguns utilitários do Windows suportam e preservam os atributos estendidos. No entanto, se o software de backup não suportar backup e restauração dos atributos estendidos, ele não preservará os metadados associados a cada arquivo e não processará os links simbólicos corretamente.

Configuração do Windows

Os aplicativos de backup executados em um servidor Microsoft Windows podem receber um privilégio especial, permitindo que eles ignorem a segurança normal de arquivos. Isso geralmente é feito adicionando os aplicativos ao grupo operadores de backup. Os aplicativos podem então fazer backup e restaurar arquivos conforme necessário, bem como executar outras operações relacionadas ao sistema. Há alterações sutis no protocolo SMB usado pelos aplicativos de backup que podem ser detetadas pelo ONTAP à medida que os dados são lidos e gravados.

Requisitos

O recurso de backup de link simbólico tem vários requisitos, incluindo:

- O cluster está executando o ONTAP 9.15,1 ou posterior.
- Um aplicativo de backup do Windows que recebeu Privileges de backup especial.
- O aplicativo de backup também deve dar suporte a atributos estendidos e solicitá-los durante as operações de backup.
- O recurso de backup de link simbólico do ONTAP está habilitado para o SVM de dados aplicável.

Opções de configuração

Além da CLI do ONTAP, você também pode gerenciar esse recurso usando a API REST. Consulte "[Novidades com a API REST e a automação do ONTAP](#)" para obter mais informações. A configuração que determina como o ONTAP processa os links simbólicos em estilo Unix deve ser executada separadamente para cada SVM.

Ative o recurso de backup de link simbólico no ONTAP

Uma opção de configuração foi introduzida a um comando CLI existente com ONTAP 9.15,1. Você pode usar essa opção para ativar ou desativar o processamento de link simbólico estilo Unix.

Antes de começar

Reveja o básico [Requisitos](#). Além disso:

- Ser capaz de elevar seu privilégio CLI para o nível avançado.
- Determine os dados SVM que você deseja modificar. O SVM `vs1` é usado no comando exemplo.

Passos

1. Defina o nível de privilégio avançado.

```
set privilege advanced
```

2. Habilite o backup de arquivos de link simbólico.

```
vserver cifs options modify -vserver vs1 -is-backup-symlink-enabled true
```

Use BranchCache para armazenar em cache conteúdo de compartilhamento SMB em uma filial

Use o BranchCache para armazenar em cache conteúdo de compartilhamento SMB em uma visão geral de filiais

BranchCache foi desenvolvido pela Microsoft para permitir o armazenamento em cache de conteúdo em computadores locais para clientes solicitantes. A implementação do ONTAP do BranchCache pode reduzir a utilização da rede de área ampla (WAN) e fornecer um melhor tempo de resposta de acesso quando os usuários de uma filial acessam conteúdo armazenado em máquinas virtuais de armazenamento (SVMs) usando SMB.

Se você configurar o BranchCache, os clientes do Windows BranchCache primeiro recuperam o conteúdo do SVM e, em seguida, armazenam o conteúdo em um computador dentro da filial. Se outro cliente habilitado para BranchCache na filial solicitar o mesmo conteúdo, o SVM autentica e autoriza o usuário solicitante. Em seguida, o SVM determina se o conteúdo em cache ainda está atualizado e, se estiver, envia os metadados do cliente sobre o conteúdo em cache. O cliente então usa os metadados para recuperar conteúdo diretamente do cache baseado localmente.

Informações relacionadas

[Usando arquivos off-line para permitir o armazenamento em cache de arquivos para uso off-line](#)

Requisitos e diretrizes

Suporte à versão BranchCache

Você deve estar ciente de quais versões do BranchCache o ONTAP suporta.

O ONTAP oferece suporte ao BranchCache 1 e ao BranchCache 2 aprimorado:

- Ao configurar o BranchCache no servidor SMB para a máquina virtual de armazenamento (SVM), você pode habilitar o BranchCache 1, o BranchCache 2 ou todas as versões.

Por padrão, todas as versões estão ativadas.

- Se você ativar apenas o BranchCache 2, as máquinas cliente Windows do escritório remoto devem suportar o BranchCache 2.

Somente clientes SMB 3,0 ou posteriores suportam BranchCache 2.

Para obter mais informações sobre as versões do BranchCache, consulte a Biblioteca Microsoft TechNet.

Informações relacionadas

["Microsoft TechNet Library: technet.microsoft.com/en-us/library/"](https://technet.microsoft.com/en-us/library/)

Requisitos de suporte ao protocolo de rede

Você deve estar ciente dos requisitos de protocolo de rede para implementar o ONTAP BranchCache.

Você pode implementar o recurso ONTAP BranchCache em redes IPv4 e IPv6 usando SMB 2,1 ou posterior.

Todos os servidores CIFS e máquinas de filiais que participam da implementação do BranchCache devem ter o protocolo SMB 2,1 ou posterior ativado. O SMB 2,1 tem extensões de protocolo que permitem que um cliente participe de um ambiente BranchCache. Esta é a versão mínima do protocolo SMB que oferece suporte ao BranchCache. O SMB 2,1 suporta a versão BranchCache 1.

Se você quiser usar o BranchCache versão 2, o SMB 3,0 é a versão mínima suportada. Todos os servidores CIFS e máquinas de filiais que participam de uma implementação BranchCache 2 devem ter o SMB 3,0 ou posterior habilitado.

Se você tiver escritórios remotos onde alguns dos clientes suportam apenas o SMB 2,1 e alguns dos clientes suportam o SMB 3,0, você pode implementar uma configuração BranchCache no servidor CIFS que fornece suporte de cache tanto no BranchCache 1 quanto no BranchCache 2.



Embora o recurso Microsoft BranchCache suporte ao uso dos protocolos HTTP/HTTPS e SMB como protocolos de acesso a arquivos, o ONTAP BranchCache só suporta o uso de SMB.

O ONTAP e o Windows hosts requisitos de versão

Os hosts do ONTAP e da filial do Windows devem atender a certos requisitos de versão antes de poder configurar o BranchCache.

Antes de configurar o BranchCache, você deve garantir que a versão do ONTAP no cluster e clientes de filiais participantes ofereçam suporte ao SMB 2,1 ou posterior e ofereça suporte ao recurso BranchCache. Se você configurar o modo Cache hospedado, você também deve garantir que você use um host suportado para o servidor de cache.

O BranchCache 1 é compatível com as seguintes versões do ONTAP e hosts do Windows:

- Servidor de conteúdo: Máquina virtual de storage (SVM) com ONTAP
- Servidor de cache: Windows Server 2008 R2 ou Windows Server 2012 ou posterior
- Peer ou cliente: Windows 7 Enterprise, Windows 7 Ultimate, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 ou posterior

O BranchCache 2 é compatível com as seguintes versões do ONTAP e hosts do Windows:

- Servidor de conteúdo: SVM com ONTAP
- Servidor de cache: Windows Server 2012 ou posterior

- Peer ou cliente: Windows 8 ou Windows Server 2012 ou posterior

Razões pelas quais o ONTAP invalida hashes do BranchCache

Entender as razões pelas quais o ONTAP invalida hashes pode ser útil ao Planejar sua configuração do BranchCache. Ele pode ajudá-lo a decidir qual modo de operação você deve configurar e pode ajudá-lo a escolher em quais compartilhamentos ativar o BranchCache.

O ONTAP deve gerenciar hashes do BranchCache para garantir que os hashes sejam válidos. Se um hash não for válido, o ONTAP invalida o hash e computa um novo hash na próxima vez que o conteúdo for solicitado, supondo que o BranchCache ainda esteja habilitado.

O ONTAP invalida hashes pelos seguintes motivos:

- A chave do servidor é modificada.

Se a chave do servidor for modificada, o ONTAP invalida todos os hashes no armazenamento de hash.

- Um hash é removido do cache porque o tamanho máximo do armazenamento de hash BranchCache foi atingido.

Este é um parâmetro sintonizável e pode ser modificado para atender aos requisitos da sua empresa.

- Um arquivo é modificado por meio do acesso SMB ou NFS.
- Um arquivo para o qual há hashes computados é restaurado usando o `snap restore` comando.
- Um volume que contém compartilhamentos SMB habilitados para BranchCache é restaurado usando o `snap restore` comando.

Diretrizes para escolher o local de armazenamento de hash

Ao configurar o BranchCache, você escolhe onde armazenar hashes e qual tamanho o armazenamento de hash deve ser. Entender as diretrizes ao escolher o local e o tamanho do armazenamento de hash pode ajudá-lo a Planejar sua configuração do BranchCache em um SVM habilitado para CIFS.

- Você deve localizar o armazenamento de hash em um volume onde atualizações de tempo são permitidas.

O tempo de acesso em um arquivo hash é usado para manter os arquivos acessados com frequência no armazenamento de hash. Se as atualizações do atime estiverem desativadas, a hora de criação será usada para esse fim. É preferível usar o tempo para rastrear arquivos usados com frequência.

- Não é possível armazenar hashes em sistemas de arquivos somente leitura, como destinos SnapMirror e volumes SnapLock.
- Se o tamanho máximo do armazenamento de hash for atingido, os hashes mais antigos serão lavados para abrir espaço para novos hashes.

Você pode aumentar o tamanho máximo do armazenamento de hash para reduzir a quantidade de hashes que são lavados do cache.

- Se o volume no qual você armazena hashes estiver indisponível ou cheio, ou se houver um problema com a comunicação intra-cluster em que o serviço BranchCache não pode recuperar informações de hash, os serviços BranchCache não estarão disponíveis.

O volume pode estar indisponível porque está offline ou porque o administrador de armazenamento especificou um novo local para o armazenamento de hash.

Isso não causa problemas com acesso a arquivos. Se o acesso ao armazenamento de hash for impedido, o ONTAP retornará um erro definido pela Microsoft ao cliente, o que faz com que o cliente solicite o arquivo usando a solicitação de leitura normal de SMB.

Informações relacionadas

[Configure o BranchCache no servidor SMB](#)

[Modifique a configuração do BranchCache](#)

Recomendações do BranchCache

Antes de configurar o BranchCache, há certas recomendações que você deve ter em mente ao decidir quais compartilhamentos SMB você deseja ativar o armazenamento em cache do BranchCache.

Você deve ter em mente as seguintes recomendações ao decidir em qual modo de operação usar e em quais compartilhamentos SMB para ativar o BranchCache:

- Os benefícios do BranchCache são reduzidos quando os dados a serem armazenados remotamente em cache são alterados com frequência.
- Os serviços BranchCache são benéficos para compartilhamentos que contêm conteúdo de arquivo que é reutilizado por vários clientes de escritório remoto ou por conteúdo de arquivo que é repetidamente acessado por um único usuário remoto.
- Considere ativar o armazenamento em cache para conteúdo somente leitura, como dados em cópias Snapshot e destinos SnapMirror.

Configurar BranchCache

Configurar visão geral do BranchCache

Você configura o BranchCache no servidor SMB usando comandos ONTAP. Para implementar o BranchCache, você também deve configurar seus clientes e, opcionalmente, seus servidores de cache hospedados nas filiais onde você deseja armazenar conteúdo em cache.

Se você configurar o BranchCache para habilitar o armazenamento em cache de forma compartilhada, você deverá habilitar o BranchCache nos compartilhamentos SMB para os quais deseja fornecer serviços de armazenamento em cache do BranchCache.

Requisitos para configurar o BranchCache

Depois de atender a alguns pré-requisitos, você pode configurar o BranchCache.

Antes de configurar o BranchCache no servidor CIFS para sua SVM, você precisa atender aos requisitos a

seguir:

- O ONTAP deve ser instalado em todos os nós do cluster.
- O CIFS deve ser licenciado e um servidor SMB deve ser configurado. A licença SMB está incluída no "ONTAP One". Se não tiver o ONTAP One e a licença não estiver instalada, contacte o seu representante de vendas.
- A conectividade de rede IPv4G ou IPv6G deve ser configurada.
- Para BranchCache 1, o SMB 2,1 ou posterior deve estar ativado.
- Para BranchCache 2, o SMB 3,0 deve estar ativado e os clientes remotos do Windows devem suportar o BranchCache 2.

Configure o BranchCache no servidor SMB

Você pode configurar o BranchCache para fornecer serviços do BranchCache por compartilhamento. Como alternativa, você pode configurar o BranchCache para ativar automaticamente o cache em todos os compartilhamentos SMB.

Sobre esta tarefa

Você pode configurar o BranchCache em SVMs.

- Você pode criar uma configuração BranchCache de todos os compartilhamentos se quiser oferecer serviços de cache para todo o conteúdo contido em todos os compartilhamentos SMB no servidor CIFS.
- Você pode criar uma configuração de BranchCache por compartilhamento se quiser oferecer serviços de cache para conteúdo contido em compartilhamentos SMB selecionados no servidor CIFS.

Você deve especificar os seguintes parâmetros ao configurar o BranchCache:

Parâmetros necessários	Descrição
<i>Nome da SVM</i>	O BranchCache é configurado por SVM. Você deve especificar em qual SVM habilitado para CIFS deseja configurar o serviço BranchCache.

Parâmetros necessários	Descrição
<i>Path to hash store</i>	<p>Os hashes do BranchCache são armazenados em arquivos regulares no volume SVM. Você deve especificar o caminho para um diretório existente onde você deseja que o ONTAP armazene os dados de hash. o caminho de hash do BranchCache deve ser lido-gravável. Caminhos somente leitura, como diretórios Snapshot, não são permitidos. Você pode armazenar dados de hash em um volume que contém outros dados ou pode criar um volume separado para armazenar dados de hash.</p> <p>Se o SVM for uma fonte de recuperação de desastres SVM, o caminho hash não poderá estar no volume raiz. Isso ocorre porque o volume raiz não é replicado para o destino de recuperação de desastres.</p> <p>O caminho hash pode conter espaços em branco e quaisquer caracteres de nome de arquivo válidos.</p>

Opcionalmente, você pode especificar os seguintes parâmetros:

Parâmetros opcionais	Descrição
<i>Versões suportadas</i>	<p>ONTAP suporta BranchCache 1 e 2. Pode ativar a versão 1, a versão 2 ou ambas as versões. O padrão é ativar ambas as versões.</p>
<i>Tamanho máximo do armazenamento de hash</i>	<p>Você pode especificar o tamanho a ser usado para o armazenamento de dados de hash. Se os dados de hash excederem esse valor, o ONTAP excluirá hashes mais antigos para abrir espaço para hashes mais recentes. O tamanho padrão para o armazenamento de hash é de 1 GB. O BranchCache funciona de forma mais eficiente se os hashes não forem descartados de forma excessivamente agressiva. Se você determinar que hashes são descartados frequentemente porque o armazenamento de hash está cheio, você pode aumentar o tamanho do armazenamento de hash modificando a configuração BranchCache.</p>

Parâmetros opcionais	Descrição
<i>Chave do servidor</i>	Você pode especificar uma chave de servidor que o serviço BranchCache usa para impedir que os clientes personifiquem o servidor BranchCache. Se você não especificar uma chave de servidor, uma será gerada aleatoriamente quando você criar a configuração BranchCache. Você pode definir a chave do servidor para um valor específico para que, se vários servidores estiverem fornecendo dados do BranchCache para os mesmos arquivos, os clientes possam usar hashes de qualquer servidor usando essa mesma chave do servidor. Se a chave do servidor contiver espaços, você deverá inserir a chave do servidor entre aspas.
<i>Modo de funcionamento</i>	O padrão é habilitar o BranchCache por compartilhamento. <ul style="list-style-type: none"> • Para criar uma configuração do BranchCache na qual você habilite o BranchCache por compartilhamento, não é possível especificar esse parâmetro opcional ou especificar <code>per-share</code>. • Para ativar automaticamente o BranchCache em todos os compartilhamentos, você deve definir o modo operacional como <code>all-shares</code>.

Passos

1. Habilite o SMB 2,1 e 3,0 conforme necessário:

- Defina o nível de privilégio como avançado: `set -privilege advanced`
- Verifique as configurações configuradas do SVM SMB para determinar se todas as versões necessárias do SMB estão ativadas: `vserver cifs options show -vserver vserver_name`
- Se necessário, ative o SMB 2,1: `vserver cifs options modify -vserver vserver_name -smb2-enabled true`

O comando habilita o SMB 2,0 e o SMB 2,1.

- Se necessário, ative o SMB 3,0: `vserver cifs options modify -vserver vserver_name -smb3-enabled true`

- Voltar ao nível de privilégio de administrador: `set -privilege admin`

2. Configurar BranchCache: `vserver cifs branchcache create -vserver vserver_name -hash -store-path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all}] [-server-key text] -operating-mode {per-share|all-shares}`

O caminho de storage de hash especificado deve existir e residir em um volume gerenciado pela SVM. O caminho também deve estar localizado em um volume gravável de leitura. O comando falha se o caminho for somente leitura ou não existir.

Se você quiser usar a mesma chave de servidor para configurações adicionais do SVM BranchCache, registre o valor inserido para a chave de servidor. A chave do servidor não aparece quando você exibe informações sobre a configuração do BranchCache.

3. Verifique se a configuração do BranchCache está correta: `vserver cifs branchcache show -vserver vserver_name`

Exemplos

Os comandos a seguir verificam se o SMB 2,1 e o 3,0 estão ativados e configuram o BranchCache para habilitar automaticamente o armazenamento em cache em todos os compartilhamentos SMB no SVM VS1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
-----
vs1      true      true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
Supported BranchCache Versions: enable_all
                                Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
                                CIFS BranchCache Operating Modes: all_shares
```

Os comandos a seguir verificam se o SMB 2,1 e o 3,0 estão ativados, configuram o BranchCache para habilitar o armazenamento em cache por compartilhamento no SVM VS1 e verificam a configuração do BranchCache:


```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
-----
vs1      true      true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
Supported BranchCache Versions: enable_all
                                Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share

```

Informações relacionadas

[Requisitos e diretrizes: Suporte à versão BranchCache](#)

[Onde encontrar informações sobre como configurar o BranchCache no escritório remoto](#)

[Crie um compartilhamento SMB habilitado para BranchCache](#)

[Ative o BranchCache em um compartilhamento SMB existente](#)

[Modifique a configuração do BranchCache](#)

[Desative a visão geral de BranchCache na SMB shares](#)

[Exclua a configuração BranchCache em SVMs](#)

Onde encontrar informações sobre como configurar o BranchCache no escritório remoto

Depois de configurar o BranchCache no servidor SMB, você deve instalar e configurar o BranchCache em computadores clientes e, opcionalmente, em servidores de cache em seu escritório remoto. A Microsoft fornece instruções para configurar o BranchCache no escritório remoto.

Instruções para configurar clientes de filiais e, opcionalmente, colocar em cache servidores para usar o BranchCache estão no site do Microsoft BranchCache.

["Microsoft BranchCache Docs: O que há de novo"](#)

Configurar compartilhamentos SMB habilitados para BranchCache

Configure a visão geral de compartilhamentos SMB habilitados para BranchCache

Depois de configurar o BranchCache no servidor SMB e na filial, você pode habilitar o BranchCache em compartilhamentos SMB que contenham conteúdo que você deseja permitir que os clientes nas filiais armazenem cache.

O cache BranchCache pode ser ativado em todos os compartilhamentos SMB no servidor SMB ou em uma base de compartilhamento por compartilhamento.

- Se você ativar o BranchCache de forma compartilhada, poderá ativar o BranchCache à medida que você cria o compartilhamento ou modificando compartilhamentos existentes.

Se você habilitar o armazenamento em cache em um compartilhamento SMB existente, o ONTAP começará a computar hashes e enviar metadados para clientes solicitando conteúdo assim que você ativar o BranchCache nesse compartilhamento.

- Quaisquer clientes que tenham uma conexão SMB existente a um compartilhamento não recebem suporte do BranchCache se o BranchCache for posteriormente habilitado nesse compartilhamento.

O ONTAP anuncia o suporte do BranchCache para um compartilhamento no momento em que a sessão SMB é configurada. Os clientes que já tiverem sessões estabelecidas quando o BranchCache estiver habilitado precisam se desconectar e se reconectar para usar o conteúdo em cache para esse compartilhamento.



Se o BranchCache em um compartilhamento SMB for posteriormente desativado, o ONTAP interrompe o envio de metadados para o cliente solicitante. Um cliente que precisa de dados recupera-os diretamente do servidor de conteúdo (servidor SMB).

Crie um compartilhamento SMB habilitado para BranchCache

Você pode ativar o BranchCache em um compartilhamento SMB ao criar o compartilhamento definindo a `branchcache` propriedade compartilhar.

Sobre esta tarefa

- Se o BranchCache estiver ativado no compartilhamento SMB, o compartilhamento deve ter a configuração de arquivos off-line definida como cache manual.

Esta é a configuração padrão quando você cria um compartilhamento.

- Você também pode especificar parâmetros opcionais adicionais de compartilhamento quando você cria o compartilhamento habilitado para BranchCache.
- Você pode definir a `branchcache` propriedade em um compartilhamento, mesmo que o BranchCache não esteja configurado e habilitado na máquina virtual de storage (SVM).

No entanto, se você quiser que o compartilhamento ofereça conteúdo em cache, configure e ative o

BranchCache no SVM.

- Como não há propriedades de compartilhamento padrão aplicadas ao compartilhamento quando você usa o `-share-properties` parâmetro, você deve especificar todas as outras propriedades de compartilhamento que deseja aplicar ao compartilhamento além da `branchcache` propriedade de compartilhamento usando uma lista delimitada por vírgulas.
- Para obter mais informações, consulte a página `man` para o `vserver cifs share create` comando.

Passo

1. Crie um compartilhamento SMB habilitado para BranchCache

```
vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties branchcache[,...]
```

2. Verifique se a propriedade BranchCache Share está definida no compartilhamento SMB usando o `vserver cifs share show` comando.

Exemplo

O comando a seguir cria um compartilhamento SMB habilitado para BranchCache chamado "data" com um caminho de `/data` no SVM VS1. Por padrão, a configuração arquivos off-line é definida como `manual`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path /data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
          Vserver: vs1
          Share: data
CIFS Server NetBIOS Name: VS1
          Path: /data
    Share Properties: branchcache
                    oplocks
                    browsable
                    changenotify
    Symlink Properties: enable
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
          Share Comment: -
          Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
          Volume Name: data
          Offline Files: manual
    Vscan File-Operations Profile: standard
```

Informações relacionadas

[Desativar BranchCache em um único compartilhamento SMB](#)

Ative o BranchCache em um compartilhamento SMB existente

Você pode ativar o BranchCache em um compartilhamento SMB existente adicionando a

`branchcache` propriedade share à lista existente de propriedades de compartilhamento.

Sobre esta tarefa

- Se o BranchCache estiver ativado no compartilhamento SMB, o compartilhamento deve ter a configuração de arquivos off-line definida como cache manual.

Se a configuração arquivos offline do compartilhamento existente não estiver definida como armazenamento manual em cache, você deverá configurá-lo modificando o compartilhamento.

- Você pode definir a `branchcache` propriedade em um compartilhamento, mesmo que o BranchCache não esteja configurado e habilitado na máquina virtual de storage (SVM).

No entanto, se você quiser que o compartilhamento ofereça conteúdo em cache, configure e ative o BranchCache no SVM.

- Quando você adiciona a `branchcache` propriedade de compartilhamento ao compartilhamento, as configurações de compartilhamento existentes e as propriedades de compartilhamento são preservadas.

A propriedade de compartilhamento BranchCache é adicionada à lista existente de propriedades de compartilhamento. Para obter mais informações sobre como usar o `vserver cifs share properties add` comando, consulte as páginas de manual.

Passos

1. Se necessário, configure a configuração de compartilhamento de arquivos offline para cache manual:
 - a. Determine qual é a configuração de compartilhamento de arquivos off-line usando o `vserver cifs share show` comando.
 - b. Se a definição de partilha de ficheiros offline não estiver definida para manual, altere-a para o valor pretendido: `vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual`
2. Ativar BranchCache em um compartilhamento SMB existente: `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`
3. Verifique se a propriedade BranchCache Share está definida no compartilhamento SMB: `vserver cifs share show -vserver vserver_name -share-name share_name`

Exemplo

O comando a seguir habilita o BranchCache em um compartilhamento SMB existente chamado "ata2" com um caminho `/data2` de no SVM VS1:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2
```

```
          Vserver: vs1
          Share: data2
CIFS Server NetBIOS Name: VS1
          Path: /data2
Share Properties: oplocks
                  browsable
                  changenotify
                  showsnapshot
Symlink Properties: -
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
          Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
          Volume Name: -
          Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties branchcache
```

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2
```

```
          Vserver: vs1
          Share: data2
CIFS Server NetBIOS Name: VS1
          Path: /data2
Share Properties: oplocks
                  browsable
                  showsnapshot
                  changenotify
                  branchcache
Symlink Properties: -
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
          Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
          Volume Name: -
          Offline Files: manual
Vscan File-Operations Profile: standard
```

Informações relacionadas

Gerencie e monitore a configuração do BranchCache

Modifique as configurações do BranchCache

Você pode modificar a configuração do serviço BranchCache em SVMs, incluindo alterar o caminho do diretório de armazenamento de hash, o tamanho máximo do diretório de armazenamento de hash, o modo operacional e quais versões do BranchCache são suportadas. Você também pode aumentar o tamanho do volume que contém o armazenamento de hash.

Passos

1. Execute a ação apropriada:

Se você quiser...	Digite o seguinte...
Modifique o tamanho do diretório de armazenamento de hash	<code>`vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB</code>
MB	GB
TB	PB]}`
Aumente o tamanho do volume que contém o armazenamento de hash	<code>`volume size -vserver vserver_name -volume volume_name -new-size new_size[k</code>
m	g
t]` Se o volume que contém o armazenamento de hash for preenchido, você poderá aumentar o tamanho do volume. Você pode especificar o novo tamanho de volume como um número seguido de uma designação de unidade.	Modifique o caminho do diretório de armazenamento de hash
Saiba mais sobre " Gerenciamento de volumes do FlexVol "	

Se você quiser...	Digite o seguinte...
<pre>`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true</pre>	<pre>false}`</pre> <p>Se o SVM for uma fonte de recuperação de desastres SVM, o caminho hash não poderá estar no volume raiz. Isso ocorre porque o volume raiz não é replicado para o destino de recuperação de desastres.</p> <p>O caminho hash BranchCache pode conter espaços em branco e quaisquer caracteres de nome de arquivo válidos.</p> <p>Se você modificar o caminho de hash, <code>-flush -hashes</code> é um parâmetro obrigatório que especifica se você deseja que o ONTAP lave os hashes do local de armazenamento de hash original. Pode definir os seguintes valores para o <code>-flush -hashes</code> parâmetro:</p> <p>Se você especificar <code>true</code>, o ONTAP excluirá os hashes no local original e criará novos hashes no novo local à medida que novas solicitações forem feitas por clientes habilitados para BranchCache.</p> <p>Se você especificar <code>false</code>, os hashes não serão lavados.</p> <p>+</p> <p>Nesse caso, você pode optar por reutilizar os hashes existentes mais tarde alterando o caminho de armazenamento de hash de volta para o local original.</p>
<p>Altere o modo de funcionamento</p>	<pre>`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share</pre>
<p>all-shares</p>	<pre>disable}`</pre> <p>Ao modificar o modo de funcionamento, deve estar ciente do seguinte:</p> <p>O ONTAP anuncia o suporte do BranchCache para um compartilhamento quando a sessão SMB está configurada.</p> <p>Os clientes que já tiverem sessões estabelecidas quando o BranchCache estiver habilitado precisam se desconectar e se reconectar para usar o conteúdo em cache para esse compartilhamento.</p>
<p>Altere o suporte à versão do BranchCache</p>	<pre>`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable</pre>
<p>v2-enable</p>	<pre>enable-all}`</pre>

2. Verifique as alterações de configuração usando o `vserver cifs branchcache show` comando.

Exibir informações sobre configurações do BranchCache

Você pode exibir informações sobre as configurações do BranchCache em máquinas virtuais de armazenamento (SVMs), que podem ser usadas ao verificar uma configuração ou ao determinar as configurações atuais antes de modificar uma configuração.

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir...	Digite este comando...
Informações resumidas sobre as configurações do BranchCache em todos os SVMs	<code>vserver cifs branchcache show</code>
Informações detalhadas sobre a configuração em uma SVM específica	<code>vserver cifs branchcache show -vserver <i>vserver_name</i></code>

Exemplo

O exemplo a seguir exibe informações sobre a configuração BranchCache no SVM VS1:

```
cluster1::> vserver cifs branchcache show -vserver vs1

                Vserver: vs1
Supported BranchCache Versions: enable_all
          Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share
```

Altere a chave do servidor BranchCache

Você pode alterar a chave do servidor BranchCache modificando a configuração BranchCache na máquina virtual de armazenamento (SVM) e especificando uma chave de servidor diferente.

Sobre esta tarefa

Você pode definir a chave do servidor para um valor específico para que, se vários servidores estiverem fornecendo dados do BranchCache para os mesmos arquivos, os clientes possam usar hashes de qualquer servidor usando essa mesma chave do servidor.

Quando você altera a chave do servidor, você também deve lavar o cache hash. Depois de limpar os hashes, o ONTAP cria novos hashes à medida que novas solicitações são feitas por clientes habilitados para BranchCache.

Passos

1. Altere a chave do servidor usando o seguinte comando: `vserver cifs branchcache modify`


```
-vserver vserver_name -server-key text -flush-hashes true
```

Ao configurar uma nova chave de servidor, você também deve especificar `-flush-hashes` e definir o valor como `true`.

2. Verifique se a configuração BranchCache está correta usando o `vserver cifs branchcache show` comando.

Exemplo

O exemplo a seguir define uma nova chave de servidor que contém espaços e limpa o cache de hash no SVM VS1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                Vserver: vs1
Supported BranchCache Versions: enable_all
                Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share
```

Informações relacionadas

[Razões pelas quais o ONTAP invalida hashes do BranchCache](#)

O BranchCache pré-computar hashes em caminhos especificados

Você pode configurar o serviço BranchCache para pré-calcular hashes para um único arquivo, para um diretório ou para todos os arquivos em uma estrutura de diretório. Isso pode ser útil se você quiser calcular hashes de dados em um compartilhamento habilitado pelo BranchCache durante horas fora do horário de pico.

Sobre esta tarefa

Se você quiser coletar uma amostra de dados antes de exibir estatísticas de hash, você deve usar os `statistics start` comandos e opcionais `statistics stop`.

- É necessário especificar a máquina virtual de storage (SVM) e o caminho no qual você deseja pré-calcular hashes.
- Você também deve especificar se deseja que os hashes sejam computados recursivamente.
- Se você quiser que os hashes sejam computados recursivamente, o serviço BranchCache percorre toda a árvore de diretórios sob o caminho especificado e calcula hashes para cada objeto elegível.

Passos

1. Pré-calcular hashes como desejado:

Se você quiser pré-calcular hashes em...	Digite o comando...
Um único arquivo ou diretório	<pre>vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false</pre>
Recursivamente em todos os arquivos em uma estrutura de diretório	<pre>vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true</pre>

2. Verifique se os hashes estão sendo computados usando o `statistics` comando:

- a. Exiba estatísticas para o `hashd` objeto na instância SVM desejada: `statistics show -object hashd -instance vserver_name`
- b. Verifique se o número de hashes criados está aumentando repetindo o comando.

Exemplos

O exemplo a seguir cria hashes no caminho `/data` e em todos os arquivos e subdiretórios contidos no SVM VS1:

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true
```

```
cluster1::> statistics show -object hashd -instance vs1
```

```
Object: hashd
```

```
Instance: vs1
```

```
Start-time: 9/6/2012 19:09:54
```

```
End-time: 9/6/2012 19:11:15
```

```
Cluster: cluster1
```

Counter	Value
branchcache_hash_created	85
branchcache_hash_files_replaced	0
branchcache_hash_rejected	0
branchcache_hash_store_bytes	0
branchcache_hash_store_size	0
instance_name	vs1
node_name	node1
node_uuid	11111111-1111-1111-1111-111111111111
process_name	-

```
cluster1::> statistics show -object hashd -instance vs1
```

```
Object: hashd
```

```
Instance: vs1
```

```
Start-time: 9/6/2012 19:09:54
```

```
End-time: 9/6/2012 19:11:15
```

```
Cluster: cluster1
```

Counter	Value
branchcache_hash_created	92
branchcache_hash_files_replaced	0
branchcache_hash_rejected	0
branchcache_hash_store_bytes	0
branchcache_hash_store_size	0
instance_name	vs1
node_name	node1
node_uuid	11111111-1111-1111-1111-111111111111
process_name	-

Informações relacionadas

["Configuração do monitoramento de desempenho"](#)

Lave os hashes do armazenamento de hash do SVM BranchCache

Você pode lavar todos os hashes armazenados em cache do armazenamento de hash BranchCache na máquina virtual de armazenamento (SVM). Isso pode ser útil se você tiver alterado a configuração BranchCache da filial. Por exemplo, se você reconfigurou recentemente o modo de armazenamento em cache de armazenamento distribuído para o modo de armazenamento em cache hospedado, você deseja limpar o armazenamento de hash.

Sobre esta tarefa

Depois de limpar os hashes, o ONTAP cria novos hashes à medida que novas solicitações são feitas por clientes habilitados para BranchCache.

Passo

1. Lave os hashes do armazenamento de hash BranchCache: `vserver cifs branchcache hash-flush -vserver vserver_name`

`vserver cifs branchcache hash-flush -vserver vs1`

Exibir estatísticas do BranchCache

Você pode exibir estatísticas do BranchCache para, entre outras coisas, identificar o desempenho do cache, determinar se sua configuração está fornecendo conteúdo em cache para clientes e determinar se os arquivos hash foram excluídos para dar espaço aos dados de hash mais recentes.

Sobre esta tarefa

O `hashd` objeto estatístico contém contadores que fornecem informações estatísticas sobre hashes BranchCache. O `cifs` objeto estatístico contém contadores que fornecem informações estatísticas sobre a atividade relacionada ao BranchCache. Você pode coletar e exibir informações sobre esses objetos no nível avançado de privilégios.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them  
only when directed to do so by support personnel.  
Do you want to continue? {y|n}: y
```

2. Exiba os contadores relacionados ao BranchCache usando o `statistics catalog counter show` comando.

Para obter mais informações sobre contadores de estatísticas, consulte a página de manual deste comando.

```
cluster1::*> statistics catalog counter show -object hashd
```

```
Object: hashd
```

Counter	Description
branchcache_hash_created	Number of times a request to generate BranchCache hash for a file succeeded.
branchcache_hash_files_replaced	Number of times a BranchCache hash file was deleted to make room for more recent hash data. This happens if the hash store size is exceeded.
branchcache_hash_rejected	Number of times a request to generate BranchCache hash data failed.
branchcache_hash_store_bytes	Total number of bytes used to store hash data.
branchcache_hash_store_size	Total space used to store BranchCache hash data for the Vserver.
instance_name	Instance Name
instance_uuid	Instance UUID
node_name	System node name
node_uuid	System node id

9 entries were displayed.

```
cluster1::*> statistics catalog counter show -object cifs
```

```
Object: cifs
```

Counter	Description
active_searches	Number of active searches over SMB and SMB2
auth_reject_too_many	Authentication refused after too many requests were made in rapid succession
avg_directory_depth	Average number of directories crossed by SMB and SMB2 path-based commands
avg_junction_depth	Average number of junctions crossed by SMB and SMB2 path-based commands

```

branchcache_hash_fetch_fail Total number of times a request to fetch
hash
data failed. These are failures when
attempting to read existing hash data.
It
does not include attempts to fetch hash
data
that has not yet been generated.
branchcache_hash_fetch_ok Total number of times a request to fetch
hash
data succeeded.
branchcache_hash_sent_bytes Total number of bytes sent to clients
requesting hashes.
branchcache_missing_hash_bytes
Total number of bytes of data that had
to be
read by the client because the hash for
that
content was not available on the server.
....Output truncated....

```

3. Colete estatísticas relacionadas ao BranchCache usando os `statistics start` comandos e `statistics stop`

```

cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11

```

4. Exiba as estatísticas coletadas do BranchCache usando o `statistics show` comando.

```
cluster1::*> statistics show -object cifs -counter  
branchcache_hash_sent_bytes -sample-id 11
```

```
Object: cifs  
Instance: vs1  
Start-time: 12/26/2012 19:50:24  
End-time: 12/26/2012 19:51:01  
Cluster: cluster1
```

Counter	Value
branchcache_hash_sent_bytes	0
branchcache_hash_sent_bytes	0
branchcache_hash_sent_bytes	0
branchcache_hash_sent_bytes	0

```
cluster1::*> statistics show -object cifs -counter  
branchcache_missing_hash_bytes -sample-id 11
```

```
Object: cifs  
Instance: vs1  
Start-time: 12/26/2012 19:50:24  
End-time: 12/26/2012 19:51:01  
Cluster: cluster1
```

Counter	Value
branchcache_missing_hash_bytes	0
branchcache_missing_hash_bytes	0
branchcache_missing_hash_bytes	0
branchcache_missing_hash_bytes	0

5. Voltar ao nível de privilégio de administrador: `set -privilege admin`

```
cluster1::*> set -privilege admin
```

Informações relacionadas

[Exibindo estatísticas](#)

["Configuração do monitoramento de desempenho"](#)

Suporte para objetos de Diretiva de Grupo BranchCache

O ONTAP BranchCache fornece suporte para objetos de Diretiva de Grupo (GPOs) do

BranchCache, que permitem o gerenciamento centralizado para determinados parâmetros de configuração do BranchCache. Existem dois GPOs usados para BranchCache, a publicação Hash para BranchCache GPO e o suporte de versão Hash para BranchCache GPO.

- **Publicação Hash para o GPO BranchCache**

A publicação Hash para BranchCache GPO corresponde ao `-operating-mode` parâmetro. Quando ocorrem atualizações de GPO, esse valor é aplicado a objetos de máquina virtual de armazenamento (SVM) contidos na unidade organizacional (ou) à qual a diretiva de grupo se aplica.

- **Suporte a versão Hash para o GPO BranchCache**

O suporte de versão Hash para GPO BranchCache corresponde ao `-versions` parâmetro. Quando ocorrem atualizações de GPO, esse valor é aplicado a objetos SVM contidos na unidade organizacional à qual a diretiva de grupo se aplica.

Informações relacionadas

[Aplicando objetos de Diretiva de Grupo a servidores CIFS](#)

Exibir informações sobre os objetos de Diretiva de Grupo BranchCache

Você pode exibir informações sobre a configuração GPO (Group Policy Object) do servidor CIFS para determinar se os GPOs de BranchCache estão definidos para o domínio ao qual o servidor CIFS pertence e, em caso afirmativo, quais são as configurações permitidas. Você também pode determinar se as configurações de GPO do BranchCache são aplicadas ao servidor CIFS.

Sobre esta tarefa

Embora uma configuração de GPO seja definida dentro do domínio ao qual o servidor CIFS pertence, ela não é necessariamente aplicada à unidade organizacional (ou) que contém a máquina virtual de armazenamento (SVM) habilitada para CIFS. A configuração de GPO aplicada é o subconjunto de todos os GPOs definidos que são aplicados ao SVM habilitado para CIFS. As configurações do BranchCache aplicadas por meio de GPOs substituem as configurações aplicadas por meio da CLI.

Passos

1. Exiba a configuração de GPO BranchCache definida para o domínio do ativo Directory usando o `vserver cifs group-policy show-defined` comando.



Este exemplo não exibe todos os campos de saída disponíveis para o comando. A saída é truncada.


```
cluster1::> vserver cifs group-policy show-defined -vserver vs1
```

```
Vserver: vs1
```

```
-----  
      GPO Name: Default Domain Policy  
      Level: Domain  
      Status: enabled  
Advanced Audit Settings:  
  Object Access:  
    Central Access Policy Staging: failure  
Registry Settings:  
  Refresh Time Interval: 22  
  Refresh Random Offset: 8  
  Hash Publication Mode for BranchCache: per-share  
  Hash Version Support for BranchCache: version1  
[...]  
  
      GPO Name: Resultant Set of Policy  
      Status: enabled  
Advanced Audit Settings:  
  Object Access:  
    Central Access Policy Staging: failure  
Registry Settings:  
  Refresh Time Interval: 22  
  Refresh Random Offset: 8  
  Hash Publication for Mode BranchCache: per-share  
  Hash Version Support for BranchCache: version1  
[...]
```

2. Exiba a configuração de GPO BranchCache aplicada ao servidor CIFS usando o `vserver cifs group-policy show-applied` comando. ""



Este exemplo não exibe todos os campos de saída disponíveis para o comando. A saída é truncada.

```

cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
-----
    GPO Name: Default Domain Policy
      Level: Domain
      Status: enabled
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication Mode for BranchCache: per-share
  Hash Version Support for BranchCache: version1
[...]

    GPO Name: Resultant Set of Policy
      Level: RSOP
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication Mode for BranchCache: per-share
  Hash Version Support for BranchCache: version1
[...]

```

Informações relacionadas

[Ativar ou desativar o suporte de GPO num servidor CIFS](#)

Desativar BranchCache em compartilhamentos SMB

Desative a visão geral de BranchCache na SMB shares

Se você não quiser fornecer serviços de armazenamento em cache BranchCache em determinados compartilhamentos SMB, mas talvez queira fornecer serviços de armazenamento em cache nesses compartilhamentos posteriormente, você pode desativar o BranchCache de forma compartilhada. Se você tiver o BranchCache configurado para oferecer armazenamento em cache em todos os compartilhamentos, mas quiser desativar temporariamente todos os serviços de armazenamento em cache, você pode modificar a configuração do BranchCache para interromper o armazenamento em cache automático em todos os compartilhamentos.

Se o BranchCache em um compartilhamento SMB for posteriormente desativado após a primeira ativação, o ONTAP pára de enviar metadados para o cliente solicitante. Um cliente que precisa de dados os recupera diretamente do servidor de conteúdo (servidor CIFS na máquina virtual de armazenamento (SVM)).

Informações relacionadas

[Configurando compartilhamentos SMB habilitados para BranchCache](#)

Desative o BranchCache em um único compartilhamento SMB

Se você não quiser oferecer serviços de armazenamento em cache em determinados compartilhamentos que ofereciam conteúdo em cache anteriormente, você pode desativar o BranchCache em um compartilhamento SMB existente.

Passo

1. Introduza o seguinte comando: `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties branchcache`

A propriedade BranchCache Share foi removida. Outras propriedades de compartilhamento aplicadas permanecem em vigor.

Exemplo

O comando a seguir desativa o BranchCache em um compartilhamento SMB existente chamado "ata2":

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2
```

```
        Vserver: vs1
        Share: data2
CIFS Server NetBIOS Name: VS1
        Path: /data2
    Share Properties: oplocks
                    browsable
                    changenotify
                    attributecache
                    branchcache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
            Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: -
        Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
data2 -share-properties branchcache
```

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2
```

```
        Vserver: vs1
        Share: data2
CIFS Server NetBIOS Name: VS1
        Path: /data2
    Share Properties: oplocks
                    browsable
                    changenotify
                    attributecache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
            Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: -
        Offline Files: manual
Vscan File-Operations Profile: standard
```

Parar o armazenamento em cache automático em todos os compartilhamentos SMB

Se a configuração do BranchCache ativar automaticamente o armazenamento em cache em todos os compartilhamentos SMB em cada máquina virtual de storage (SVM), você poderá modificar a configuração do BranchCache para interromper o armazenamento em cache automático de conteúdo para todos os compartilhamentos SMB.

Sobre esta tarefa

Para interromper o armazenamento em cache automático em todos os compartilhamentos SMB, você altera o modo operacional BranchCache para cache por compartilhamento.

Passos

1. Configure o BranchCache para interromper o armazenamento em cache automático em todos os compartilhamentos SMB: `vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
2. Verifique se a configuração do BranchCache está correta: `vserver cifs branchcache show -vserver vserver_name`

Exemplo

O comando a seguir altera a configuração BranchCache na máquina virtual de armazenamento (SVM, anteriormente conhecido como SVM) VS1 para parar o armazenamento em cache automático em todos os compartilhamentos SMB:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                Vserver: vs1
Supported BranchCache Versions: enable_all
                Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share
```

Desative ou ative o BranchCache no SVM

O que acontece quando você desativa ou reabilita o BranchCache no servidor CIFS

Se você configurou anteriormente o BranchCache, mas não quer que os clientes da filial usem conteúdo em cache, você pode desativar o cache no servidor CIFS. Você deve estar ciente do que acontece quando você desativa o BranchCache.

Quando você desativa o BranchCache, o ONTAP não computa hashes ou envia os metadados para o cliente solicitante. No entanto, não há interrupção no acesso aos arquivos. Depois disso, quando clientes habilitados para BranchCache solicitam informações de metadados para conteúdo que desejam acessar, o ONTAP responde com um erro definido pela Microsoft, que faz com que o cliente envie uma segunda solicitação, solicitando o conteúdo real. Em resposta à solicitação de conteúdo, o servidor CIFS envia o conteúdo real

armazenado na máquina virtual de storage (SVM).

Depois que o BranchCache é desativado no servidor CIFS, os compartilhamentos SMB não anunciam os recursos do BranchCache. Para acessar dados em novas conexões SMB, os clientes fazem solicitações normais de leitura SMB.

Você pode reativar o BranchCache no servidor CIFS a qualquer momento.

- Como o armazenamento de hash não é excluído quando você desabilita o BranchCache, o ONTAP pode usar os hashes armazenados ao responder a solicitações de hash depois de reativar o BranchCache, desde que o hash solicitado ainda seja válido.
- Quaisquer clientes que tenham feito conexões SMB com compartilhamentos habilitados para BranchCache durante o tempo em que o BranchCache foi desativado não recebem suporte para BranchCache se o BranchCache for posteriormente reativado.

Isso ocorre porque o ONTAP anuncia o suporte do BranchCache para um compartilhamento no momento em que a sessão SMB é configurada. Os clientes que estabeleceram sessões para compartilhamentos habilitados para BranchCache enquanto o BranchCache foi desativado precisam se desconectar e se reconectar para usar conteúdo em cache para esse compartilhamento.



Se você não quiser salvar o armazenamento de hash depois de desativar o BranchCache em um servidor CIFS, você pode excluí-lo manualmente. Se você reabilitar o BranchCache, você deve garantir que o diretório de armazenamento de hash existe. Depois que o BranchCache é reativado, os compartilhamentos habilitados para BranchCache anunciam os recursos do BranchCache. O ONTAP cria novos hashes à medida que novas solicitações são feitas por clientes habilitados para BranchCache.

Desative ou ative o BranchCache

Você pode desativar o BranchCache na máquina virtual de armazenamento (SVM) alterando o modo operacional BranchCache para `disabled`. Você pode ativar o BranchCache a qualquer momento alterando o modo operacional para oferecer serviços BranchCache por compartilhamento ou automaticamente para todos os compartilhamentos.

Passos

1. Execute o comando apropriado:

Se você quiser...	Em seguida, digite o seguinte...
Desativar BranchCache	<pre>vserver cifs branchcache modify -vserver vserver_name -operating-mode disable</pre>
Ativar BranchCache por partilha	<pre>vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share</pre>

Se você quiser...	Em seguida, digite o seguinte...
Ative o BranchCache para todos os compartilhamentos	<code>vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares</code>

2. Verifique se o modo de operação BranchCache está configurado com a configuração desejada: `vserver cifs branchcache show -vserver vserver_name`

Exemplo

O exemplo a seguir desativa o BranchCache no SVM VS1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                Vserver: vs1
Supported BranchCache Versions: enable_all
                Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: disable
```

Exclua a configuração BranchCache em SVMs

O que acontece quando você exclui a configuração BranchCache

Se você configurou o BranchCache anteriormente, mas não deseja que a máquina virtual de armazenamento (SVM) continue fornecendo conteúdo em cache, você pode excluir a configuração BranchCache no servidor CIFS. Você deve estar ciente do que acontece quando você exclui a configuração.

Quando você exclui a configuração, o ONTAP remove as informações de configuração desse SVM do cluster e interrompe o serviço BranchCache. Você pode escolher se o ONTAP deve excluir o armazenamento de hash no SVM.

A exclusão da configuração BranchCache não interrompe o acesso por clientes habilitados para BranchCache. Depois disso, quando clientes habilitados para BranchCache solicitam informações de metadados sobre conexões SMB existentes para conteúdo que já está em cache, o ONTAP responde com um erro definido pela Microsoft, o que faz com que o cliente envie uma segunda solicitação, solicitando o conteúdo real. Em resposta à solicitação de conteúdo, o servidor CIFS envia o conteúdo real armazenado no SVM.

Depois que a configuração do BranchCache é excluída, compartilhamentos SMB não anunciam recursos do BranchCache. Para acessar conteúdo que não foi armazenado em cache anteriormente usando novas conexões SMB, os clientes fazem solicitações de SMB de leitura normais.

Exclua a configuração do BranchCache

O comando que você usa para excluir o serviço BranchCache na máquina virtual de armazenamento (SVM) difere dependendo se você deseja excluir ou manter hashes existentes.

Passo

1. Execute o comando apropriado:

Se você quiser...	Em seguida, digite o seguinte...
Exclua a configuração do BranchCache e exclua hashes existentes	<pre>vserver cifs branchcache delete -vserver vserver_name -flush-hashes true</pre>
Exclua a configuração do BranchCache, mas mantenha hashes existentes	<pre>vserver cifs branchcache delete -vserver vserver_name -flush-hashes false</pre>

Exemplo

O exemplo a seguir exclui a configuração BranchCache no SVM VS1 e exclui todos os hashes existentes:

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes  
true
```

O que acontece com BranchCache ao reverter

É importante entender o que acontece quando você reverte o ONTAP para uma versão que não suporte o BranchCache.

- Quando você reverte para uma versão do ONTAP que não suporta BranchCache, os compartilhamentos SMB não anunciam os recursos do BranchCache para clientes habilitados para BranchCache; portanto, os clientes não solicitam informações de hash.

Em vez disso, eles solicitam o conteúdo real usando solicitações normais de leitura SMB. Em resposta à solicitação de conteúdo, o servidor SMB envia o conteúdo real armazenado na máquina virtual de storage (SVM).

- Quando um nó que hospeda um armazenamento de hash é revertido para uma versão que não suporta BranchCache, o administrador de armazenamento precisa reverter manualmente a configuração do BranchCache usando um comando que é impresso durante a reversão.

Esse comando exclui a configuração e os hashes do BranchCache.

Após a conclusão da reversão, o administrador de armazenamento pode excluir manualmente o diretório que continha o armazenamento de hash, se desejado.

Informações relacionadas

Melhorar o desempenho de cópia remota da Microsoft

Melhore a visão geral do desempenho de cópia remota da Microsoft

A Microsoft Offloaded Data Transfer (ODX), também conhecida como *copy offload*, permite transferências diretas de dados dentro ou entre dispositivos de armazenamento compatíveis sem transferir os dados através do computador host.

O ONTAP oferece suporte ao ODX para os protocolos SMB e SAN. A origem pode ser um servidor CIFS ou LUN, e o destino pode ser um servidor CIFS ou LUN.

Em transferências de arquivos não ODX, os dados são lidos da fonte e são transferidos pela rede para o computador cliente. O computador cliente transfere os dados de volta pela rede para o destino. Em resumo, o computador cliente lê os dados da origem e grava-os no destino. Com as transferências de arquivos ODX, os dados são copiados diretamente da origem para o destino.

Como as cópias descarregadas do ODX são realizadas diretamente entre o armazenamento de origem e destino, há benefícios significativos de desempenho. Os benefícios de desempenho obtidos incluem tempo de cópia mais rápido entre a origem e o destino, utilização reduzida de recursos (CPU, memória) no cliente e utilização reduzida da largura de banda de e/S de rede.

Para ambientes SMB, essa funcionalidade só está disponível quando o cliente e o servidor de armazenamento suportam SMB 3,0 e o recurso ODX. Para ambientes SAN, essa funcionalidade só está disponível quando o cliente e o servidor de armazenamento suportam o recurso ODX. Os computadores clientes que suportam ODX e têm o ODX ativado automaticamente e de forma transparente usam transferência de arquivos descarregados ao mover ou copiar arquivos. O ODX é usado independentemente de você arrastar e soltar arquivos através do Windows Explorer ou usar comandos de cópia de arquivo de linha de comando, ou se um aplicativo cliente inicia solicitações de cópia de arquivo.

Informações relacionadas

[Melhorar o tempo de resposta do cliente fornecendo referências de nó automáticas SMB com localização automática](#)

["Configuração SMB para Microsoft Hyper-V e SQL Server"](#)

Como o ODX funciona

A descarga de cópia ODX usa um mecanismo baseado em token para ler e gravar dados dentro ou entre servidores CIFS habilitados para ODX. Em vez de rotear os dados através do host, o servidor CIFS envia um pequeno token, que representa os dados, para o cliente. O cliente ODX apresenta esse token para o servidor de destino, que então pode transferir os dados representados por esse token da origem para o destino.

Quando um cliente ODX descobre que o servidor CIFS é compatível com ODX, ele abre o arquivo de origem e solicita um token do servidor CIFS. Depois de abrir o arquivo de destino, o cliente usa o token para instruir o servidor a copiar os dados diretamente da origem para o destino.

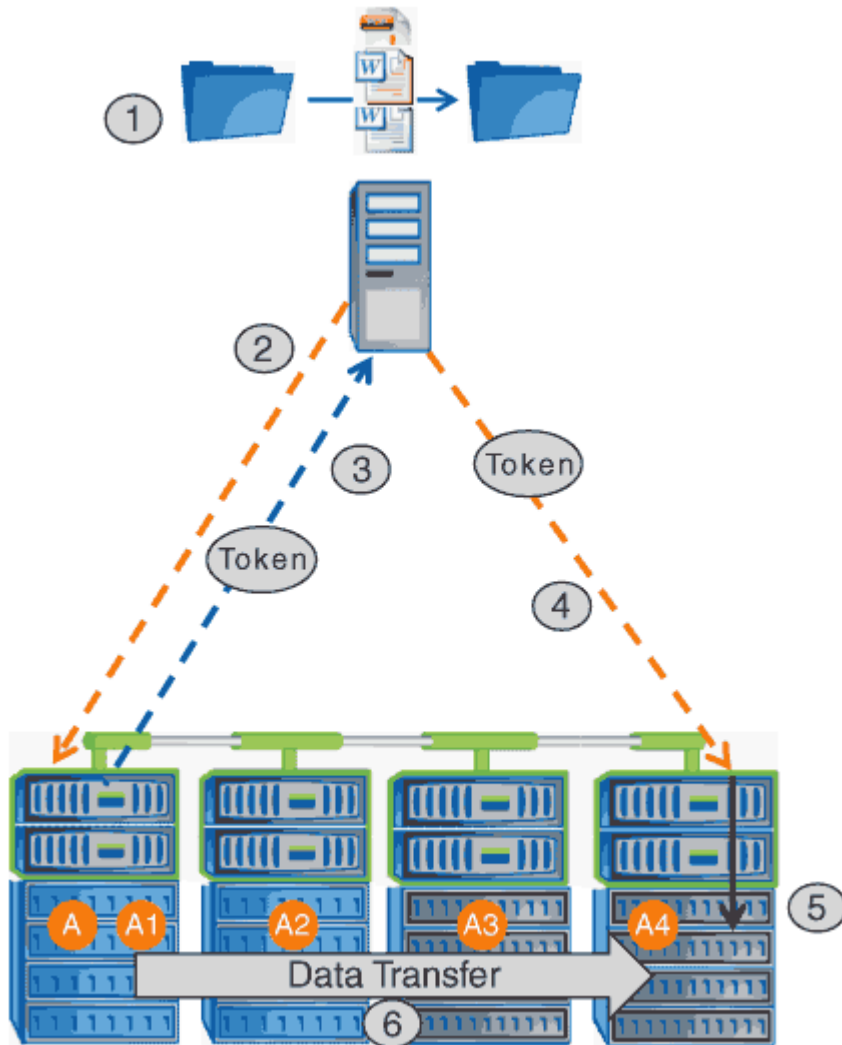


A origem e o destino podem estar na mesma máquina virtual de storage (SVM) ou em SVMs diferentes, dependendo do escopo da operação de cópia.

O token serve como uma representação pontual dos dados. Como exemplo, quando você copia dados entre locais de armazenamento, um token representando um segmento de dados é retornado ao cliente solicitante, que o cliente copia para o destino, removendo assim a necessidade de copiar os dados subjacentes através do cliente.

O ONTAP suporta tokens que representam 8 MB de dados. Cópias ODX de mais de 8 MB são executadas usando vários tokens, com cada token representando 8 MB de dados.

A figura a seguir explica as etapas envolvidas com uma operação de cópia ODX:



1. Um usuário copia ou move um arquivo usando o Windows Explorer, uma interface de linha de comando ou como parte de uma migração de máquina virtual, ou um aplicativo inicia cópias ou movimentos de arquivo.
2. O cliente compatível com ODX converte automaticamente essa solicitação de transferência em uma solicitação ODX.

A solicitação ODX que é enviada para o servidor CIFS contém uma solicitação de um token.

3. Se o ODX estiver habilitado no servidor CIFS e a conexão for sobre SMB 3,0, o servidor CIFS gera um token, que é uma representação lógica dos dados na origem.
4. O cliente recebe um token que representa os dados e os envia com a solicitação de gravação para o servidor CIFS de destino.

Estes são os únicos dados que são copiados pela rede da origem para o cliente e, em seguida, do cliente para o destino.

5. O token é entregue ao subsistema de armazenamento.
6. O SVM executa a cópia ou a movimentação internamente.

Se o arquivo copiado ou movido for maior que 8 MB, vários tokens serão necessários para executar a cópia. Passos 2 a 6 conforme executado conforme necessário para concluir a cópia.



Se houver uma falha com a cópia descarregada do ODX, a operação de cópia ou movimentação volta para leituras e gravações tradicionais para a operação de cópia ou movimentação. Da mesma forma, se o servidor CIFS de destino não suportar ODX ou ODX estiver desativado, a operação de cópia ou movimentação volta para leituras e gravações tradicionais para a operação de cópia ou movimentação.

Requisitos para usar ODX

Antes de usar o ODX para descarregar cópias com sua máquina virtual de armazenamento (SVM), você precisa estar ciente de certos requisitos.

Requisitos de versão do ONTAP

As versões do ONTAP suportam ODX para descarregamentos de cópias.

Requisitos de versão SMB

- O ONTAP suporta ODX com SMB 3,0 e posterior.
- O SMB 3,0 deve estar habilitado no servidor CIFS antes que o ODX possa ser habilitado:
 - Ativar o ODX também ativa o SMB 3,0, se ele ainda não estiver ativado.
 - Desativar o SMB 3,0 também desativa o ODX.

Requisitos de servidor e cliente do Windows

Antes de poder utilizar o ODX para descarregar cópias, o cliente Windows tem de suportar a funcionalidade.

O "[Matriz de interoperabilidade do NetApp](#)" contém as informações mais recentes sobre clientes Windows suportados.

Requisitos de volume

- Os volumes de origem devem ter no mínimo 1,25 GB.
- Se você usar volumes compactados, o tipo de compactação deve ser adaptável e somente o tamanho do grupo de compactação 8K é suportado.

O tipo de compressão secundária não é suportado.

Diretrizes para o uso do ODX

Antes de poder usar o ODX para descarga de cópia, você precisa estar ciente das diretrizes. Por exemplo, você precisa saber em quais tipos de volumes você pode usar

ODX e você precisa entender as considerações do ODX intra-cluster e inter-cluster.

Diretrizes de volume

- Você não pode usar o ODX para descarga de cópia com as seguintes configurações de volume:
 - O tamanho do volume de origem é inferior a 1,25 GB
O tamanho do volume deve ser de 1,25 GB ou maior para usar o ODX.
 - Volumes só de leitura
O ODX não é usado para arquivos e pastas residentes em espelhos de compartilhamento de carga ou em volumes de destino SnapMirror ou SnapVault.
 - Se o volume de origem não for deduplicado
- Cópias ODX são suportadas apenas para cópias intra-cluster.

Não é possível usar o ODX para copiar arquivos ou pastas para um volume em outro cluster.

Outras diretrizes

- Em ambientes SMB, para usar o ODX para descarga de cópia, os arquivos devem ter 256 kb ou mais.
Arquivos menores são transferidos usando uma operação de cópia tradicional.
- O descarregamento de cópia ODX usa a deduplicação como parte do processo de cópia.
Se você não quiser que a deduplicação ocorra em volumes SVM ao copiar ou mover dados, desative a descarga de cópia ODX nesse SVM.
- O aplicativo que executa a transferência de dados deve ser escrito para suportar ODX.

As operações de aplicação que suportam ODX incluem o seguinte:

- Operações de gerenciamento do Hyper-V, como criar e converter discos rígidos virtuais (VHDs), gerenciar cópias Snapshot e copiar arquivos entre máquinas virtuais
- Operações do Windows Explorer
- Comandos de cópia do Windows PowerShell
- Comandos de cópia do prompt de comando do Windows

Robocopy no prompt de comando do Windows suporta ODX.



Os aplicativos devem estar em execução em servidores Windows ou clientes que suportem ODX.

+

Para obter mais informações sobre aplicativos ODX compatíveis em servidores e clientes Windows, consulte a Biblioteca Microsoft TechNet.

Informações relacionadas

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Casos de uso para ODX

Você deve estar ciente dos casos de uso para usar o ODX em SVMs para que você possa determinar em que circunstâncias o ODX fornece benefícios de desempenho.

Os servidores e clientes do Windows que suportam ODX usam a descarga de cópia como a forma padrão de copiar dados em servidores remotos. Se o servidor ou cliente do Windows não suportar ODX ou a descarga de cópia ODX falhar em qualquer ponto, a operação de cópia ou movimentação volta para leituras e gravações tradicionais para a operação de cópia ou movimentação.

Os seguintes casos de uso suportam o uso de cópias e movimentos ODX:

- Intra-volume

Os arquivos de origem e destino ou LUNs estão dentro do mesmo volume.

- Entre volumes, mesmo nó e SVM

Os arquivos de origem e destino ou LUNs estão em volumes diferentes localizados no mesmo nó. Os dados pertencem ao mesmo SVM.

- Entre volumes, nós diferentes e o mesmo SVM

Os arquivos de origem e destino ou LUNs estão em volumes diferentes localizados em nós diferentes. Os dados pertencem ao mesmo SVM.

- Entre SVM, mesmo nó

O arquivo de origem e destino ou LUNs estão em volumes diferentes localizados no mesmo nó. Os dados pertencem a diferentes SVMs.

- Entre SVM, nós diferentes

O arquivo de origem e destino ou LUNs estão em volumes diferentes localizados em nós diferentes. Os dados pertencem a diferentes SVMs.

- Inter-cluster

As LUNs de origem e destino estão em volumes diferentes, localizados em nós diferentes, entre clusters. Isso só é suportado para SAN e não funciona para CIFS.

Existem alguns casos de uso especiais adicionais:

- Com a implementação do ONTAP ODX, você pode usar o ODX para copiar arquivos entre compartilhamentos SMB e unidades virtuais conectadas a FC ou iSCSI.

Você pode usar o Windows Explorer, a CLI do Windows ou PowerShell, Hyper-V ou outras aplicações compatíveis com ODX para copiar ou mover arquivos sem interrupções usando a descarga de cópia ODX entre compartilhamentos SMB e LUNs conectados, desde que os compartilhamentos SMB e LUNs estejam no mesmo cluster.

- O Hyper-V fornece alguns casos de uso adicionais para descarga de cópia ODX:

- Você pode usar a passagem de descarga de cópia ODX com o Hyper-V para copiar dados dentro ou através de arquivos de disco rígido virtual (VHD) ou para copiar dados entre compartilhamentos SMB

mapeados e LUNs iSCSI conectados dentro do mesmo cluster.

Isso permite que cópias de sistemas operacionais convidados passem para o storage subjacente.

- Ao criar VHDs de tamanho fixo, o ODX é usado para inicializar o disco com zeros, usando um token zerado bem conhecido.
- A descarga de cópia ODX é usada para migração de armazenamento de máquina virtual se o armazenamento de origem e destino estiver no mesmo cluster.



Para aproveitar os casos de uso para a passagem de descarga de cópia ODX com Hyper-V, o sistema operacional convidado deve suportar ODX e os discos do sistema operacional convidado devem ser discos SCSI suportados pelo armazenamento (SMB ou SAN) que suporte ODX. Os discos IDE no sistema operacional convidado não suportam passagem ODX.

Ativar ou desativar o ODX

Você pode ativar ou desativar o ODX em máquinas virtuais de armazenamento (SVMs). O padrão é habilitar o suporte para descarga de cópia ODX se o SMB 3,0 também estiver habilitado.

Antes de começar

O SMB 3,0 deve estar ativado.

Sobre esta tarefa

Se você desabilitar o SMB 3,0, o ONTAP também desabilitará o SMB ODX. Se você reabilitar o SMB 3,0, será necessário reativar manualmente o SMB ODX.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Execute uma das seguintes ações:

Se você quiser que o descarregamento de cópia ODX seja...	Digite o comando...
Ativado	<pre>vserver cifs options modify -vserver vserver_name -copy-offload-enabled true</pre>
Desativado	<pre>vserver cifs options modify -vserver vserver_name -copy-offload-enabled false</pre>

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exemplo

O exemplo a seguir habilita a descarga de cópia ODX no SVM VS1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster1::*> set -privilege admin
```

Informações relacionadas

[Opções de servidor SMB disponíveis](#)

Melhore o tempo de resposta do cliente fornecendo referências de nó automáticas SMB com localização automática

Melhore o tempo de resposta do cliente fornecendo referências de nó automáticas SMB com visão geral de localização automática

A localização automática usa referências de nó automáticas SMB para aumentar a performance do cliente SMB em máquinas virtuais de armazenamento (SVMs). As referências automáticas de nós redirecionam automaticamente o cliente solicitante para um LIF no SVM do nó que hospeda o volume no qual os dados residem, o que pode levar a tempos de resposta aprimorados do cliente.

Quando um cliente SMB se conecta a um compartilhamento SMB hospedado no SVM, ele pode se conectar usando um LIF que está em um nó que não possui os dados solicitados. O nó ao qual o cliente está conectado acessa dados de propriedade de outro nó usando a rede do cluster. O cliente pode ter tempos de resposta mais rápidos se a conexão SMB usar um LIF localizado no nó que contém os dados solicitados:

- O ONTAP fornece essa funcionalidade usando referências do Microsoft DFS para informar clientes SMB que um arquivo ou pasta solicitado no namespace está hospedado em outro lugar.

Um nó faz uma referência quando determina que há um LIF SVM no nó que contém os dados.

- As referências automáticas de nós são suportadas para endereços IP IPv4 e IPv6 LIF.
- As referências são feitas com base na localização da raiz da partilha através da qual o cliente está ligado.
- A referência ocorre durante a negociação SMB.

A referência é feita antes da conexão ser estabelecida. Depois que o ONTAP refere o cliente SMB ao nó de destino, a conexão é feita e o cliente acessa os dados através do caminho LIF referido a partir desse ponto. Isso permite que os clientes tenham acesso mais rápido aos dados e evite a comunicação de cluster adicional.



Se um compartilhamento abranger vários pontos de junção e algumas das junções forem para volumes contidos em outros nós, os dados dentro do compartilhamento serão espalhados por vários nós. Como o ONTAP fornece referências locais à raiz do compartilhamento, o ONTAP deve usar a rede de cluster para recuperar os dados contidos nesses volumes não locais. Com esse tipo de arquitetura de namespace, as referências de nó automáticas podem não fornecer benefícios significativos de desempenho.

Se o nó que hospeda os dados não tiver um LIF disponível, o ONTAP estabelece a conexão usando o LIF escolhido pelo cliente. Depois que um arquivo é aberto por um cliente SMB, ele continua a acessar o arquivo através da mesma conexão referida.

Se, por qualquer motivo, o servidor CIFS não puder fazer uma referência, não haverá interrupção no serviço SMB. A conexão SMB é estabelecida como se as referências de nó automáticas não estivessem ativadas.

Informações relacionadas

[Melhorando o desempenho de cópia remota da Microsoft](#)

Requisitos e diretrizes para o uso de referências automáticas de nós

Antes de poder usar referências de nó automáticas SMB, também conhecidas como *autolocation*, você precisa estar ciente de certos requisitos, incluindo quais versões do ONTAP suportam o recurso. Você também precisa saber sobre versões de protocolo SMB compatíveis e algumas outras diretrizes especiais.

Requisitos de versão e licença do ONTAP

- Todos os nós no cluster devem estar executando uma versão do ONTAP que suporte referências automáticas de nós.
- Os Widelinks devem estar ativados em um compartilhamento SMB para usar a autenticação automática.
- O CIFS deve ser licenciado e um servidor SMB deve existir nos SVMs. A licença SMB está incluída no "ONTAP One". Se não tiver o ONTAP One e a licença não estiver instalada, contacte o seu representante de vendas.

Requisitos de versão do protocolo SMB

- Para SVMs, o ONTAP oferece suporte a referências automáticas de nós em todas as versões do SMB.

Requisitos do cliente SMB

Todos os clientes Microsoft suportados pelo ONTAP suportam referências de nó automáticas SMB.

A Matriz de interoperabilidade contém as informações mais recentes sobre quais clientes Windows ONTAP suportam.

["Ferramenta de Matriz de interoperabilidade do NetApp"](#)

Requisitos de LIF de dados

Se você quiser usar um data LIF como potencial referência para clientes SMB, crie LIFs de dados com NFS e CIFS habilitados.

As referências automáticas de nós podem falhar ao funcionar se o nó de destino contiver LIFs de dados que são ativados apenas para o protocolo NFS ou ativados apenas para o protocolo SMB.

Se este requisito não for cumprido, o acesso aos dados não será afetado. O cliente SMB mapeia o compartilhamento usando o LIF original usado pelo cliente para se conectar ao SVM.

Requisitos de autenticação NTLM ao fazer uma conexão SMB referida

A autenticação NTLM deve ser permitida no domínio que contém o servidor CIFS e nos domínios que contêm clientes que desejam usar referências automáticas de nós.

Ao fazer uma referência, o servidor SMB refere um endereço IP ao cliente Windows. Como a autenticação NTLM é usada ao fazer uma conexão usando um endereço IP, a autenticação Kerberos não é executada para conexões referidas.

Isso acontece porque o cliente Windows não pode criar o nome principal do serviço usado pelo Kerberos (que é do formulário `service/NetBIOS name` e `service/FQDN`), o que significa que o cliente não pode solicitar um ticket Kerberos ao serviço.

Diretrizes para o uso de referências automáticas de nós com o recurso de diretório base

Quando os compartilhamentos são configurados com a propriedade de compartilhamento do diretório base ativada, pode haver um ou mais caminhos de pesquisa do diretório base configurados para uma configuração do diretório base. Os caminhos de pesquisa podem apontar para volumes contidos em cada nó que contém volumes SVM. Os clientes recebem uma referência e, se um LIF de dados local ativo estiver disponível, se conectam através de um LIF referido que é local para o diretório home do usuário doméstico.

Há diretrizes quando clientes SMB 1,0 acessam diretórios base dinâmicos com referências automáticas de nós ativadas. Isso ocorre porque os clientes SMB 1,0 exigem a referência automática do nó antes de autenticarem, o que é antes que o servidor SMB tenha o nome do usuário. No entanto, o acesso ao diretório home SMB funciona corretamente para clientes SMB 1,0 se as seguintes instruções forem verdadeiras:

- Os diretórios home SMB são configurados para usar nomes simples, como "%W" (nome de usuário do Windows) ou "%u" (nome de usuário UNIX mapeado), e não nomes de estilo de nome de domínio, como "%d%W" (nome de domínio/nome de usuário).
- Ao criar compartilhamentos de diretório base, os nomes de compartilhamentos de diretório base CIFS são configurados com variáveis ("%W" ou "%u") e não com nomes estáticos, como "HOME".

Para clientes SMB 2.x e SMB 3,0, não há diretrizes especiais ao acessar diretórios base usando referências automáticas de nós.

Diretrizes para desabilitar referências automáticas de nós em servidores CIFS com conexões referidas existentes

Se você desativar as referências automáticas de nós depois que a opção tiver sido ativada, os clientes atualmente conectados a um LIF referido mantêm a conexão referida. Como o ONTAP usa referências DFS como o mecanismo para referências de nó automáticas SMB, os clientes podem até se reconectar ao LIF referido depois de desativar a opção até que a referência DFS armazenada em cache do cliente para a conexão referida expire. Isso é verdade mesmo no caso de uma reversão para uma versão do ONTAP que não suporta referências automáticas de nós. Os clientes continuam a usar referências até que o encaminhamento do DFS termine do cache do cliente.

A Autolocation usa referências de nó automáticas SMB para aumentar o desempenho do cliente SMB, referindo os clientes ao LIF no nó que possui o volume de dados de um SVM. Quando um cliente SMB se conecta a um compartilhamento SMB hospedado em um SVM, ele pode se conectar usando um LIF em um nó

que não possui os dados solicitados e usa a rede de interconexão de cluster para recuperar dados. O cliente pode ter tempos de resposta mais rápidos se a conexão SMB usar um LIF localizado no nó que contém os dados solicitados.

O ONTAP fornece essa funcionalidade usando referências do sistema de arquivos distribuídos da Microsoft (DFS) para informar os clientes SMB que um arquivo ou pasta solicitado no namespace está hospedado em outro lugar. Um nó faz uma referência quando determina que há um LIF SVM no nó que contém os dados. As referências são feitas com base na localização da raiz da partilha através da qual o cliente está ligado.

A referência ocorre durante a negociação SMB. A referência é feita antes da conexão ser estabelecida. Depois que o ONTAP refere o cliente SMB ao nó de destino, a conexão é feita e o cliente acessa os dados através do caminho LIF referido a partir desse ponto. Isso permite que os clientes tenham acesso mais rápido aos dados e evite a comunicação de cluster adicional.

Diretrizes para o uso de referências automáticas de nó com clientes Mac os

Os clientes Mac os X não suportam referências de nó automáticas SMB, mesmo que o Mac os suporte o sistema de arquivos distribuídos (DFS) da Microsoft. Os clientes Windows fazem uma solicitação de referência DFS antes de se conectar a um compartilhamento SMB. O ONTAP fornece uma referência a um LIF de dados encontrado no mesmo nó que hospeda os dados solicitados, o que leva a melhores tempos de resposta do cliente. Embora o Mac os suporte DFS, os clientes do Mac os não se comportam exatamente como os clientes do Windows nesta área.

Informações relacionadas

[Como o ONTAP ativa diretórios base dinâmicos](#)

["Gerenciamento de rede"](#)

["Ferramenta de Matriz de interoperabilidade do NetApp"](#)

Suporte para referências de nó automáticas SMB

Antes de ativar as referências de nó automático SMB, você deve estar ciente de que certas funcionalidades do ONTAP não suportam referências.

- Os seguintes tipos de volumes não suportam referências de nó automáticas SMB:
 - Membros somente leitura de um espelho de compartilhamento de carga
 - Volume de destino de um espelho de proteção de dados
- As referências de nó não se movem ao lado de uma movimentação de LIF.

Se um cliente estiver usando uma conexão referida por meio de uma conexão SMB 2.x ou SMB 3,0 e um LIF de dados se mover sem interrupções, o cliente continuará a usar a mesma conexão referida, mesmo que o LIF não seja mais local para os dados.

- As referências de nó não se movem ao lado de uma movimentação de volume.

Se um cliente estiver usando uma conexão referida em qualquer conexão SMB e ocorrer uma movimentação de volume, o cliente continuará a usar a mesma conexão referida, mesmo que o volume não esteja mais localizado no mesmo nó que o LIF de dados.

Ative ou desative referências de nó automáticas SMB

Você pode habilitar referências de nó automáticas SMB para aumentar o desempenho de acesso de cliente SMB. Você pode desativar referências automáticas de nós se não quiser que o ONTAP faça referências a clientes SMB.

Antes de começar

Um servidor CIFS deve ser configurado e executado na máquina virtual de storage (SVM).

Sobre esta tarefa

A funcionalidade de referências de nó automático SMB está desativada por predefinição. Você pode ativar ou desativar essa funcionalidade em cada SVM conforme necessário.

Esta opção está disponível no nível de privilégio avançado.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Ative ou desative referências de nó automáticas SMB conforme necessário:

Se você quiser que as referências de nó automático SMB sejam...	Digite o seguinte comando...
Ativado	<pre>vserver cifs options modify -vserver vserver_name -is-referral-enabled true</pre>
Desativado	<pre>vserver cifs options modify -vserver vserver_name -is-referral-enabled false</pre>

A configuração de opção entra em vigor para novas sessões SMB. Os clientes com conexão existente podem utilizar referência de nó somente quando o tempo limite de cache existente expirar.

3. Mudar para o nível de privilégio de administrador: `set -privilege admin`

Informações relacionadas

[Opções de servidor SMB disponíveis](#)

Use as estatísticas para monitorar a atividade automática de referência de nós

Para determinar quantas conexões SMB são referidas, você pode monitorar a atividade automática de referência de nó usando o `statistics` comando. Ao monitorar referências, você pode determinar em que medida as referências automáticas estão localizando conexões em nós que hospedam os compartilhamentos e se você deve redistribuir seus LIFs de dados para fornecer melhor acesso local aos compartilhamentos no servidor CIFS.

Sobre esta tarefa

O `cifs` objeto fornece vários contadores no nível de privilégio avançado que são úteis ao monitorar referências automáticas de nó SMB:

- `node_referral_issued`

Número de clientes que receberam uma referência para o nó da raiz de compartilhamento depois que o cliente se conectou usando um LIF hospedado por um nó diferente do nó da raiz de compartilhamento.

- `node_referral_local`

Número de clientes que se conectaram usando um LIF hospedado pelo mesmo nó que hospeda a raiz de compartilhamento. O acesso local geralmente proporciona um desempenho ideal.

- `node_referral_not_possible`

Número de clientes que não receberam uma referência para o nó que hospeda a raiz de compartilhamento depois de se conectar usando um LIF hospedado por um nó diferente do nó da raiz de compartilhamento. Isso ocorre porque um LIF de dados ativo para o nó da raiz de compartilhamento não foi encontrado.

- `node_referral_remote`

Número de clientes que se conectaram usando um LIF hospedado por um nó diferente do nó que hospeda a raiz de compartilhamento. O acesso remoto pode resultar em desempenho degradado.

Você pode monitorar as estatísticas automáticas de referência de nós na sua máquina virtual de storage (SVM) coletando e visualizando dados para um período de tempo específico (uma amostra). Você pode exibir dados da amostra se não parar a coleta de dados. Parar a coleta de dados dá-lhe uma amostra fixa. Não interromper a coleta de dados dá a você a capacidade de obter dados atualizados que você pode usar para comparar com consultas anteriores. A comparação pode ajudá-lo a identificar tendências de desempenho.



Para avaliar e usar as informações que você coleta a partir do `statistics` comando, você deve entender a distribuição de clientes em seus ambientes.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Visualize estatísticas automáticas de referência de nó usando o `statistics` comando.

Este exemplo exibe estatísticas automáticas de referência de nó coletando e visualizando dados para um período de tempo de amostragem:

- a. Inicie a coleção: `statistics start -object cifs -instance vs1 -sample-id sample1`

```
Statistics collection is being started for Sample-id: sample1
```

- b. Aguarde até que o tempo de recolha pretendido decorra.
- c. Parar a coleção: `statistics stop -sample-id sample1`

```
Statistics collection is being stopped for Sample-id: sample1
```

- d. Veja as estatísticas automáticas de referência de nó: `statistics show -sample-id sample1`

```
-counter node
```

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1
```

Counter	Value
node_name	node1
node_referral_issued	0
node_referral_local	1
node_referral_not_possible	2
node_referral_remote	2
...	
node_name	node2
node_referral_issued	2
node_referral_local	1
node_referral_not_possible	0
node_referral_remote	2
...	

A saída exibe contadores para todos os nós participantes do SVM VS1. Para maior clareza, apenas os campos de saída relacionados às estatísticas automáticas de referência de nó são fornecidos no exemplo.

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Informações relacionadas

[Exibindo estatísticas](#)

["Configuração do monitoramento de desempenho"](#)

Monitore informações de referência automática de nós SMB no lado do cliente usando um cliente Windows

Para determinar quais referências são feitas da perspectiva do cliente, você pode usar o utilitário Windows `dfsutil.exe`.

O kit RSAT (Remote Server Administration Tools) disponível com o Windows 7 e clientes posteriores contém o `dfsutil.exe` utilitário. Usando este utilitário, você pode exibir informações sobre o conteúdo do cache de referência, bem como visualizar informações sobre cada referência que o cliente está usando atualmente. Você também pode usar o utilitário para limpar o cache de referência do cliente. Para obter mais informações, consulte a Microsoft TechNet Library.

Informações relacionadas

Forneça segurança de pastas em compartilhamentos com enumeração baseada em acesso

Forneça segurança de pastas em compartilhamentos com visão geral de enumeração baseada em acesso

Quando a enumeração baseada em acesso (ABE) está ativada em um compartilhamento SMB, os usuários que não têm permissão para acessar uma pasta ou arquivo contido no compartilhamento (seja por restrições de permissão individuais ou de grupo) não veem esse recurso compartilhado exibido em seu ambiente, embora o próprio compartilhamento permaneça visível.

As propriedades de compartilhamento convencionais permitem especificar quais usuários (individualmente ou em grupos) têm permissão para exibir ou modificar arquivos ou pastas contidos no compartilhamento. No entanto, eles não permitem que você controle se pastas ou arquivos dentro do compartilhamento são visíveis para usuários que não têm permissão para acessá-los. Isso pode causar problemas se os nomes dessas pastas ou arquivos dentro do compartilhamento descreverem informações confidenciais, como os nomes de clientes ou produtos em desenvolvimento.

A enumeração baseada em acesso (ABE) estende as propriedades de compartilhamento para incluir a enumeração de arquivos e pastas dentro do compartilhamento. Portanto, O ABE permite filtrar a exibição de arquivos e pastas dentro do compartilhamento com base nos direitos de acesso do usuário. Ou seja, o compartilhamento em si seria visível para todos os usuários, mas os arquivos e pastas dentro do compartilhamento poderiam ser exibidos ou ocultados de usuários designados. Além de proteger informações confidenciais em seu local de trabalho, o ABE permite simplificar a exibição de grandes estruturas de diretórios para benefício dos usuários que não precisam acessar toda a sua gama de conteúdo. Por exemplo, o compartilhamento em si seria visível para todos os usuários, mas arquivos e pastas dentro do compartilhamento poderiam ser exibidos ou ocultos.

Saiba mais "[Impacto no desempenho ao usar enumeração baseada em acesso SMB/CIFS](#)" sobre .

Ative ou desative a enumeração baseada em acesso em compartilhamentos SMB

Você pode ativar ou desativar a enumeração baseada em acesso (ABE) em compartilhamentos SMB para permitir ou impedir que os usuários vejam recursos compartilhados que eles não têm permissão para acessar.

Sobre esta tarefa

Por padrão, o ABE está desativado.

Passos

1. Execute uma das seguintes ações:

Se você quiser...	Digite o comando...
Ative o ABE em um novo compartilhamento	<pre>vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access- based-enumeration</pre> <p>Você pode especificar configurações de compartilhamento opcionais adicionais e propriedades de compartilhamento adicionais ao criar um compartilhamento SMB. Para obter mais informações, consulte a página man para o <code>vserver cifs share create</code> comando.</p>
Ative o ABE em um compartilhamento existente	<pre>vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access- based-enumeration</pre> <p>As propriedades de compartilhamento existentes são preservadas. A propriedade ABE Share é adicionada à lista existente de propriedades de ações.</p>
Desative o ABE em um compartilhamento existente	<pre>vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access- based-enumeration</pre> <p>Outras propriedades de compartilhamento são preservadas. Somente a propriedade ABE Share é removida da lista de propriedades de compartilhamento.</p>

2. Verifique se a configuração de compartilhamento está correta usando o `vserver cifs share show` comando.

Exemplos

O exemplo a seguir cria um compartilhamento ABE SMB chamado "vendas" com um caminho de `/sales` no SVM VS1. A ação é criada com `access-based-enumeration` como uma propriedade de ação:

```

cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path
/sales -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

          Vserver: vs1
          Share: sales
CIFS Server NetBIOS Name: VS1
          Path: /sales
    Share Properties: access-based-enumeration
                    oplocks
                    browsable
                    changenotify
    Symlink Properties: enable
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
          Share Comment: -
          Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
          Volume Name: -
          Offline Files: manual
Vscan File-Operations Profile: standard

```

O exemplo a seguir adiciona a `access-based-enumeration` propriedade share a um compartilhamento SMB chamado "ata2":

```

cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
-----
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration

```

Informações relacionadas

[Adicionar ou remover propriedades de compartilhamento em um compartilhamento SMB existente](#)

Ativar ou desativar a enumeração baseada em acesso a partir de um cliente Windows

Você pode ativar ou desativar a enumeração baseada em acesso (ABE) em compartilhamentos SMB de um cliente Windows, o que permite configurar essa

configuração de compartilhamento sem precisar se conectar ao servidor CIFS.



O `abecmd` utilitário não está disponível em novas versões dos clientes Windows Server e Windows. Foi lançado como parte do Windows Server 2008. O suporte terminou para o Windows Server 2008 em 14 de janeiro de 2020.

Passos

1. Em um cliente Windows que suporte ABE, digite o seguinte comando: `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

Para obter mais informações sobre o `abecmd` comando, consulte a documentação do cliente Windows.

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 INTERRUPTÃO 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.