



Gerencie SMB com a CLI

ONTAP 9

NetApp
January 17, 2025

Índice

Gerencie SMB com a CLI	1
Visão geral da SMB	1
Suporte ao servidor SMB	1
Gerenciar servidores SMB	9
Configure o acesso a arquivos usando SMB	109
Gerencie o acesso a arquivos usando SMB	178
Implantar serviços baseados em cliente SMB	271
Implante serviços baseados em servidor SMB	286
Dependências de nomes de arquivos e diretórios NFS e SMB	357

Gerencie SMB com a CLI

Visão geral da SMB

Os recursos de acesso a arquivos ONTAP estão disponíveis para o protocolo SMB. Você pode habilitar um servidor CIFS, criar compartilhamentos e ativar serviços Microsoft.



SMB (bloco de mensagens de servidor) refere-se aos dialetos modernos do protocolo Common Internet File System (CIFS). Você ainda verá *CIFS* na interface de linha de comando (CLI) do ONTAP e nas ferramentas de gerenciamento do OnCommand.

Suporte ao servidor SMB

Visão geral do suporte ao servidor SMB

Você pode ativar e configurar servidores SMB em máquinas virtuais de armazenamento (SVMs) para permitir que os clientes SMB acessem arquivos no cluster.

- Cada SVM de dados no cluster pode ser vinculado a exatamente um domínio do active Directory.
- Os SVMs de dados não precisam estar vinculados ao mesmo domínio.
- Vários SVMs podem ser vinculados ao mesmo domínio.

Você deve configurar as SVMs e LIFs que você está usando para fornecer dados antes de criar um servidor SMB. Se sua rede de dados não for plana, talvez você também precise configurar IPspaces, domínios de broadcast e sub-redes.

Informações relacionadas

["Gerenciamento de rede"](#)

[Modificar servidores SMB](#)

["Administração do sistema"](#)

Versões e funcionalidade SMB compatíveis

O bloco de mensagens de servidor (SMB) é um protocolo de compartilhamento remoto de arquivos usado por clientes e servidores Microsoft Windows. No ONTAP 9, todas as versões SMB são suportadas; no entanto, o suporte padrão ao SMB 1,0 depende da versão do ONTAP. Você deve verificar se o servidor SMB do ONTAP suporta os clientes e a funcionalidade necessária no seu ambiente.

As informações mais recentes sobre quais clientes SMB e controladores de domínio o ONTAP suporta estão disponíveis na *ferramenta Matriz de interoperabilidade*.

O SMB 2,0 e versões posteriores são ativados por padrão para servidores SMB do ONTAP 9 e podem ser ativados ou desativados conforme necessário. A tabela a seguir mostra o suporte ao SMB 1,0 e a configuração padrão.

Funcionalidade SMB 1,0:	Nestes lançamentos do ONTAP 9:			
	9,0	9,1	9,2	9,3 e mais tarde
Está ativado por predefinição	Sim	Sim	Sim	Não
Pode ser ativado ou desativado	Não	Sim * 9,1 P8 ou posterior necessário.	Sim	Sim



As configurações padrão para conexões SMB 1,0 e 2,0 para controladores de domínio também dependem da versão do ONTAP. Mais informações estão disponíveis na `vserver cifs security modify` página de manual. Para ambientes com servidores CIFS existentes que executam o SMB 1,0, você deve migrar para uma versão SMB posterior o mais rápido possível para se preparar para melhorias de segurança e conformidade. Contacte o seu representante da NetApp para obter mais informações.

A tabela a seguir mostra quais recursos SMB são suportados em cada versão SMB. Algumas funcionalidades SMB estão ativadas por predefinição e algumas requerem uma configuração adicional.

Esta funcionalidade e:	Requer habilitação:	É suportado no ONTAP 9 para estas versões SMB:				
		1,0	2,0	2,1	3,0	3.1.1
Funcionalidade e SMB 1,0 legada		X	X	X	X	X
Alças duráveis			X	X	X	X
Operações combinadas			X	X	X	X
Operações assíncronas			X	X	X	X
Tamanhos aumentados do buffer de leitura e gravação			X	X	X	X
Maior escalabilidade			X	X	X	X

Esta funcionalidade:	Requer habilitação:	É suportado no ONTAP 9 para estas versões SMB:				
Assinatura SMB	X	X	X	X	X	X
Formato de arquivo de fluxo de dados alternativo (ADS)	X	X	X	X	X	X
MTU grande (ativada por predefinição a partir de ONTAP 9.7)	X			X	X	X
Calços de leasing				X	X	X
Compartilhamentos disponíveis continuamente	X				X	X
Alças persistentes					X	X
Testemunha					X	X
CRIPTOGRAFIA SMB: AES-128-CCM	X				X	X
Escalabilidade e horizontal (exigida pelos compartilhamentos da CA)					X	X
Failover transparente					X	X

Esta funcionalidade:	Requer habilitação:	É suportado no ONTAP 9 para estas versões SMB:				
Multicanal SMB (começando com ONTAP 9.4)	X				X	X
Integridade de pré-autenticação						X
Failover de cliente de cluster v,2 (CCFv2)						X
Criptografia SMB: AES-128-GCM (começando com ONTAP 9.1)	X					X

Informações relacionadas

[Utilizar a assinatura SMB para melhorar a segurança da rede](#)

[Definir o nível mínimo de segurança de autenticação do servidor SMB](#)

[Configuração da criptografia SMB necessária em servidores SMB para transferências de dados por SMB](#)

["Interoperabilidade do NetApp"](#)

Recursos do Windows não suportados

Antes de usar o CIFS na rede, você precisa estar ciente de certos recursos do Windows que o ONTAP não oferece suporte.

O ONTAP não suporta os seguintes recursos do Windows:

- Sistema de arquivos criptografados (EFS)
- Registo de eventos do NT File System (NTFS) no diário de alterações
- Microsoft File Replication Service (FRS)
- Serviço de Indexação do Microsoft Windows
- Armazenamento remoto por meio do HSM (Hierarchical Storage Management)
- Gerenciamento de cotas de clientes Windows
- Semântica de cota do Windows

- O arquivo LMHOSTS
- Compactação nativa NTFS

Configure os serviços de nomes NIS ou LDAP no SVM

Com o acesso SMB, o mapeamento do usuário para um usuário UNIX é sempre realizado, mesmo quando você acessa dados em um volume de estilo de segurança NTFS. Se você mapear usuários do Windows para usuários UNIX correspondentes cujas informações são armazenadas em armazenamentos de diretório NIS ou LDAP ou se você usar LDAP para mapeamento de nomes, configure esses serviços de nomes durante a configuração SMB.

Antes de começar

Você precisa ter personalizado a configuração do banco de dados dos serviços de nomes para corresponder à infraestrutura do serviço de nomes.

Sobre esta tarefa

Os SVMs usam os bancos de dados ns-switch de serviços de nome para determinar a ordem na qual procurar as fontes para um determinado banco de dados de serviço de nome. A fonte ns-switch pode ser qualquer combinação de `files`, `nis`, ou `ldap`. Para o banco de dados de grupos, o ONTAP tenta obter as associações de grupos de todas as fontes configuradas e, em seguida, usa as informações de associação de grupo consolidado para verificações de acesso. Se uma dessas fontes não estiver disponível no momento da obtenção de informações do grupo UNIX, o ONTAP não poderá obter as credenciais UNIX completas e as verificações de acesso subsequentes poderão falhar. Portanto, você deve sempre verificar se todas as fontes do ns-switch estão configuradas para o banco de dados de grupo nas configurações do ns-switch.

O padrão é fazer com que o servidor SMB mapeie todos os usuários do Windows para o usuário UNIX padrão armazenado no banco de dados local `passwd`. Se você quiser usar a configuração padrão, a configuração de serviços de nome de usuário e grupo NIS ou LDAP UNIX ou mapeamento de usuário LDAP é opcional para o acesso SMB.

Passos

1. Se as informações de usuário, grupo e netgroup UNIX forem gerenciadas por serviços de nome NIS, configure os serviços de nome NIS:
 - a. Determine a ordem atual dos serviços de nome usando o `vserver services name-service ns-switch show` comando.

Neste exemplo, os três bancos de dados (`group`, `passwd` e `netgroup`) que podem ser usados `nis` como uma fonte de serviço de nomes estão usando `files` apenas como uma fonte.

```
vserver services name-service ns-switch show -vserver vs1
```

Vserver	Database	Enabled	Source Order
vs1	hosts	true	dns, files
vs1	group	true	files
vs1	passwd	true	files
vs1	netgroup	true	files
vs1	namemap	true	files

Você deve adicionar a `nis` fonte `group` aos bancos de dados e `passwd`, opcionalmente, ao `netgroup` banco de dados.

- b. Ajuste a ordenação do banco de dados `ns-switch` do serviço de nomes conforme desejado usando o `vserver services name-service ns-switch modify` comando.

Para obter a melhor performance, você não deve adicionar um serviço de nomes a um banco de dados de serviços de nomes, a menos que se Planeje configurar esse serviço de nomes no SVM.

Se você modificar a configuração para mais de um banco de dados de serviço de nome, deverá executar o comando separadamente para cada banco de dados de serviço de nome que deseja modificar.

Neste exemplo, `nis` e `files` são configurados como fontes para os `group` bancos de dados e `passwd`, nessa ordem. O restante dos bancos de dados do serviço de nomes não foi alterado.

```
vserver services name-service ns-switch modify -vserver vs1 -database group
-vsources nis,files vserver services name-service ns-switch modify -vserver
vs1 -database passwd -sources nis,files
```

- c. Verifique se a ordem dos serviços de nome está correta usando o `vserver services name-service ns-switch show` comando.

```
vserver services name-service ns-switch show -vserver vs1
```

Vserver	Database	Enabled	Source Order
vs1	hosts	true	dns, files
vs1	group	true	nis, files
vs1	passwd	true	nis, files
vs1	netgroup	true	files
vs1	namemap	true	files

- d. Crie a configuração do serviço de nomes NIS `vserver services name-service nis-domain create -vserver <vserver_name> -domain <NIS_domain_name> -servers <NIS_server_IPaddress>,...`

```
vserver services name-service nis-domain create -vserver vs1 -domain example.com -servers 10.0.0.60
```



A partir de ONTAP 9.2, o campo `-nis-servers` substitui o `-servers` campo. Este novo campo pode ter um nome de host ou um endereço IP para o servidor NIS.

- e. Verifique se o serviço de nomes NIS está configurado corretamente: `vserver services name-service nis-domain show vserver <vserver_name>`

```
vserver services name-service nis-domain show vserver vs1
```

Vserver	Domain	Server
vs1	example.com	10.0.0.60

2. Se as informações de usuário, grupo e netgroup UNIX ou mapeamento de nomes for gerenciado por serviços de nomes LDAP, configure os serviços de nomes LDAP usando as informações localizadas ["Gerenciamento de NFS"](#).

Como funciona a configuração do switch do serviço de nomes ONTAP

O ONTAP armazena informações de configuração do serviço de nomes em uma tabela equivalente `/etc/nsswitch.conf` ao arquivo em sistemas UNIX. Você deve entender a função da tabela e como o ONTAP a usa para que você possa configurá-la adequadamente para o seu ambiente.

A tabela de switch de serviço de nome do ONTAP determina quais fontes de serviço de nome o ONTAP consulta para obter informações para um determinado tipo de informações de serviço de nome. O ONTAP mantém uma tabela de switch de serviço de nomes separada para cada SVM.

Tipos de banco de dados

A tabela armazena uma lista de serviços de nomes separada para cada um dos seguintes tipos de banco de dados:

Tipo de banco de dados	Define fontes de serviço de nome para...	Fontes válidas são...
hosts	Conversão de nomes de host para endereços IP	ficheiros, dns
grupo	Procurar informações do grupo de utilizadores	arquivos, nis, ldap

Tipo de banco de dados	Define fontes de serviço de nome para...	Fontes válidas são...
passwd	Procurar informações do utilizador	arquivos, nis, ldap
grupo de rede	Procurar informações do netgroup	arquivos, nis, ldap
namemap	Mapeando nomes de usuários	ficheiros, ldap

Tipos de origem

As fontes especificam qual fonte de serviço de nomes usar para recuperar as informações apropriadas.

Especificar tipo de origem...	Para procurar informações em...	Gerenciado pelas famílias de comando...
ficheiros	Arquivos de origem local	<pre>vserver services name- service unix-user vserver services name-service unix-group vserver services name- service netgroup vserver services name- service dns hosts</pre>
nis	Servidores NIS externos, conforme especificado na configuração do domínio NIS da SVM	<pre>vserver services name- service nis-domain</pre>
ldap	Servidores LDAP externos, conforme especificado na configuração de cliente LDAP do SVM	<pre>vserver services name- service ldap</pre>
dns	Servidores DNS externos conforme especificado na configuração DNS do SVM	<pre>vserver services name- service dns</pre>

Mesmo que você Planeje usar NIS ou LDAP para acesso a dados e autenticação de administração SVM, você ainda deve incluir `files` e configurar usuários locais como um fallback caso a autenticação NIS ou LDAP falhe.

Protocolos usados para acessar fontes externas

Para acessar os servidores para fontes externas, o ONTAP usa os seguintes protocolos:

Fonte do serviço de nomes externo	Protocolo utilizado para acesso
NIS	UDP
DNS	UDP
LDAP	TCP

Exemplo

O exemplo a seguir exibe a configuração do switch de serviço de nomes para o SVM `svm_1`:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
Source
Vserver      Database      Order
-----
svm_1        hosts         files,
              dns
svm_1        group         files
svm_1        passwd        files
svm_1        netgroup      nis,
              files
```

Para procurar informações de usuários ou grupos, o ONTAP consulta apenas arquivos de fontes locais. Se a consulta não retornar nenhum resultado, a pesquisa falhará.

Para procurar informações de netgroup, o ONTAP primeiro consulta servidores NIS externos. Se a consulta não retornar nenhum resultado, o arquivo netgroup local será marcado em seguida.

Não há entradas de serviço de nomes para o mapeamento de nomes na tabela para o SVM `svm_1`. Portanto, o ONTAP consulta apenas arquivos de origem local por padrão.

Gerenciar servidores SMB

Modificar servidores SMB

Pode mover um servidor SMB de um grupo de trabalho para um domínio do Active Directory, de um grupo de trabalho para outro grupo de trabalho ou de um domínio do Active Directory para um grupo de trabalho utilizando o `vserver cifs modify` comando.

Sobre esta tarefa

Você também pode modificar outros atributos do servidor SMB, como o nome do servidor SMB e o status administrativo. Consulte a página de manual para obter detalhes.

Opções

- Mova o servidor SMB de um grupo de trabalho para um domínio do Active Directory:
 - a. Defina o status administrativo do servidor SMB como `down`.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. Mova o servidor SMB do grupo de trabalho para um domínio do ativo Directory: `vserver cifs modify -vserver vserver_name -domain domain_name`

```
Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
```

Para criar uma conta de máquina do ativo Directory para o servidor SMB, você deve fornecer o nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores ao `ou=example` ou contentor dentro do `example` domínio `.com`.

A partir do ONTAP 9.7, o administrador do AD pode fornecer um URI para um arquivo keytab como alternativa para fornecer um nome e uma senha para uma conta privilegiada do Windows. Quando receber o URI, inclua-o `-keytab-uri` no parâmetro com os `vserver cifs` comandos.

- Mover o servidor SMB de um grupo de trabalho para outro grupo de trabalho:
 - a. Defina o status administrativo do servidor SMB como `down`.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. Modifique o grupo de trabalho para o servidor SMB: `vserver cifs modify -vserver vserver_name -workgroup new_workgroup_name`

```
Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
```

- Mova o servidor SMB de um domínio do ativo Directory para um grupo de trabalho:
 - a. Defina o status administrativo do servidor SMB como `down`.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. Mova o servidor SMB do domínio do ativo Directory para um grupo de trabalho: `vserver cifs modify -vserver vserver_name -workgroup workgroup_name`

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```



Para entrar no modo de grupo de trabalho, todos os recursos baseados em domínio devem ser desativados e suas configurações removidas automaticamente pelo sistema, incluindo compartilhamentos continuamente disponíveis, cópias de sombra e AES. No entanto, as ACLs de compartilhamento configuradas por domínio, como "EXAMPLE.COM\userName", não funcionarão corretamente, mas não poderão ser removidas pelo ONTAP. Remova essas ACLs de compartilhamento o mais rápido possível usando ferramentas externas após a conclusão do comando. Se o AES estiver ativado, você poderá ser solicitado a fornecer o nome e a senha de uma conta do Windows com Privileges suficiente para desativá-lo no domínio "example.com".

- Modifique outros atributos usando o parâmetro apropriado do `vserver cifs modify` comando.

Use as opções para personalizar servidores SMB

Opções de servidor SMB disponíveis

É útil saber quais opções estão disponíveis ao considerar como personalizar o servidor SMB. Embora algumas opções sejam para uso geral no servidor SMB, várias são usadas para ativar e configurar a funcionalidade SMB específica. As opções de servidor SMB são controladas com a `vserver cifs options modify` opção.

A lista a seguir especifica as opções do servidor SMB que estão disponíveis no nível de privilégio de administrador:

- **Configurando o valor de tempo limite da sessão SMB**

Configurar esta opção permite especificar o número de segundos de tempo ocioso antes de uma sessão SMB ser desconectada. Uma sessão ociosa é uma sessão na qual um usuário não tem arquivos ou diretórios abertos no cliente. O valor padrão é de 900 segundos.

- **Configurando o usuário UNIX padrão**

Configurar esta opção permite especificar o utilizador UNIX predefinido que o servidor SMB utiliza. O ONTAP cria automaticamente um usuário padrão chamado "pcuser" (com um UID de 65534), cria um grupo chamado "pcuser" (com um GID de 65534) e adiciona o usuário padrão ao grupo "pcuser". Quando você cria um servidor SMB, o ONTAP configura automaticamente "pcuser" como o usuário UNIX padrão.

- **Configurando o usuário UNIX convidado**

A configuração desta opção permite especificar o nome de um usuário UNIX ao qual os usuários que fazem login de domínios não confiáveis são mapeados, o que permite que um usuário de um domínio não confiável se conecte ao servidor SMB. Por padrão, essa opção não está configurada (não há valor padrão); portanto, o padrão é não permitir que usuários de domínios não confiáveis se conectem ao servidor SMB.

- * Ativar ou desativar a execução de concessão de leitura para bits de modo*

Ativar ou desativar esta opção permite que você especifique se deseja permitir que clientes SMB executem arquivos executáveis com bits de modo UNIX aos quais eles têm acesso de leitura, mesmo quando o bit executável UNIX não está definido. Esta opção está desativada por predefinição.

- **Ativar ou desativar a capacidade de eliminar ficheiros só de leitura de clientes NFS**

Ativar ou desativar esta opção determina se os clientes NFS devem excluir arquivos ou pastas com o conjunto de atributos somente leitura. A semântica de exclusão NTFS não permite a exclusão de um arquivo ou pasta quando o atributo somente leitura é definido. A semântica de exclusão do UNIX ignora o bit somente leitura, usando as permissões do diretório pai para determinar se um arquivo ou pasta pode ser excluído. A configuração padrão é `disabled`, o que resulta em semântica de exclusão NTFS.

- **Configurando endereços de servidor do Windows Internet Name Service**

Configurar esta opção permite especificar uma lista de endereços de servidor WINS (Serviço de nomes de Internet do Windows) como uma lista delimitada por vírgulas. Você deve especificar endereços IPv4. Os endereços IPv6 não são suportados. Não há valor padrão.

A lista a seguir especifica as opções do servidor SMB que estão disponíveis no nível avançado de privilégio:

- **Concessão de permissões de grupo UNIX para usuários CIFS**

Configurar esta opção determina se o usuário CIFS de entrada que não é o proprietário do arquivo pode receber a permissão de grupo. Se o usuário CIFS não for o proprietário do arquivo de estilo de segurança UNIX e esse parâmetro estiver definido como `true`, a permissão de grupo será concedida para o arquivo. Se o usuário CIFS não for o proprietário do arquivo de estilo de segurança UNIX e esse parâmetro estiver definido como `false`, as regras UNIX normais serão aplicáveis para conceder a permissão de arquivo. Este parâmetro é aplicável a arquivos de estilo de segurança UNIX que têm permissão definida como `mode bits` e não é aplicável a arquivos com o modo de segurança NTFS ou NFSv4. A predefinição é `false`.

- **Ativar ou desativar o SMB 1,0**

O SMB 1,0 é desativado por padrão em uma SVM para a qual um servidor SMB é criado no ONTAP 9.3.



A partir do ONTAP 9.3, o SMB 1,0 é desativado por padrão para novos servidores SMB criados no ONTAP 9.3. Você deve migrar para uma versão SMB mais recente o mais rápido possível para se preparar para melhorias de segurança e conformidade. Contacte o seu representante da NetApp para obter mais informações.

- **Ativar ou desativar o SMB 2.x**

SMB 2,0 é a versão mínima de SMB que suporta failover de LIF. Se desativar o SMB 2.x, o ONTAP também desativa automaticamente o SMB 3.X.

O SMB 2,0 é compatível apenas com SVMs. A opção é ativada por padrão em SVMs

- **Ativar ou desativar o SMB 3,0**

O SMB 3,0 é a versão mínima para SMB compatível com compartilhamentos disponíveis continuamente. O Windows Server 2012 e o Windows 8 são as versões mínimas do Windows que suportam SMB 3,0.

O SMB 3,0 é compatível apenas com SVMs. A opção é ativada por padrão em SVMs

- **Ativar ou desativar o SMB 3,1**

O Windows 10 é a única versão do Windows que suporta SMB 3,1.

O SMB 3,1 é compatível apenas com SVMs. A opção é ativada por padrão em SVMs

- * Ativar ou desativar a descarga de cópia ODX*

O descarregamento de cópia ODX é usado automaticamente por clientes Windows que o suportam. Esta opção está ativada por predefinição.

- * Ativar ou desativar o mecanismo de cópia direta para descarga de cópia ODX*

O mecanismo de cópia direta aumenta o desempenho da operação de descarga de cópia quando os clientes do Windows tentam abrir o arquivo de origem de uma cópia em um modo que impede que o arquivo seja alterado enquanto a cópia está em andamento. Por padrão, o mecanismo de cópia direta está ativado.

- * Ativar ou desativar referências automáticas de nós*

Com referências automáticas de nós, o servidor SMB refere automaticamente os clientes a um data LIF local para o nó que hospeda os dados acessados através do compartilhamento solicitado.

- **Ativar ou desativar políticas de exportação para SMB**

Esta opção está desativada por predefinição.

- * Ativar ou desativar usando pontos de junção como pontos de reparação*

Se esta opção estiver ativada, o servidor SMB expõe pontos de junção para clientes SMB como pontos de reparação. Esta opção é válida apenas para ligações SMB 2.x ou SMB 3.0. Esta opção está ativada por predefinição.

Esta opção é suportada apenas em SVMs. A opção é ativada por padrão em SVMs

- **Configurando o número máximo de operações simultâneas por conexão TCP**

O valor padrão é 255.

- **Ativar ou desativar a funcionalidade de grupos e utilizadores locais do Windows**

Esta opção está ativada por predefinição.

- **Ativar ou desativar a autenticação de utilizadores locais do Windows**

Esta opção está ativada por predefinição.

- * Ativar ou desativar a funcionalidade de cópia de sombra VSS*

O ONTAP usa a funcionalidade de cópia de sombra para executar backups remotos de dados armazenados usando a solução Hyper-V sobre SMB.

Esta opção é suportada apenas em SVMs e apenas para configurações Hyper-V em SMB. A opção é ativada por padrão em SVMs

- **Configurando a profundidade do diretório de cópia de sombra**

A configuração desta opção permite definir a profundidade máxima dos diretórios para criar cópias de sombra ao usar a funcionalidade de cópia de sombra.

Esta opção é suportada apenas em SVMs e apenas para configurações Hyper-V em SMB. A opção é ativada por padrão em SVMs

- * Ativar ou desativar recursos de pesquisa de vários domínios para mapeamento de nomes*

Se ativado, quando um usuário UNIX é mapeado para um usuário de domínio do Windows usando um curinga (*) na parte de domínio do nome de usuário do Windows (por exemplo, * / joe), o ONTAP procura o usuário especificado em todos os domínios com confiança bidirecional para o domínio doméstico. O domínio inicial é o domínio que contém a conta de computador do servidor SMB.

Como alternativa à pesquisa de todos os domínios bidirecionalmente confiáveis, você pode configurar uma lista de domínios confiáveis preferenciais. Se esta opção estiver ativada e uma lista de preferências estiver configurada, a lista de preferências será utilizada para efetuar pesquisas de mapeamento de nomes de vários domínios.

O padrão é habilitar pesquisas de mapeamento de nomes de vários domínios.

- **Configurando o tamanho do setor do sistema de arquivos**

A configuração desta opção permite configurar o tamanho do setor do sistema de arquivos em bytes que o ONTAP reporta para clientes SMB. Existem dois valores válidos para esta opção: 4096 E 512. O valor padrão é 4096. Talvez seja necessário definir esse valor 512 se o aplicativo Windows suportar apenas um tamanho de setor de 512 bytes.

- **Ativar ou desativar o controle de Acesso Dinâmico**

Ativar esta opção permite proteger objetos no servidor SMB utilizando o controle de Acesso Dinâmico (DAC), incluindo a utilização de auditoria para encenar políticas de acesso centrais e utilizar objetos de Diretiva de Grupo para implementar políticas de acesso centrais. A opção está desativada por predefinição.

Esta opção é suportada apenas em SVMs.

- * Definir as restrições de acesso para sessões não autenticadas (restringir anônimo)*

Definir esta opção determina quais são as restrições de acesso para sessões não autenticadas. As restrições são aplicadas a usuários anônimos. Por padrão, não há restrições de acesso para usuários anônimos.

- * Ativar ou desativar a apresentação de ACLs NTFS em volumes com segurança eficaz UNIX (volumes estilo de segurança UNIX ou volumes mistos estilo de segurança com segurança eficaz UNIX)*

Ativar ou desativar esta opção determina como a segurança de arquivos em arquivos e pastas com segurança UNIX é apresentada aos clientes SMB. Se ativado, o ONTAP apresenta arquivos e pastas em volumes com segurança UNIX para clientes SMB como tendo segurança de arquivos NTFS com ACLs NTFS. Se desativado, o ONTAP apresenta volumes com segurança UNIX como volumes FAT, sem segurança de arquivos. Por padrão, os volumes são apresentados como tendo segurança de arquivos NTFS com ACLs NTFS.

- * Habilitando ou desativando a funcionalidade de abertura falsa do SMB*

A ativação dessa funcionalidade melhora o desempenho do SMB 2.x e do SMB 3,0, otimizando como o ONTAP faz solicitações abertas e fechadas ao consultar informações de atributos em arquivos e diretórios. Por padrão, a funcionalidade de abertura falsa do SMB está ativada. Essa opção é útil somente para conexões feitas com SMB 2.x ou posterior.

- * Ativar ou desativar as extensões UNIX*

Ativar esta opção ativa extensões UNIX num servidor SMB. As extensões UNIX permitem que a segurança de estilo POSIX/UNIX seja exibida através do protocolo SMB. Por predefinição, esta opção está desativada.

Se você tiver clientes SMB baseados em UNIX, como clientes Mac OSX, em seu ambiente, você deve habilitar extensões UNIX. A habilitação de extensões UNIX permite que o servidor SMB transmita informações de segurança POSIX/UNIX sobre SMB para o cliente baseado em UNIX, o que converte as informações de segurança em segurança POSIX/UNIX.

- * Ativar ou desativar o suporte para pesquisas de nomes curtos*

Ativar esta opção permite que o servidor SMB realize pesquisas em nomes curtos. Uma consulta de pesquisa com esta opção ativada tenta corresponder a nomes de arquivo 8,3 juntamente com nomes de arquivo longos. O valor padrão para este parâmetro é `false`.

- * Ativar ou desativar o suporte para publicidade automática de capacidades DFS*

Ativar ou desativar esta opção determina se os servidores SMB anunciam automaticamente os recursos DFS para clientes SMB 2.x e SMB 3,0 que se conectam a compartilhamentos. O ONTAP usa referências DFS na implementação de links simbólicos para acesso SMB. Se ativado, o servidor SMB sempre anuncia recursos DFS, independentemente de o acesso a links simbólicos estar habilitado. Se estiver desativado, o servidor SMB anunciará os recursos DFS somente quando os clientes se conectarem a compartilhamentos onde o acesso ao link simbólico está habilitado.

- **Configurando o número máximo de créditos SMB**

A partir do ONTAP 9.4, a configuração da `-max-credits` opção permite limitar o número de créditos a serem concedidos em uma conexão SMB quando clientes e servidor estão executando o SMB versão 2 ou posterior. O valor padrão é 128.

- * Ativar ou desativar o suporte para SMB Multichannel*

Ativar a `-is-multichannel-enabled` opção no ONTAP 9.4 e versões posteriores permite que o servidor SMB estabeleça várias conexões para uma única sessão SMB quando as NICs apropriadas são implantadas no cluster e em seus clientes. Isso melhora a taxa de transferência e a tolerância a falhas. O valor padrão para este parâmetro é `false`.

Quando o Multichannel SMB está ativado, você também pode especificar os seguintes parâmetros:

- O número máximo de conexões permitido por sessão multicanal. O valor padrão para este parâmetro é 32.
- O número máximo de interfaces de rede anunciadas por sessão multicanal. O valor padrão para este parâmetro é 256.

Configurando opções de servidor SMB

Você pode configurar as opções de servidor SMB a qualquer momento depois de criar um servidor SMB em uma máquina virtual de storage (SVM).

Passo

1. Execute a ação desejada:

Se pretender configurar as opções do servidor SMB...	Digite o comando...
No nível de privilégios de administrador	<code>vserver cifs options modify -vserver vserver_name options</code>
Em nível avançado de privilégios	<ul style="list-style-type: none"> a. <code>set -privilege advanced</code> b. <code>vserver cifs options modify -vserver vserver_name options</code> c. <code>set -privilege admin</code>

Para obter mais informações sobre como configurar as opções do servidor SMB, consulte a página de manual do `vserver cifs options modify` comando.

Configure a permissão Grant UNIX group para usuários SMB

Você pode configurar essa opção para conceder permissões de grupo para acessar arquivos ou diretórios, mesmo que o usuário SMB de entrada não seja o proprietário do arquivo.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Configure a permissão Grant UNIX group conforme apropriado:

Se você quiser	Introduza o comando
Ative o acesso aos arquivos ou diretórios para obter permissões de grupo, mesmo que o usuário não seja o proprietário do arquivo	<code>vserver cifs options modify -grant-unix-group-perms-to-others true</code>
Desative o acesso aos arquivos ou diretórios para obter permissões de grupo, mesmo que o usuário não seja o proprietário do arquivo	<code>vserver cifs options modify -grant-unix-group-perms-to-others false</code>

3. Verifique se a opção está definida para o valor desejado: `vserver cifs options show -fields grant-unix-group-perms-to-others`
4. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Configurar restrições de acesso para usuários anônimos

Por padrão, um usuário anônimo e não autenticado (também conhecido como *null user*) pode acessar certas informações na rede. Você pode usar uma opção de servidor SMB para configurar restrições de acesso para o usuário anônimo.

Sobre esta tarefa

A `-restrict-anonymous` opção servidor SMB corresponde à `RestrictAnonymous` entrada do Registro

no Windows.

Os usuários anônimos podem listar ou enumerar certos tipos de informações de sistema de hosts do Windows na rede, incluindo nomes e detalhes de usuários, políticas de conta e nomes de compartilhamento. Você pode controlar o acesso para o usuário anônimo especificando uma das três configurações de restrição de acesso:

Valor	Descrição
no-restriction (predefinição)	Não especifica restrições de acesso para usuários anônimos.
no-enumeration	Especifica que somente a enumeração é restrita para usuários anônimos.
no-access	Especifica que o acesso é restrito para usuários anônimos.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Configure a configuração restringir anônimo: `vserver cifs options modify -vserver vserver_name -restrict-anonymous {no-restriction|no-enumeration|no-access}`
3. Verifique se a opção está definida para o valor desejado: `vserver cifs options show -vserver vserver_name`
4. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Informações relacionadas

[Opções de servidor SMB disponíveis](#)

Gerencie como a segurança de arquivos é apresentada aos clientes SMB para dados de estilo de segurança UNIX

Gerencie como a segurança de arquivos é apresentada aos clientes SMB para visão geral de dados em estilo de segurança UNIX

Você pode escolher como deseja apresentar a segurança de arquivos a clientes SMB para dados de estilo de segurança UNIX ativando ou desativando a apresentação de ACLs NTFS para clientes SMB. Há vantagens em cada configuração, que você deve entender para escolher a configuração mais adequada para seus requisitos de negócios.

Por padrão, o ONTAP apresenta permissões UNIX em volumes estilo de segurança UNIX para clientes SMB como ACLs NTFS. Existem cenários em que isso é desejável, incluindo o seguinte:

- Você deseja exibir e editar permissões UNIX usando a guia **Segurança** na caixa Propriedades do Windows.

Não é possível modificar permissões de um cliente Windows se a operação não for permitida pelo sistema UNIX. Por exemplo, você não pode alterar a propriedade de um arquivo que você não possui, porque o sistema UNIX não permite essa operação. Essa restrição impede que clientes SMB ignorem permissões UNIX definidas nos arquivos e pastas.

- Os usuários estão editando e salvando arquivos no volume estilo de segurança UNIX usando certos aplicativos do Windows, por exemplo, Microsoft Office, onde o ONTAP deve preservar permissões UNIX durante operações de salvamento.
- Existem certos aplicativos do Windows no seu ambiente que esperam ler ACLs NTFS em arquivos que usam.

Em certas circunstâncias, você pode querer desativar a apresentação de permissões UNIX como ACLs NTFS. Se esta funcionalidade estiver desativada, o ONTAP apresenta volumes de estilo de segurança UNIX como volumes FAT para clientes SMB. Existem razões específicas pelas quais você pode querer apresentar volumes de estilo de segurança UNIX como volumes FAT para clientes SMB:

- Você só altera permissões UNIX usando montagens em clientes UNIX.

A guia Segurança não está disponível quando um volume de estilo de segurança UNIX é mapeado em um cliente SMB. A unidade mapeada parece ser formatada com o sistema de arquivos FAT, que não tem permissões de arquivo.

- Você está usando aplicativos sobre SMB que definem ACLs NTFS em arquivos e pastas acessados, o que pode falhar se os dados residirem em volumes de estilo de segurança UNIX.

Se o ONTAP relatar o volume como FAT, o aplicativo não tenta alterar uma ACL.

Informações relacionadas

[Configurando estilos de segurança no FlexVol volumes](#)

[Configurando estilos de segurança no qtrees](#)

Ative ou desative a apresentação de ACLs NTFS para dados de estilo de segurança UNIX

Você pode ativar ou desativar a apresentação de ACLs NTFS para clientes SMB para dados de estilo de segurança UNIX (volumes de estilo de segurança UNIX e volumes mistos de estilo de segurança com segurança efetiva UNIX).

Sobre esta tarefa

Se você ativar essa opção, o ONTAP apresenta arquivos e pastas em volumes com estilo de segurança UNIX eficaz para clientes SMB como tendo ACLs NTFS. Se desativar esta opção, os volumes são apresentados como volumes FAT para clientes SMB. O padrão é apresentar ACLs NTFS a clientes SMB.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Configure a configuração da opção ACL NTFS UNIX: `vserver cifs options modify -vserver vserver_name -is-unix-nt-acl-enabled {true|false}`
3. Verifique se a opção está definida para o valor desejado: `vserver cifs options show -vserver vserver_name`
4. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Como o ONTAP preserva as permissões UNIX

Quando os arquivos em um FlexVol volume que atualmente têm permissões UNIX são editados e salvos por aplicativos do Windows, o ONTAP pode preservar as permissões

UNIX.

Quando os aplicativos em clientes do Windows editam e salvam arquivos, eles leem as propriedades de segurança do arquivo, criam um novo arquivo temporário, aplicam essas propriedades ao arquivo temporário e dão ao arquivo temporário o nome do arquivo original.

Quando os clientes Windows executam uma consulta para as propriedades de segurança, eles recebem uma ACL construída que representa exatamente as permissões UNIX. O único propósito desta ACL construída é preservar as permissões UNIX do arquivo, pois os arquivos são atualizados por aplicativos do Windows para garantir que os arquivos resultantes tenham as mesmas permissões UNIX. O ONTAP não define nenhuma ACLs NTFS usando a ACL construída.

Gerenciar permissões UNIX usando a guia Segurança do Windows

Se você quiser manipular permissões UNIX de arquivos ou pastas em volumes mistos de estilo de segurança ou qtrees em SVMs, você pode usar a guia Segurança em clientes Windows. Como alternativa, você pode usar aplicativos que podem consultar e definir ACLs do Windows.

- Modificação de permissões UNIX

Você pode usar a guia Segurança do Windows para exibir e alterar permissões UNIX para um volume ou qtree misto de estilo de segurança. Se você usar a guia principal de Segurança do Windows para alterar permissões UNIX, primeiro remova o ACE existente que deseja editar (isso define os bits de modo como 0) antes de fazer as alterações. Como alternativa, você pode usar o editor avançado para alterar permissões.

Se as permissões de modo forem usadas, você pode alterar diretamente as permissões de modo para o UID listado, GID e outros (todos os outros com uma conta no computador). Por exemplo, se o UID exibido tiver permissões r-x, você pode alterar as permissões UID para rwx.

- Alterando permissões UNIX para permissões NTFS

Você pode usar a guia Segurança do Windows para substituir objetos de segurança UNIX por objetos de segurança do Windows em um volume de estilo de segurança misto ou qtree onde os arquivos e pastas têm um estilo de segurança eficaz UNIX.

Você deve primeiro remover todas as entradas de permissão UNIX listadas antes de poder substituí-las pelos objetos de Usuário e Grupo do Windows desejados. Em seguida, você pode configurar ACLs baseadas em NTFS nos objetos Usuário e Grupo do Windows. Removendo todos os objetos de segurança UNIX e adicionando apenas usuários e grupos do Windows a um arquivo ou pasta em um volume ou qtree misto de estilo de segurança, você altera o estilo de segurança efetivo no arquivo ou pasta de UNIX para NTFS.

Ao alterar permissões em uma pasta, o comportamento padrão do Windows é propagar essas alterações para todas as subpastas e arquivos. Portanto, você deve alterar a opção de propagação para a configuração desejada se não quiser propagar uma alteração no estilo de segurança para todas as pastas, subpastas e arquivos filhos.

Gerenciar configurações de segurança do servidor SMB

Como o ONTAP lida com a autenticação de cliente SMB

Antes que os usuários possam criar conexões SMB para acessar dados contidos no SVM, elas devem ser autenticadas pelo domínio ao qual o servidor SMB pertence. O servidor SMB suporta dois métodos de autenticação, Kerberos e NTLM (NTLMv1 ou NTLMv2). Kerberos é o método padrão usado para autenticar usuários de domínio.

Autenticação Kerberos

O ONTAP oferece suporte à autenticação Kerberos ao criar sessões SMB autenticadas.

Kerberos é o serviço de autenticação principal do Active Directory. O servidor Kerberos, ou serviço KDC (Centro de distribuição de chaves Kerberos), armazena e recupera informações sobre princípios de segurança no Active Directory. Ao contrário do modelo NTLM, os clientes do Active Directory que desejam estabelecer uma sessão com outro computador, como o servidor SMB, contatam diretamente um KDC para obter suas credenciais de sessão.

Autenticação NTLM

A autenticação de cliente NTLM é feita usando um protocolo de resposta de desafio baseado no conhecimento compartilhado de um segredo específico do usuário com base em uma senha.

Se um usuário criar uma conexão SMB usando uma conta de usuário local do Windows, a autenticação é feita localmente pelo servidor SMB usando NTLMv2.

Diretrizes para configurações de segurança de servidor SMB em uma configuração de recuperação de desastres SVM

Antes de criar um SVM configurado como um destino de recuperação de desastres em que a identidade não seja preservada (a `-identity-preserve` opção está definida como `false` na configuração do SnapMirror), você deve saber como as configurações de segurança do servidor SMB são gerenciadas no SVM de destino.

- As configurações de segurança de servidor SMB não padrão não são replicadas para o destino.

Quando você cria um servidor SMB no SVM de destino, todas as configurações de segurança do servidor SMB são definidas como valores padrão. Quando o destino de recuperação de desastres da SVM é inicializado, atualizado ou ressincido, as configurações de segurança do servidor SMB na origem não são replicadas para o destino.

- Você deve configurar manualmente configurações de segurança de servidor SMB não padrão.

Se você tiver configurações de segurança de servidor SMB não padrão configuradas no SVM de origem, será necessário configurar manualmente essas mesmas configurações no SVM de destino depois que o destino se tornar leitura-gravação (depois que a relação SnapMirror for interrompida).

Exibir informações sobre as configurações de segurança do servidor SMB

Você pode exibir informações sobre as configurações de segurança do servidor SMB em suas máquinas virtuais de armazenamento (SVMs). Pode utilizar estas informações para verificar se as definições de segurança estão corretas.

Sobre esta tarefa

Uma configuração de segurança exibida pode ser o valor padrão para esse objeto ou um valor não padrão configurado usando a CLI do ONTAP ou usando objetos de diretiva de grupo (GPOs) do Active Directory.

Não use o `vserver cifs security show` comando para servidores SMB no modo de grupo de trabalho, porque algumas das opções não são válidas.

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre...	Digite o comando...
Todas as configurações de segurança em uma SVM especificada	<code>vserver cifs security show -vserver <i>vserver_name</i></code>
Configurações ou configurações de segurança específicas no SVM	<code>vserver cifs security show -vserver <i>_vserver_name_</i> -fields [fieldname,...]</code> Você pode inserir <code>-fields ?</code> para determinar quais campos você pode usar.

Exemplo

O exemplo a seguir mostra todas as configurações de segurança do SVM VS1:

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

Vserver: vs1

                Kerberos Clock Skew:           5 minutes
                Kerberos Ticket Age:            10 hours
                Kerberos Renewal Age:           7 days
                Kerberos KDC Timeout:          3 seconds
                Is Signing Required:            false
                Is Password Complexity Required: true
                Use start_tls For AD LDAP connection: false
                Is AES Encryption Enabled:      false
                LM Compatibility Level:         lm-ntlm-ntlmv2-krb
                Is SMB Encryption Required:     false
                Client Session Security:       none
                SMB1 Enabled for DC Connections: false
                SMB2 Enabled for DC Connections: system-default
                LDAP Referral Enabled For AD LDAP connections: false
                Use LDAPS for AD LDAP connection: false
                Encryption is required for DC Connections: false
                AES session key enabled for NetLogon channel: false
                Try Channel Binding For AD LDAP Connections: false
```

Observe que as configurações exibidas dependem da versão do ONTAP em execução.

O exemplo a seguir mostra a inclinação do relógio Kerberos para SVM VS1:

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew

      vserver kerberos-clock-skew
      -----
vs1      5
```

Informações relacionadas

[Exibindo informações sobre as configurações do GPO](#)

Ative ou desative a complexidade de senha necessária para usuários SMB locais

A complexidade de senha necessária fornece segurança aprimorada para usuários locais de SMB em suas máquinas virtuais de armazenamento (SVMs). A funcionalidade de complexidade de palavra-passe necessária está ativada por predefinição. Você pode desativá-lo e reativá-lo a qualquer momento.

Antes de começar

Usuários locais, grupos locais e autenticação de usuário local devem estar habilitados no servidor CIFS.



Sobre esta tarefa

Não use o `vserver cifs security modify` comando para um servidor CIFS no modo de grupo de trabalho porque algumas das opções não são válidas.

Passos

1. Execute uma das seguintes ações:

Se você quiser que a complexidade de senha necessária para usuários SMB locais seja...	Digite o comando...
Ativado	<pre>vserver cifs security modify -vserver vserver_name -is-password-complexity -required true</pre>
Desativado	<pre>vserver cifs security modify -vserver vserver_name -is-password-complexity -required false</pre>

2. Verifique a configuração de segurança para a complexidade necessária da senha: `vserver cifs security show -vserver vserver_name`

Exemplo

O exemplo a seguir mostra que a complexidade de senha necessária está habilitada para usuários SMB locais

para SVM VS1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
-----
vs1      true
```

Informações relacionadas

[Exibindo informações sobre as configurações de segurança do servidor CIFS](#)

[Usando usuários locais e grupos para autenticação e autorização](#)

[Requisitos para senhas de usuários locais](#)

[Alterando senhas de contas de usuário locais](#)

Modifique as configurações de segurança Kerberos do servidor CIFS

Você pode modificar certas configurações de segurança Kerberos do servidor CIFS, incluindo o tempo máximo permitido de distorção do relógio Kerberos, a vida útil do ticket Kerberos e o número máximo de dias de renovação de ticket.

Sobre esta tarefa

Modificar as configurações do Kerberos do servidor CIFS usando o `vserver cifs security modify` comando modifica as configurações somente na máquina virtual de armazenamento (SVM) única que você especificar com o `-vserver` parâmetro. Você pode gerenciar centralmente as configurações de segurança Kerberos para todos os SVMs no cluster que pertencem ao mesmo domínio do ativo Directory usando os GPOs (objetos de diretiva de grupo) do ativo Directory.

Passos

1. Execute uma ou mais das seguintes ações:

Se você quiser...	Digite...
Especifique o tempo máximo permitido de distorção do relógio Kerberos em minutos (9.13.1 e posterior) ou segundos (9.12.1 ou anterior).	<pre>vserver cifs security modify -vserver vserver_name -kerberos-clock-skew integer_in_minutes</pre> <p>A predefinição é 5 minutos.</p>
Especifique a vida útil do ticket Kerberos em horas.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-ticket-age integer_in_hours</pre> <p>A predefinição é 10 horas.</p>

Especifique o número máximo de dias de renovação do ticket.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-renew-age integer_in_days</pre> <p>A configuração padrão é de 7 dias.</p>
Especifique o tempo limite para sockets em KDCs após o qual todos os KDCs são marcados como inalcançáveis.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-kdc-timeout integer_in_seconds</pre> <p>A predefinição é 3 segundos.</p>

2. Verifique as configurações de segurança do Kerberos:

```
vserver cifs security show -vserver vserver_name
```

Exemplo

O exemplo a seguir faz as seguintes alterações na segurança Kerberos: "Kerberos Clock Skew" está definido como 3 minutos e "Kerberos Ticket Age" está definido como 8 horas para o SVM VS1:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                Kerberos Clock Skew:                3 minutes
                Kerberos Ticket Age:                  8 hours
                Kerberos Renewal Age:                  7 days
                Kerberos KDC Timeout:                  3 seconds
                Is Signing Required:                    false
                Is Password Complexity Required:         true
                Use start_tls For AD LDAP connection:   false
                Is AES Encryption Enabled:              false
                LM Compatibility Level: lm-ntlm-ntlmv2-krb
                Is SMB Encryption Required:             false
```

Informações relacionadas

["Exibindo informações sobre as configurações de segurança do servidor CIFS"](#)

["GPOs compatíveis"](#)

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

Defina o nível mínimo de segurança de autenticação do servidor SMB

Você pode definir o nível mínimo de segurança do servidor SMB, também conhecido como *LMCompatibilityLevel*, em seu servidor SMB para atender aos requisitos de segurança da sua empresa para acesso ao cliente SMB. O nível mínimo de segurança é o nível mínimo dos tokens de segurança que o servidor SMB aceita de clientes SMB.

Sobre esta tarefa



- Os servidores SMB no modo de grupo de trabalho suportam apenas a autenticação NTLM. A autenticação Kerberos não é suportada.
- *LMCompatibilityLevel* aplica-se apenas à autenticação de cliente SMB, não à autenticação de administrador.

Você pode definir o nível mínimo de segurança de autenticação para um dos quatro níveis de segurança suportados.

Valor	Descrição
lm-ntlm-ntlmv2-krb (predefinição)	A máquina virtual de armazenamento (SVM) aceita segurança de autenticação LM, NTLM, NTLMv2 e Kerberos.
ntlm-ntlmv2-krb	O SVM aceita segurança de autenticação NTLM, NTLMv2 e Kerberos. O SVM nega a autenticação LM.
ntlmv2-krb	O SVM aceita a segurança de autenticação NTLMv2 e Kerberos. O SVM nega a autenticação LM e NTLM.
krb	O SVM aceita apenas a segurança de autenticação Kerberos. O SVM nega a autenticação LM, NTLM e NTLMv2.

Passos

1. Defina o nível mínimo de segurança de autenticação: `vserver cifs security modify -vserver vserver_name -lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. Verifique se o nível de segurança de autenticação está definido para o nível desejado: `vserver cifs security show -vserver vserver_name`

Informações relacionadas

[Ativar ou desativar a criptografia AES para comunicação baseada no Kerberos](#)

Configurar segurança forte para comunicação baseada no Kerberos usando criptografia AES

Para uma segurança mais forte com comunicação baseada no Kerberos, é possível ativar a criptografia AES-256 e AES-128 no servidor SMB. Por padrão, quando você cria um servidor SMB no SVM, a criptografia AES (Advanced Encryption Standard) é desativada. Você deve habilitá-lo para aproveitar a segurança forte fornecida pela

criptografia AES.

A comunicação relacionada ao Kerberos para SMB é usada durante a criação do servidor SMB na SVM, bem como durante a fase de configuração da sessão SMB. O servidor SMB suporta os seguintes tipos de criptografia para comunicação Kerberos:

- AES 256
- AES 128
- DES
- RC4-HMAC

Se você quiser usar o tipo de criptografia de segurança mais alto para comunicação Kerberos, ative a criptografia AES para comunicação Kerberos no SVM.

Quando o servidor SMB é criado, o controlador de domínio cria uma conta de máquina de computador no ative Directory. Neste momento, o KDC se torna ciente dos recursos de criptografia da conta de máquina específica. Posteriormente, um tipo de criptografia específico é selecionado para criptografar o ticket de serviço que o cliente apresenta ao servidor durante a autenticação.

A partir do ONTAP 9.12,1, você pode especificar quais tipos de criptografia anunciar no KDC do ative Directory (AD). Pode utilizar a `-advertised-enc-types` opção para ativar os tipos de encriptação recomendados e pode utilizá-la para desativar os tipos de encriptação mais fracos. Aprenda a ["Ative e desative os tipos de criptografia para comunicação baseada no Kerberos"](#).



As novas instruções Intel AES (Intel AES NI) estão disponíveis no SMB 3,0, melhorando o algoritmo AES e acelerando a criptografia de dados com famílias de processadores suportadas. Começando com SMB 3,1.1, AES-128-GCM substitui AES-128-CCM como o algoritmo hash usado pela criptografia SMB.

Informações relacionadas

[Modificação das configurações de segurança Kerberos do servidor CIFS](#)

Ativar ou desativar a encriptação AES para comunicação baseada no Kerberos

Para aproveitar a segurança mais forte com a comunicação baseada no Kerberos, você deve usar a criptografia AES-256 e AES-128 no servidor SMB. A partir do ONTAP 9.13,1, a encriptação AES é ativada por predefinição. Se você não quiser que o servidor SMB selecione os tipos de criptografia AES para comunicação baseada em Kerberos com o KDC do ative Directory (AD), você pode desativar a criptografia AES.

Se a encriptação AES está ativada por predefinição e se tem a opção de especificar tipos de encriptação depende da versão do ONTAP.

Versão de ONTAP	A encriptação AES está ativada ...	Você pode especificar tipos de criptografia?
9.13.1 e mais tarde	Por padrão	Sim
9.12.1	Manualmente	Sim
9.11.1 e anteriores	Manualmente	Não

A partir do ONTAP 9.12,1, a criptografia AES é ativada e desativada usando a `-advertised-enc-types` opção, que permite especificar os tipos de criptografia anunciados para o AD KDC. A configuração padrão é `rc4` e `des`, mas quando um tipo AES é especificado, a criptografia AES é ativada. Você também pode usar a opção para desativar explicitamente os tipos de criptografia RC4 e DES mais fracos. No ONTAP 9.11,1 e anterior, você deve usar a `-is-aes-encryption-enabled` opção para ativar e desativar a criptografia AES e os tipos de criptografia não podem ser especificados.

Para melhorar a segurança, a máquina virtual de armazenamento (SVM) altera a senha da conta de máquina no AD sempre que a opção de segurança AES é modificada. A alteração da senha pode exigir credenciais administrativas do AD para a unidade organizacional (ou) que contém a conta da máquina.

Se um SVM for configurado como um destino de recuperação de desastres em que a identidade não seja preservada (a `-identity-preserve` opção está definida como `false` na configuração do SnapMirror), as configurações de segurança do servidor SMB não padrão não serão replicadas para o destino. Se você ativou a criptografia AES no SVM de origem, será necessário habilitá-la manualmente.

Exemplo 1. Passos

ONTAP 9.12,1 e posterior

1. Execute uma das seguintes ações:

Se você quiser que os tipos de criptografia AES para comunicação Kerberos sejam...	Digite o comando...
Ativado	<pre>vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256</pre>
Desativado	<pre>vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4</pre>

Nota: a `-is-aes-encryption-enabled` opção está obsoleta no ONTAP 9.12,1 e pode ser removida em uma versão posterior.

2. Verifique se a criptografia AES está ativada ou desativada conforme desejado: `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

Exemplos

O exemplo a seguir habilita os tipos de criptografia AES para o servidor SMB no SVM VS1:

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver  advertised-enc-types
-----  -----
vs1      aes-128,aes-256
```

O exemplo a seguir habilita os tipos de criptografia AES para o servidor SMB no SVM VS2. O administrador é solicitado a inserir as credenciais administrativas do AD para a UO que contém o servidor SMB.

```
cluster1::> vserver cifs security modify -vserver vs2 -advertised-enc
-types aes-128,aes-256
```

Info: In order to enable SMB AES encryption, the password for the SMB server machine account must be reset. Enter the username and password for the SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

```
cluster1::> vserver cifs security show -vserver vs2 -fields advertised-
enc-types
```

```
vserver  advertised-enc-types
-----  -----
vs2      aes-128,aes-256
```

ONTAP 9.11,1 e anteriores

1. Execute uma das seguintes ações:

Se você quiser que os tipos de criptografia AES para comunicação Kerberos sejam...	Digite o comando...
Ativado	<pre>vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled true</pre>
Desativado	<pre>vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false</pre>

2. Verifique se a criptografia AES está ativada ou desativada conforme desejado: `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

O `is-aes-encryption-enabled` campo é exibido `true` se a criptografia AES estiver ativada e `false` se estiver desativada.

Exemplos

O exemplo a seguir habilita os tipos de criptografia AES para o servidor SMB no SVM VS1:

```

cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-----
vs1      true

```

O exemplo a seguir habilita os tipos de criptografia AES para o servidor SMB no SVM VS2. O administrador é solicitado a inserir as credenciais administrativas do AD para a UO que contém o servidor SMB.

```

cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-----
vs2      true

```

Informações relacionadas

["O usuário de domínio não consegue fazer login no cluster com Domain-Tunnel"](#)

Utilize a assinatura SMB para melhorar a segurança da rede

Utilize a assinatura SMB para melhorar a visão geral da segurança da rede

A assinatura SMB ajuda a garantir que o tráfego de rede entre o servidor SMB e o cliente não seja comprometido; isso evita ataques de repetição. Por padrão, o ONTAP oferece suporte à assinatura SMB quando solicitado pelo cliente. Opcionalmente, o administrador de armazenamento pode configurar o servidor SMB para exigir assinatura SMB.

Como as políticas de assinatura SMB afetam a comunicação com um servidor CIFS

Além das configurações de segurança de assinatura SMB do servidor CIFS, duas diretivas de assinatura SMB em clientes Windows controlam a assinatura digital de comunicações entre clientes e o servidor CIFS. Você pode configurar a configuração que atende aos requisitos da sua empresa.

As diretivas SMB do cliente são controladas por meio das configurações de diretiva de segurança local do Windows, que são configuradas usando o MMC (Console de Gerenciamento da Microsoft) ou GPOs do ative Directory. Para obter mais informações sobre a assinatura SMB do cliente e problemas de segurança, consulte a documentação do Microsoft Windows.

Aqui estão descrições das duas políticas de assinatura SMB em clientes Microsoft:

- `Microsoft network client: Digitally sign communications (if server agrees)`

Esta configuração controla se a capacidade de assinatura SMB do cliente está ativada. Ele é habilitado por padrão. Quando essa configuração é desativada no cliente, as comunicações do cliente com o servidor CIFS dependem da configuração de assinatura SMB no servidor CIFS.

- `Microsoft network client: Digitally sign communications (always)`

Esta configuração controla se o cliente requer assinatura SMB para se comunicar com um servidor. Ele está desativado por padrão. Quando essa configuração é desativada no cliente, o comportamento de assinatura SMB é baseado na configuração de diretiva `Microsoft network client: Digitally sign communications (if server agrees)` e na configuração no servidor CIFS.



Se o seu ambiente incluir clientes Windows configurados para exigir assinatura SMB, você deverá ativar a assinatura SMB no servidor CIFS. Se você não fizer isso, o servidor CIFS não poderá fornecer dados a esses sistemas.

Os resultados efetivos das configurações de assinatura SMB do cliente e do servidor CIFS dependem se as sessões SMB usam SMB 1,0 ou SMB 2.x e posterior.

A tabela a seguir resume o comportamento eficaz de assinatura SMB se a sessão usar SMB 1,0:

Cliente	ONTAP—assinatura não necessária	ONTAP - assinatura necessária
Assinatura desativada e não necessária	Não assinado	Assinado
Assinatura ativada e não necessária	Não assinado	Assinado
Assinatura desativada e necessária	Assinado	Assinado
Assinatura ativada e necessária	Assinado	Assinado



Clientes Windows SMB 1 mais antigos e alguns clientes SMB 1 não Windows podem não conseguir se conectar se a assinatura estiver desativada no cliente, mas necessária no servidor CIFS.

A tabela a seguir resume o comportamento eficaz de assinatura SMB se a sessão usar SMB 2.x ou SMB 3,0:



Para clientes SMB 2.x e SMB 3,0, a assinatura SMB está sempre ativada. Não pode ser desativado.

Cliente	ONTAP—assinatura não necessária	ONTAP - assinatura necessária
Assinatura não necessária	Não assinado	Assinado
Assinatura necessária	Assinado	Assinado

A tabela a seguir resume o comportamento padrão de assinatura SMB de cliente e servidor da Microsoft:

Protocolo	Algoritmo hash	Pode ativar/desativar	Pode exigir/não exigir	Padrão do cliente	Padrão do servidor	DC predefinido
SMB 1,0	MD5	Sim	Sim	Ativado (não necessário)	Desativado (não necessário)	Obrigatório
SMB 2.x	HMAC SHA-256	Não	Sim	Não é necessário	Não é necessário	Obrigatório
SMB 3,0	AES-CMAC.	Não	Sim	Não é necessário	Não é necessário	Obrigatório



A Microsoft não recomenda mais o uso `Digitally sign communications (if client agrees)` das configurações de Diretiva de Grupo ou `Digitally sign communications (if server agrees)`. A Microsoft também não recomenda mais o uso das `EnableSecuritySignature` configurações do Registro. Essas opções afetam apenas o comportamento do SMB 1 e podem ser substituídas pela `Digitally sign communications (always)` configuração de Diretiva de Grupo ou pela `RequireSecuritySignature` configuração do Registro. Você também pode obter mais informações do blog da Microsoft. <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>[The Fundamentos de assinatura SMB (abrangendo SMB1 e SMB2)]

Impacto na performance da assinatura SMB

Quando as sessões SMB usam a assinatura SMB, todas as comunicações SMB de e para clientes Windows têm um impactos na performance, o que afeta tanto os clientes quanto o servidor (ou seja, os nós no cluster que executa o SVM que contém o servidor SMB).

O impacto no desempenho mostra como aumento do uso da CPU tanto nos clientes quanto no servidor, embora a quantidade de tráfego de rede não mude.

A extensão do impacto no desempenho depende da versão do ONTAP 9 que você está executando. A partir do ONTAP 9.7, um novo algoritmo de criptografia off-load pode permitir melhor desempenho no tráfego SMB assinado. A descarga de assinatura SMB é ativada por padrão quando a assinatura SMB está ativada.

O desempenho aprimorado de assinatura SMB requer a capacidade de descarga AES-NI. Consulte o Hardware Universe (HWU) para verificar se a descarga AES-NI é suportada para sua plataforma.

Melhorias adicionais de desempenho também são possíveis se você for capaz de usar SMB versão 3,11, que suporta o algoritmo GCM muito mais rápido.

Dependendo da sua rede, versão do ONTAP 9, versão do SMB e implementação do SVM, o impacto na performance da assinatura SMB pode variar muito. Você pode verificá-lo somente por meio de testes em seu ambiente de rede.

A maioria dos clientes do Windows negocia a assinatura SMB por padrão se estiver habilitada no servidor. Se você precisar de proteção SMB para alguns de seus clientes Windows e se a assinatura SMB estiver causando problemas de desempenho, você poderá desativar a assinatura SMB em qualquer um de seus clientes Windows que não precisem de proteção contra ataques de repetição. Para obter informações sobre como desativar a assinatura SMB em clientes Windows, consulte a documentação do Microsoft Windows.

Recomendações para configurar a assinatura SMB

Você pode configurar o comportamento de assinatura SMB entre clientes SMB e o servidor CIFS para atender aos seus requisitos de segurança. As configurações escolhidas ao configurar a assinatura SMB no servidor CIFS dependem de quais são os requisitos de segurança.

Você pode configurar a assinatura SMB no cliente ou no servidor CIFS. Considere as seguintes recomendações ao configurar a assinatura SMB:

Se...	Recomendação...
Você deseja aumentar a segurança da comunicação entre o cliente e o servidor	Torne a assinatura SMB necessária no cliente ativando a <code>Require Option (Sign always)</code> configuração de segurança no cliente.
Você deseja que todo o tráfego SMB para uma determinada máquina virtual de storage (SVM) seja assinado	Torne necessária a assinatura SMB no servidor CIFS configurando as configurações de segurança para exigir assinatura SMB.

Consulte a documentação da Microsoft para obter mais informações sobre como configurar as configurações de segurança do cliente Windows.

Diretrizes para assinatura SMB quando vários dados LIFS são configurados

Se você ativar ou desativar a assinatura SMB necessária no servidor SMB, você deve estar ciente das diretrizes para várias configurações LIFS de dados para um SVM.

Quando você configura um servidor SMB, pode haver várias LIFs de dados configuradas. Nesse caso, o

servidor DNS contém várias A entradas de Registro para o servidor CIFS, todas usando o mesmo nome de host do servidor SMB, mas cada uma com um endereço IP exclusivo. Por exemplo, um servidor SMB que tem duas LIFs de dados configuradas pode ter as seguintes entradas de Registro DNS A:

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

O comportamento normal é que, ao alterar a configuração de assinatura SMB necessária, apenas novas conexões de clientes são afetadas pela alteração na configuração de assinatura SMB. No entanto, há uma exceção a esse comportamento. Há um caso em que um cliente tem uma conexão existente com um compartilhamento, e o cliente cria uma nova conexão com o mesmo compartilhamento após a configuração ser alterada, mantendo a conexão original. Nesse caso, tanto a conexão SMB nova quanto a existente adotam os novos requisitos de assinatura SMB.

Considere o seguinte exemplo:

1. Client1 conecta-se a um compartilhamento sem a assinatura SMB necessária usando o caminho `o:\`.
2. O administrador de armazenamento modifica a configuração do servidor SMB para exigir assinatura SMB.
3. O Client1 conecta-se ao mesmo compartilhamento com a assinatura SMB necessária usando o caminho `s:\` (mantendo a conexão usando o caminho `o:\`).
4. O resultado é que a assinatura SMB é usada ao acessar dados `o:\` nas unidades e `s:\`.

Ative ou desative a assinatura SMB necessária para o tráfego SMB de entrada

Você pode impor o requisito para que os clientes assinem mensagens SMB habilitando a assinatura SMB necessária. Se ativado, o ONTAP aceita mensagens SMB somente se elas tiverem assinaturas válidas. Se você quiser permitir a assinatura SMB, mas não a exigir, você pode desativar a assinatura SMB necessária.

Sobre esta tarefa

Por padrão, a assinatura SMB necessária está desativada. Você pode ativar ou desativar a assinatura SMB necessária a qualquer momento.

A assinatura SMB não está desativada por padrão nas seguintes circunstâncias:

1. A assinatura SMB necessária está ativada e o cluster é revertido para uma versão do ONTAP que não suporta assinatura SMB.
2. O cluster é posteriormente atualizado para uma versão do ONTAP que suporte a assinatura SMB.



Nestas circunstâncias, a configuração de assinatura SMB que foi originalmente configurada em uma versão suportada do ONTAP é mantida por meio de reversão e atualização subsequente.

Quando você configura uma relação de recuperação de desastres de máquina virtual de storage (SVM), o valor selecionado para a `-identity-preserve` opção `snapmirror create` do comando determina os detalhes de configuração replicados no SVM de destino.

Se você definir `-identity-preserve` a opção como `true` (ID-Preserve), a configuração de segurança de assinatura SMB será replicada para o destino.

Se você definir `-identity-preserve` a opção como `false` (non-ID-Preserve), a configuração de segurança de assinatura SMB não será replicada para o destino. Nesse caso, as configurações de segurança do servidor CIFS no destino são definidas com os valores padrão. Se você ativou a assinatura SMB necessária na SVM de origem, habilite manualmente a assinatura SMB necessária no SVM de destino.

Passos

1. Execute uma das seguintes ações:

Se você quiser que a assinatura SMB seja necessária...	Digite o comando...
Ativado	<pre>vserver cifs security modify -vserver vserver_name -is-signing-required true</pre>
Desativado	<pre>vserver cifs security modify -vserver vserver_name -is-signing-required false</pre>

2. Verifique se a assinatura SMB necessária está ativada ou desativada determinando se o valor no `Is Signing Required` campo na saída do comando a seguir está definido para o valor desejado: `vserver cifs security show -vserver vserver_name -fields is-signing-required`

Exemplo

O exemplo a seguir habilita a assinatura SMB necessária para o SVM VS1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required  
true  
  
cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-  
required  
vserver  is-signing-required  
-----  
vs1      true
```



As alterações nas definições de encriptação entram em vigor para novas ligações. As ligações existentes não são afetadas.

Determine se as sessões SMB são assinadas

Você pode exibir informações sobre sessões SMB conetadas no servidor CIFS. Você pode usar essas informações para determinar se as sessões SMB são assinadas. Isso pode ser útil para determinar se as sessões de cliente SMB estão se conetando com as configurações de segurança desejadas.

Passos

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre...	Digite o comando...
Todas as sessões assinadas em uma máquina virtual de storage (SVM) especificada	<code>vserver cifs session show -vserver <i>vserver_name</i> -is-session-signed true</code>
Detalhes de uma sessão assinada com um Session ID específico no SVM	<code>vserver cifs session show -vserver <i>vserver_name</i> -session-id integer -instance</code>

Exemplos

O comando a seguir exibe informações de sessão sobre sessões assinadas no SVM VS1. A saída de resumo padrão não exibe o campo de saída "is Session signed":

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:      node1
Vserver:   vs1
Connection Session
ID          ID          Workstation      Windows User      Open      Idle
-----
3151272279  1          10.1.1.1        DOMAIN\joe        2         23s
```

O comando a seguir exibe informações detalhadas da sessão, incluindo se a sessão está assinada, em uma sessão SMB com um Session ID de 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: nodel
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted
```

Informações relacionadas

[Monitoramento de estatísticas de sessão assinadas pelo SMB](#)

Monitorar estatísticas de sessão assinadas pelo SMB

Você pode monitorar estatísticas de sessões SMB e determinar quais sessões estabelecidas são assinadas e quais não são.

Sobre esta tarefa

O `statistics` comando no nível de privilégio avançado fornece o `signed_sessions` contador que você pode usar para monitorar o número de sessões SMB assinadas. O `signed_sessions` contador está disponível com os seguintes objetos estatísticos:

- `cifs` Permite monitorar a assinatura SMB para todas as sessões SMB.
- `smb1` Permite monitorar a assinatura SMB para sessões SMB 1,0.
- `smb2` Permite monitorar a assinatura SMB para sessões SMB 2.x e SMB 3,0.

As estatísticas SMB 3,0 são incluídas na saída para o `smb2` objeto.

Se você quiser comparar o número de sessão assinada com o número total de sessões, você pode comparar a saída para o contador com a saída `established_sessions` para `signed_sessions` o contador.

Você deve iniciar uma coleta de amostras de estatísticas antes de poder visualizar os dados resultantes. 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.

Passos

1. Defina o nível de privilégio como avançado `set -privilege advanced`
2. Iniciar uma coleta de dados `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]`

Se você não especificar o `-sample-id` parâmetro, o comando gera um identificador de amostra para você e define esse exemplo como a amostra padrão para a sessão CLI. O valor para `-sample-id` é uma cadeia de texto. Se você executar esse comando durante a mesma sessão CLI e não especificar o `-sample-id` parâmetro, o comando sobrescreverá a amostra padrão anterior.

Opcionalmente, você pode especificar o nó no qual deseja coletar estatísticas. Se você não especificar o nó, a amostra coletará estatísticas para todos os nós no cluster.

3. Use o `statistics stop` comando para parar de coletar dados para a amostra.
4. Exibir estatísticas de assinatura SMB:

Se você quiser ver informações para...	Digite...
Sessões assinadas	<code>`show -sample-id <i>sample_ID</i> -counter signed_sessions</code>
<code><i>node_name</i> [-node <i>node_name</i>]</code>	Sessões assinadas e sessões estabelecidas
<code>`show -sample-id <i>sample_ID</i> -counter signed_sessions</code>	<code>established_sessions</code>

Se você quiser exibir informações apenas para um único nó, especifique o parâmetro opcional `-node`.

5. Voltar para o nível de privilégio de administrador `set -privilege admin`

Exemplos

O exemplo a seguir mostra como você pode monitorar as estatísticas de assinatura SMB 2.x e SMB 3,0 na máquina virtual de armazenamento (SVM) VS1.

O seguinte comando move-se para o nível de privilégio avançado:

```
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
```

O comando a seguir inicia a coleta de dados para uma nova amostra:

```
cluster1::*> statistics start -object smb2 -sample-id smbSigning_sample  
-vserver vs1
```

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

O comando a seguir interrompe a coleta de dados para a amostra:

```
cluster1::*> statistics stop -sample-id smbSigning_sample
```

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

O comando a seguir mostra sessões SMB assinadas e sessões SMB estabelecidas por nó da amostra:

```
cluster1::*> statistics show -sample-id smbSigning_sample -counter
signed_sessions|established_sessions|node_name
```

Object: smb2

Instance: vs1

Start-time: 2/6/2013 01:00:00

End-time: 2/6/2013 01:03:04

Cluster: cluster1

Counter	Value
-----	-----
established_sessions	0
node_name	node1
signed_sessions	0
established_sessions	1
node_name	node2
signed_sessions	1
established_sessions	0
node_name	node3
signed_sessions	0
established_sessions	0
node_name	node4
signed_sessions	0

O comando a seguir mostra sessões SMB assinadas para node2 da amostra:

```
cluster1::*> statistics show -sample-id smbSigning_sample -counter
signed_sessions|node_name -node node2
```

Object: smb2

Instance: vs1

Start-time: 2/6/2013 01:00:00

End-time: 2/6/2013 01:22:43

Cluster: cluster1

Counter	Value
-----	-----
node_name	node2
signed_sessions	1

O seguinte comando volta para o nível de privilégio admin:

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

Informações relacionadas

[Determinar se as sessões SMB são assinadas](#)

["Visão geral do gerenciamento e monitoramento de desempenho"](#)

Configurar a criptografia SMB necessária em servidores SMB para transferências de dados por SMB

Visão geral da criptografia SMB

A encriptação SMB para transferências de dados através de SMB é um melhoramento de segurança que pode ativar ou desativar em servidores SMB. Você também pode configurar a configuração de criptografia SMB desejada em uma base de compartilhamento por compartilhamento por meio de uma configuração de propriedade de compartilhamento.

Por padrão, quando você cria um servidor SMB na máquina virtual de storage (SVM), a criptografia SMB é desativada. Você deve habilitá-lo para aproveitar a segurança aprimorada fornecida pela criptografia SMB.

Para criar uma sessão SMB encriptada, o cliente SMB tem de suportar a encriptação SMB. Os clientes Windows que começam com o Windows Server 2012 e o Windows 8 suportam a encriptação SMB.

A criptografia SMB no SVM é controlada por meio de duas configurações:

- Uma opção de segurança de servidor SMB que habilita a funcionalidade no SVM
- Uma propriedade de compartilhamento SMB que configura a configuração de criptografia SMB em uma base de compartilhamento por compartilhamento

Você pode decidir se deseja exigir criptografia para acesso a todos os dados no SVM ou se exige que a criptografia SMB acesse dados somente em compartilhamentos selecionados. As configurações de nível SVM substituem as configurações de nível de compartilhamento.

A configuração eficaz de criptografia SMB depende da combinação das duas configurações e é descrita na tabela a seguir:

Encriptação SMB do servidor SMB ativada	Compartilhar criptografar a configuração de dados ativada	Comportamento de criptografia do lado do servidor
Verdadeiro	Falso	A criptografia no nível do servidor está habilitada para todos os compartilhamentos na SVM. Com essa configuração, a criptografia acontece para toda a sessão SMB.
Verdadeiro	Verdadeiro	A criptografia no nível do servidor é ativada para todos os compartilhamentos no SVM, independentemente da criptografia no nível de compartilhamento. Com essa configuração, a criptografia acontece para toda a sessão SMB.

Encriptação SMB do servidor SMB ativada	Compartilhar criptografar a configuração de dados ativada	Comportamento de criptografia do lado do servidor
Falso	Verdadeiro	A criptografia no nível de compartilhamento está ativada para compartilhamentos específicos. Com essa configuração, a criptografia acontece a partir da conexão em árvore.
Falso	Falso	Nenhuma criptografia está ativada.

Os clientes SMB que não suportam encriptação não podem estabelecer ligação a um servidor SMB ou partilha que requeira encriptação.

As alterações nas definições de encriptação entram em vigor para novas ligações. As ligações existentes não são afetadas.

Impacto na performance da criptografia SMB

Quando as sessões SMB usam criptografia SMB, todas as comunicações SMB de e para clientes Windows têm um impactos na performance, o que afeta tanto os clientes quanto o servidor (ou seja, os nós no cluster que executa o SVM que contém o servidor SMB).

O impactos no desempenho mostra como aumento do uso da CPU tanto nos clientes quanto no servidor, embora a quantidade de tráfego de rede não mude.

A extensão do impactos no desempenho depende da versão do ONTAP 9 que você está executando. A partir do ONTAP 9.7, um novo algoritmo de criptografia off-load pode permitir melhor desempenho no tráfego SMB criptografado. A descarga de criptografia SMB é ativada por padrão quando a criptografia SMB está ativada.

O desempenho aprimorado da criptografia SMB requer a capacidade de descarga AES-NI. Consulte o Hardware Universe (HWU) para verificar se a descarga AES-NI é suportada para sua plataforma.

Melhorias adicionais de desempenho também são possíveis se você for capaz de usar SMB versão 3,11, que suporta o algoritmo GCM muito mais rápido.

Dependendo da sua rede, versão do ONTAP 9, versão do SMB e implementação do SVM, o impacto na performance da criptografia SMB pode variar muito. Você pode verificá-lo somente por meio de testes em seu ambiente de rede.

A encriptação SMB está desativada por predefinição no servidor SMB. Você deve habilitar a criptografia SMB somente nos compartilhamentos SMB ou servidores SMB que exigem criptografia. Com a criptografia SMB, o ONTAP realiza processamento adicional de descriptografar as solicitações e criptografar as respostas para cada solicitação. A criptografia SMB deve, portanto, ser ativada somente quando necessário.

Ative ou desative a encriptação SMB necessária para o tráfego SMB de entrada

Se pretender exigir encriptação SMB para o tráfego SMB de entrada, pode ativá-la no servidor CIFS ou no nível de partilha. Por padrão, a criptografia SMB não é necessária.

Sobre esta tarefa

Você pode ativar a criptografia SMB no servidor CIFS, que se aplica a todos os compartilhamentos no servidor CIFS. Se não pretender a encriptação SMB necessária para todos os partilhas no servidor CIFS ou se pretender ativar a encriptação SMB necessária para o tráfego SMB de entrada numa base de partilha por partilha, pode desativar a encriptação SMB necessária no servidor CIFS.

Quando você configura uma relação de recuperação de desastres de máquina virtual de storage (SVM), o valor selecionado para a `-identity-preserve` opção `snapmirror create` do comando determina os detalhes de configuração replicados no SVM de destino.

Se você definir `-identity-preserve` a opção como `true` (ID-Preserve), a configuração de segurança de criptografia SMB será replicada para o destino.

Se você definir `-identity-preserve` a opção como `false` (não-ID-Preserve), a configuração de segurança de criptografia SMB não será replicada para o destino. Nesse caso, as configurações de segurança do servidor CIFS no destino são definidas com os valores padrão. Se tiver ativado a encriptação SMB na SVM de origem, tem de ativar manualmente a encriptação SMB do servidor CIFS no destino.

Passos

1. Execute uma das seguintes ações:

Se pretender que a encriptação SMB necessária para o tráfego SMB de entrada no servidor CIFS seja...	Digite o comando...
Ativado	<pre>vserver cifs security modify -vserver vserver_name -is-smb-encryption -required true</pre>
Desativado	<pre>vserver cifs security modify -vserver vserver_name -is-smb-encryption -required false</pre>

2. Verifique se a criptografia SMB necessária no servidor CIFS está ativada ou desativada conforme desejado: `vserver cifs security show -vserver vserver_name -fields is-smb-encryption-required`

O `is-smb-encryption-required` campo é exibido `true` se a criptografia SMB necessária estiver ativada no servidor CIFS e `false` se estiver desativada.

Exemplo

O exemplo a seguir habilita a criptografia SMB necessária para o tráfego SMB de entrada para o servidor CIFS no SVM VS1:

```

cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-----
vs1      true

```

Determine se os clientes estão conectados usando sessões SMB criptografadas

Você pode exibir informações sobre sessões SMB conectadas para determinar se os clientes estão usando conexões SMB criptografadas. Isso pode ser útil para determinar se as sessões de cliente SMB estão se conectando com as configurações de segurança desejadas.

Sobre esta tarefa

As sessões de clientes SMB podem ter um dos três níveis de criptografia:

- unencrypted

A sessão SMB não está encriptada. Nem a criptografia no nível de máquina virtual de storage (SVM) nem no nível de compartilhamento são configuradas.

- partially-encrypted

A criptografia é iniciada quando ocorre a conexão em árvore. A criptografia no nível de compartilhamento está configurada. A criptografia no nível da SVM não está ativada.

- encrypted

A sessão SMB está totalmente encriptada. A criptografia no nível da SVM está ativada. A encriptação do nível de partilha pode ou não estar ativada. A configuração de criptografia no nível da SVM substitui a configuração de criptografia no nível de compartilhamento.

Passos

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre...	Digite o comando...
Sessões com uma configuração de criptografia especificada para sessões em um SVM especificado	<code>`vserver cifs session show -vserver vserver_name {unencrypted</code>
partially-encrypted	<code>encrypted} -instance`</code>

Se você quiser exibir informações sobre...	Digite o comando...
A configuração de criptografia para um Session ID específico em um SVM especificado	<code>vserver cifs session show -vserver <i>vserver_name</i> -session-id <i>integer</i> -instance</code>

Exemplos

O comando a seguir exibe informações detalhadas da sessão, incluindo a configuração de criptografia, em uma sessão SMB com um Session ID de 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: nodel
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted
```

Monitorar estatísticas de criptografia SMB

Você pode monitorar estatísticas de criptografia SMB e determinar quais sessões estabelecidas e conexões de compartilhamento são criptografadas e quais não são.

Sobre esta tarefa

O `statistics` comando no nível avançado de privilégios fornece os seguintes contadores, que podem ser utilizados para monitorizar o número de sessões SMB encriptadas e partilhar ligações:

Nome do contador	Descrições
<code>encrypted_sessions</code>	Fornece o número de sessões criptografadas do SMB 3,0

Nome do contador	Descrições
<code>encrypted_share_connections</code>	Fornece o número de compartilhamentos criptografados nos quais uma conexão em árvore aconteceu
<code>rejected_unencrypted_sessions</code>	Fornece o número de configurações de sessão rejeitadas devido à falta de capacidade de criptografia do cliente
<code>rejected_unencrypted_shares</code>	Fornece o número de mapeamentos de compartilhamento rejeitados devido à falta de capacidade de criptografia do cliente

Esses contadores estão disponíveis com os seguintes objetos estatísticos:

- `cifs` Permite monitorizar a encriptação SMB para todas as sessões SMB 3,0.

As estatísticas SMB 3,0 são incluídas na saída para o `cifs` objeto. Se você quiser comparar o número de sessões criptografadas com o número total de sessões, você pode comparar a saída para o contador com a saída `established_sessions` para `encrypted_sessions` o contador.

Se você quiser comparar o número de conexões de compartilhamento criptografadas com o número total de conexões de compartilhamento, você pode comparar a saída para o contador com a saída `connected_shares` para `encrypted_share_connections` o contador.

- `rejected_unencrypted_sessions` Fornece o número de vezes que uma tentativa foi feita para estabelecer uma sessão SMB que requer criptografia de um cliente que não suporta criptografia SMB.
- `rejected_unencrypted_shares` Fornece o número de vezes que uma tentativa foi feita para se conectar a um compartilhamento SMB que requer criptografia de um cliente que não suporta criptografia SMB.

Você deve iniciar uma coleta de amostras de estatísticas antes de poder visualizar os dados resultantes. 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.

Passos

1. Defina o nível de privilégio como avançado `set -privilege advanced`
2. Iniciar uma coleta de dados `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]`

Se você não especificar o `-sample-id` parâmetro, o comando gera um identificador de amostra para você e define esse exemplo como a amostra padrão para a sessão CLI. O valor para `-sample-id` é uma cadeia de texto. Se você executar esse comando durante a mesma sessão CLI e não especificar o `-sample-id` parâmetro, o comando sobrescreverá a amostra padrão anterior.

Opcionalmente, você pode especificar o nó no qual deseja coletar estatísticas. Se você não especificar o nó, a amostra coletará estatísticas para todos os nós no cluster.

3. Use o `statistics stop` comando para parar de coletar dados para a amostra.

4. Exibir estatísticas de criptografia SMB:

Se você quiser ver informações para...	Digite...
Sessões criptografadas	<code>`show -sample-id <i>sample_ID</i> -counter encrypted_sessions</code>
<code><i>node_name</i> [-node <i>node_name</i>]</code>	Sessões criptografadas e sessões estabelecidas
<code>`show -sample-id <i>sample_ID</i> -counter encrypted_sessions</code>	<code>established_sessions</code>
<code><i>node_name</i> [-node <i>node_name</i>]</code>	Conexões de compartilhamento criptografadas
<code>`show -sample-id <i>sample_ID</i> -counter encrypted_share_connections</code>	<code><i>node_name</i> [-node <i>node_name</i>]</code>
Conexões de compartilhamento criptografadas e compartilhamentos conectados	<code>`show -sample-id <i>sample_ID</i> -counter encrypted_share_connections</code>
<code>connected_shares</code>	<code><i>node_name</i> [-node <i>node_name</i>]</code>
Sessões não criptografadas rejeitadas	<code>`show -sample-id <i>sample_ID</i> -counter rejected_unencrypted_sessions</code>
<code><i>node_name</i> [-node <i>node_name</i>]</code>	Conexões de compartilhamento não criptografadas rejeitadas
<code>`show -sample-id <i>sample_ID</i> -counter rejected_unencrypted_share</code>	<code><i>node_name</i> [-node <i>node_name</i>]</code>

Se você quiser exibir informações apenas para um único nó, especifique o parâmetro opcional `-node`.

5. Voltar para o nível de privilégio de administrador `set -privilege admin`

Exemplos

O exemplo a seguir mostra como você pode monitorar as estatísticas de criptografia SMB 3,0 na máquina virtual de armazenamento (SVM) VS1.

O seguinte comando move-se para o nível de privilégio avançado:

```
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
```

O comando a seguir inicia a coleta de dados para uma nova amostra:

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

O comando a seguir interrompe a coleta de dados para essa amostra:

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

O comando a seguir mostra sessões criptografadas SMB e sessões estabelecidas SMB pelo nó da amostra:

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name -node node_name
```

```
Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2
```

Counter	Value
-----	-----
established_sessions	1
encrypted_sessions	1

2 entries were displayed

O comando a seguir mostra o número de sessões SMB não criptografadas rejeitadas pelo nó da amostra:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions -node node_name
```

```
Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2
```

Counter	Value
-----	-----
rejected_unencrypted_sessions	1

1 entry was displayed.

O comando a seguir mostra o número de compartilhamentos SMB conectados e compartilhamentos SMB criptografados pelo nó da amostra:

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2
```

Counter	Value
connected_shares	2
encrypted_share_connections	1

2 entries were displayed.

O comando a seguir mostra o número de conexões de compartilhamento SMB não criptografadas rejeitadas pelo nó da amostra:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2
```

Counter	Value
rejected_unencrypted_shares	1

1 entry was displayed.

Informações relacionadas

[Determinando quais objetos e contadores de estatísticas estão disponíveis](#)

["Visão geral do gerenciamento e monitoramento de desempenho"](#)

Comunicação de sessão LDAP segura

Conceitos de assinatura e vedação LDAP

A partir do ONTAP 9, você pode configurar a assinatura e a vedação para habilitar a segurança da sessão LDAP em consultas para um servidor AD (active Directory). Você

deve configurar as configurações de segurança do servidor CIFS na máquina virtual de armazenamento (SVM) para corresponder às do servidor LDAP.

A assinatura confirma a integridade dos dados de carga útil LDAP usando tecnologia de chave secreta. A vedação criptografa os dados de carga útil LDAP para evitar a transmissão de informações confidenciais em texto não criptografado. Uma opção *LDAP Security Level* indica se o tráfego LDAP precisa ser assinado, assinado e selado, ou não. A predefinição é *none*.

A assinatura LDAP e a vedação no tráfego CIFS são ativadas no SVM com a `-session-security-for-ad-ldap` opção de `vserver cifs security modify` comando.

Ative a assinatura LDAP e a vedação no servidor CIFS

Antes que o servidor CIFS possa usar assinatura e vedação para comunicação segura com um servidor LDAP do ativo Directory, você deve modificar as configurações de segurança do servidor CIFS para habilitar a assinatura e a vedação LDAP.

Antes de começar

Você deve consultar o administrador do servidor AD para determinar os valores de configuração de segurança apropriados.

Passos

1. Configure a configuração de segurança do servidor CIFS que permite o tráfego assinado e selado com servidores LDAP do ativo Directory: `vserver cifs security modify -vserver vserver_name -session-security-for-ad-ldap {none|sign|seal}`

Você pode ativar assinatura (*sign*, integridade de dados), assinatura e vedação (*seal*, integridade e criptografia de dados) ou nenhum *none*, sem assinatura ou vedação). O valor padrão é *none*.

2. Verifique se a configuração de segurança de assinatura e vedação LDAP está definida corretamente: `vserver cifs security show -vserver vserver_name`



Se o SVM usar o mesmo servidor LDAP para consultar o mapeamento de nomes ou outras informações do UNIX, como usuários, grupos e netgroups, você deverá ativar a configuração correspondente com `-session-security` a opção do `vserver services name-service ldap client modify` comando.

Configurar LDAP em TLS

Exporte uma cópia do certificado de CA raiz autoassinado

Para usar LDAP em SSL/TLS para proteger a comunicação do ativo Directory, primeiro você deve exportar uma cópia do certificado CA raiz autoassinado do ativo Directory Service para um arquivo de certificado e convertê-lo em um arquivo de texto ASCII. Esse arquivo de texto é usado pelo ONTAP para instalar o certificado na máquina virtual de storage (SVM).

Antes de começar

O Serviço de certificados do ativo Directory já deve estar instalado e configurado para o domínio ao qual o servidor CIFS pertence. Você pode encontrar informações sobre a instalação e configuração dos Serviços de

certificados do ativo diretor consultando a Biblioteca Microsoft TechNet.

["Microsoft TechNet Library: technet.microsoft.com"](https://technet.microsoft.com)

Passo

1. Obtenha um certificado de CA raiz do controlador de domínio que está no `.pem` formato de texto.

["Microsoft TechNet Library: technet.microsoft.com"](https://technet.microsoft.com)

Depois de terminar

Instale o certificado no SVM.

Informações relacionadas

["Microsoft TechNet Library"](#)

Instale o certificado de CA raiz autoassinado no SVM

Se a autenticação LDAP com TLS for necessária ao vincular a servidores LDAP, primeiro você deverá instalar o certificado de CA raiz autoassinado no SVM.

Sobre esta tarefa

Quando o LDAP sobre TLS está ativado, o cliente LDAP do ONTAP no SVM não oferece suporte a certificados revogados no ONTAP 9.0 e 9.1.

A partir do ONTAP 9.2, todos os aplicativos do ONTAP que usam comunicações TLS podem verificar o status do certificado digital usando o protocolo OCSP (Online Certificate Status Protocol). Se o OCSP estiver ativado para LDAP através de TLS, os certificados revogados serão rejeitados e a conexão falhará.

Passos

1. Instale o certificado CA raiz autoassinado:
 - a. Inicie a instalação do certificado: `security certificate install -vserver vserver_name -type server-ca`

A saída do console exibe a seguinte mensagem: `Please enter Certificate: Press <Enter> when done`
 - b. Abra o arquivo de certificado `.pem` com um editor de texto, copie o certificado, incluindo as linhas que começam com `-----BEGIN CERTIFICATE-----` e terminam com `-----END CERTIFICATE-----`, e cole o certificado após o prompt de comando.
 - c. Verifique se o certificado é exibido corretamente.
 - d. Conclua a instalação pressionando Enter.
2. Verifique se o certificado está instalado: `security certificate show -vserver vserver_name`

Ative LDAP através de TLS no servidor

Antes que o servidor SMB possa usar TLS para comunicação segura com um servidor LDAP do ativo Directory, você deve modificar as configurações de segurança do servidor SMB para ativar o LDAP sobre TLS.

A partir do ONTAP 9.10,1, a vinculação de canal LDAP é suportada por padrão para conexões LDAP do ativo

Directory (AD) e serviços de nome. O ONTAP tentará a vinculação de canais com conexões LDAP somente se o Start-TLS ou LDAPS estiver ativado junto com a segurança da sessão definida para assinar ou selar. Para desativar ou reativar a vinculação de canais LDAP com servidores AD, use o `-try-channel-binding-for-ad-ldap` parâmetro com o `vserver cifs security modify` comando.

Para saber mais, consulte:

- ["Visão geral da LDAP"](#)
- ["2020 requisitos de vinculação de canal LDAP e assinatura LDAP para Windows"](#).

Passos

1. Configure a configuração de segurança do servidor SMB que permite a comunicação LDAP segura com servidores LDAP do ativo Directory: `vserver cifs security modify -vserver vserver_name -use-start-tls-for-ad-ldap true`
2. Verifique se a configuração de segurança LDAP sobre TLS está definida como `true`: `vserver cifs security show -vserver vserver_name`



Se o SVM usar o mesmo servidor LDAP para consultar o mapeamento de nomes ou outras informações do UNIX (como usuários, grupos e netgroups), você também deve modificar a `-use-start-tls` opção usando o `vserver services name-service ldap client modify` comando.

Configure o SMB Multichannel para desempenho e redundância

A partir do ONTAP 9.4, você pode configurar o multicanais SMB para fornecer várias conexões entre o ONTAP e os clientes em uma única sessão SMB. Isso melhora a taxa de transferência e a tolerância a falhas.

Antes de começar

Você pode usar a funcionalidade de multicanal SMB somente quando os clientes negociam em versões SMB 3,0 ou posteriores. Por padrão, o SMB 3,0 e posterior está habilitado no servidor SMB do ONTAP.

Sobre esta tarefa

Os clientes SMB detetam e usam automaticamente várias conexões de rede se uma configuração adequada for identificada no cluster ONTAP.

O número de conexões simultâneas em uma sessão SMB depende das NICs que você implantou:

- **1G NICs em cliente e cluster ONTAP**

O cliente estabelece uma conexão por NIC e liga a sessão a todas as conexões.

- **10G e placas de rede de maior capacidade no cluster cliente e ONTAP**

O cliente estabelece até quatro conexões por NIC e liga a sessão a todas as conexões. O cliente pode estabelecer conexões em várias NICs de 10G GB e maior capacidade.

Você também pode modificar os seguintes parâmetros (privilegio avançado):

- `-max-connections-per-session`

O número máximo de conexões permitido por sessão multicanal. O padrão é 32 conexões.

Se você quiser habilitar mais conexões do que o padrão, você deve fazer ajustes comparáveis à configuração do cliente, que também tem um padrão de 32 conexões.

- `-max-lifs-per-session`

O número máximo de interfaces de rede anunciadas por sessão multicanal. O padrão é 256 interfaces de rede.

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Ative SMB Multichannel no servidor SMB:

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel  
-enabled true
```

3. Verifique se o ONTAP está relatando sessões multicanais SMB:

```
vserver cifs session show
```

4. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Exemplo

O exemplo a seguir exibe informações sobre todas as sessões SMB, mostrando várias conexões para uma única sessão:


```

cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                               Open
Idle
IDs      ID      Workstation      Windows User      Files
Time
-----
-----
138683,
138684,
138685    1      10.1.1.1      DOMAIN\
4s                                               Administrator
0

```

O exemplo a seguir exibe informações detalhadas sobre uma sessão SMB com session-id 1:

```

cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
Node: node1
Session ID: 1
Connection IDs: 138683,138684,138685
Connection Count: 3
Incoming Data LIF IP Address: 192.1.1.1
Workstation IP Address: 10.1.1.1
Authentication Mechanism: NTLMv1
User Authenticated as: domain-user
Windows User: DOMAIN\administrator
UNIX User: root
Open Shares: 2
Open Files: 5
Open Other: 0
Connected Time: 5s
Idle Time: 5s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
NetBIOS Name: -

```

Configure o usuário padrão do Windows para mapeamentos de usuários UNIX no servidor SMB

Configure o usuário UNIX padrão

Você pode configurar o usuário UNIX padrão para usar se todas as outras tentativas de mapeamento falharem para um usuário ou se não quiser mapear usuários individuais entre UNIX e Windows. Alternativamente, se você quiser que a autenticação de usuários não mapeados falhe, você não deve configurar o usuário UNIX padrão.

Sobre esta tarefa

Por padrão, o nome do usuário UNIX padrão é "pcuser", o que significa que, por padrão, o mapeamento de usuário para o usuário UNIX padrão está habilitado. Você pode especificar outro nome para usar como usuário UNIX padrão. O nome especificado deve existir nos bancos de dados do serviço de nomes configurados para a máquina virtual de storage (SVM). Se essa opção for definida como uma cadeia de caracteres nula, ninguém poderá acessar o servidor CIFS como um usuário padrão UNIX. Ou seja, cada usuário deve ter uma conta no banco de dados de senhas antes de poder acessar o servidor CIFS.

Para que um usuário se conecte ao servidor CIFS usando a conta de usuário UNIX padrão, o usuário deve atender aos seguintes pré-requisitos:

- O utilizador está autenticado.
- O usuário está no banco de dados de usuários do Windows local do servidor CIFS, no domínio doméstico do servidor CIFS ou em um domínio confiável (se pesquisas de mapeamento de nomes de vários domínios estiverem ativadas no servidor CIFS).
- O nome de usuário não é explicitamente mapeado para uma cadeia de caracteres nula.

Passos

1. Configure o usuário UNIX padrão:

Se você quiser ...	Introduza ...
Use o usuário padrão do UNIX "pcuser"	<pre>vserver cifs options modify -default -unix-user pcuser</pre>
Use outra conta de usuário UNIX como usuário padrão	<pre>vserver cifs options modify -default -unix-user user_name</pre>
Desative o usuário UNIX padrão	<pre>vserver cifs options modify -default -unix-user ""</pre>

```
vserver cifs options modify -default-unix-user pcuser
```

2. Verifique se o usuário UNIX padrão está configurado corretamente:

```
vserver cifs options show -vserver vserver_name
```

No exemplo a seguir, tanto o usuário UNIX padrão quanto o usuário UNIX convidado no SVM VS1 são configurados para usar o usuário UNIX "pcuser":

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : pcuser
Guest Unix User         : pcuser
Read Grants Exec       : disabled
Read Only Delete        : disabled
WINS Servers            : -
```

Configure o usuário UNIX convidado

Configurar a opção de usuário UNIX convidado significa que os usuários que fazem login de domínios não confiáveis são mapeados para o usuário UNIX convidado e podem se conectar ao servidor CIFS. Alternativamente, se você quiser que a autenticação de usuários de domínios não confiáveis falhe, você não deve configurar o usuário UNIX convidado. O padrão é não permitir que usuários de domínios não confiáveis se conectem ao servidor CIFS (a conta UNIX convidada não está configurada).

Sobre esta tarefa

Você deve ter em mente o seguinte ao configurar a conta UNIX Guest:

- Se o servidor CIFS não puder autenticar o usuário em um controlador de domínio para o domínio doméstico ou um domínio confiável ou o banco de dados local e essa opção estiver ativada, o servidor CIFS considera o usuário como um usuário convidado e mapeia o usuário para o usuário UNIX especificado.
- Se essa opção for definida como uma cadeia de caracteres nula, o usuário UNIX convidado será desativado.
- Você deve criar um usuário UNIX para usar como usuário UNIX convidado em um dos bancos de dados do serviço de nomes de máquina virtual de armazenamento (SVM).
- Um usuário conectado como um usuário convidado é automaticamente membro do grupo BUILTIN/convidados no servidor CIFS.
- A opção 'homedirs-public' aplica-se apenas a utilizadores autenticados. Um usuário conectado como um usuário convidado não tem um diretório home e não pode acessar os diretórios home de outros usuários.

Passos

1. Execute uma das seguintes ações:

Se você quiser...	Digite...
Configure o usuário UNIX convidado	<code>vserver cifs options modify -guest -unix-user <i>unix_name</i></code>
Desative o usuário UNIX convidado	<code>vserver cifs options modify -guest -unix-user ""</code>

```
vserver cifs options modify -guest-unix-user pcuser
```

2. Verifique se o usuário UNIX convidado está configurado corretamente: `vserver cifs options show -vserver vserver_name`

No exemplo a seguir, tanto o usuário UNIX padrão quanto o usuário UNIX convidado no SVM VS1 são configurados para usar o usuário UNIX "pcuser":

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

Client Session Timeout : 900
Default Unix Group     : -
Default Unix User      : pcuser
Guest Unix User        : pcuser
Read Grants Exec       : disabled
Read Only Delete       : disabled
WINS Servers           : -
```

Mapeie o grupo administrators para root

Se você tiver apenas clientes CIFS em seu ambiente e sua máquina virtual de storage (SVM) tiver sido configurada como um sistema de storage multiprotocolo, você deverá ter pelo menos uma conta do Windows que tenha privilégios de raiz para acessar arquivos no SVM; caso contrário, não será possível gerenciar o SVM porque não tem direitos de usuário suficientes.

Sobre esta tarefa

No entanto, se o sistema de armazenamento tiver sido configurado apenas para NTFS, o `/etc` diretório tem uma ACL no nível do ficheiro que permite ao grupo de administradores aceder aos ficheiros de configuração do ONTAP.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Configure a opção de servidor CIFS que mapeia o grupo de administradores para fazer root conforme apropriado:

Se você quiser...	Então...
Mapeie os membros do grupo de administradores para fazer root	<pre>vserver cifs options modify -vserver vserver_name -is-admin-users-mapped-to -root-enabled true</pre> Todas as contas do grupo administrators são consideradas root, mesmo que você não tenha uma <code>/etc/usermap.cfg</code> entrada mapeando as contas para root. Se você criar um arquivo usando uma conta que pertence ao grupo administrators, o arquivo será de propriedade do root quando você exibir o arquivo de um cliente UNIX.
Desative o mapeamento dos membros do grupo de administradores para fazer root	<pre>vserver cifs options modify -vserver vserver_name -is-admin-users-mapped-to -root-enabled false</pre> As contas no grupo administrators não são mais mapeadas para o root. Você só pode mapear explicitamente um único usuário para o root.

3. Verifique se a opção está definida para o valor desejado: `vserver cifs options show -vserver vserver_name`
4. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exiba informações sobre quais tipos de usuários estão conetados em sessões SMB

Você pode exibir informações sobre que tipo de usuários estão conetados em sessões SMB. Isso pode ajudar você a garantir que apenas o tipo apropriado de usuário esteja se conetando por sessões SMB na máquina virtual de storage (SVM).

Sobre esta tarefa

Os seguintes tipos de usuários podem se conetar através de sessões SMB:

- `local-user`

Autenticado como um usuário CIFS local

- `domain-user`

Autenticado como um usuário de domínio (do domínio doméstico do servidor CIFS ou de um domínio confiável)

- `guest-user`

Autenticado como usuário convidado

- `anonymous-user`

Autenticado como um usuário anônimo ou nulo

Passos

1. Determine que tipo de usuário está conectado em uma sessão SMB: `vserver cifs session show -vserver vserver_name -windows-user windows_user_name -fields windows-user,address,lif-address,user-type`

Se você quiser exibir informações de tipo de usuário para sessões estabelecidas...	Digite o seguinte comando...
Para todas as sessões com um tipo de usuário especificado	<code>`vserver cifs session show -vserver vserver_name -user-type {local-user</code>
domain-user	guest-user
anonymous-user}`	Para um usuário específico

Exemplos

O comando a seguir exibe informações de sessão sobre o tipo de usuário para sessões no SVM VS1 estabelecido pelo usuário "" iebubs user1":

```
cluster1::> vserver cifs session show -vserver publ -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node          vserver session-id connection-id lif-address  address
windows-user          user-type
-----
-----
publnode1 publ      1          3439441860    10.0.0.1     10.1.1.1
IEPUBS\user1          domain-user
```

Opções de comando para limitar o consumo excessivo de recursos do cliente Windows

As opções para o `vserver cifs options modify` comando permitem controlar o consumo de recursos para clientes Windows. Isso pode ser útil se algum cliente estiver fora dos limites normais de consumo de recursos, por exemplo, se houver um número excepcionalmente alto de arquivos abertos, sessões abertas ou solicitações Change Notify.

As seguintes opções para o `vserver cifs options modify` comando foram adicionadas para controlar o consumo de recursos do cliente Windows. Se o valor máximo de qualquer uma dessas opções for excedido, a solicitação será negada e uma mensagem EMS será enviada. Uma mensagem de aviso EMS também é enviada quando 80% do limite configurado para essas opções é atingido.

- `-max-opens-same-file-per-tree`

Número máximo de aberturas no mesmo arquivo por árvore CIFS

- `-max-same-user-sessions-per-connection`

Número máximo de sessões abertas pelo mesmo usuário por conexão

- `-max-same-tree-connect-per-session`

O número máximo de árvores se conecta no mesmo compartilhamento por sessão

- `-max-watches-set-per-tree`

Número máximo de relógios (também conhecido como *change notifica*) estabelecido por árvore

Consulte as páginas man para ver os limites padrão e para exibir a configuração atual.

A partir do ONTAP 9.4, os servidores que executam o SMB versão 2 ou posterior podem limitar o número de solicitações pendentes (*créditos SMB*) que o cliente pode enviar para o servidor em uma conexão SMB. O gerenciamento de créditos SMB é iniciado pelo cliente e controlado pelo servidor.

O número máximo de solicitações pendentes que podem ser concedidas em uma conexão SMB é controlado pela `-max-credits` opção. O valor padrão para essa opção é 128.

Melhore o desempenho do cliente com os oplocks tradicionais e de leasing

Melhore o desempenho do cliente com a visão geral tradicional e dos oplocks de leasing

Os oplocks tradicionais (bloqueios oportunistas) e os oplocks de leasing permitem que um cliente SMB em determinados cenários de compartilhamento de arquivos execute o armazenamento em cache do lado do cliente de informações de leitura antecipada, gravação e bloqueio. Um cliente pode então ler ou gravar em um arquivo sem lembrar regularmente o servidor de que precisa de acesso ao arquivo em questão. Isso melhora o desempenho reduzindo o tráfego de rede.

Os calços de leasing são uma forma melhorada de oplocks disponíveis com o protocolo SMB 2,1 e posterior. Os locks permitem que um cliente obtenha e preserve o estado de cache do cliente em várias aberturas SMB originadas de si mesmo.

Os calços podem ser controlados de duas maneiras:

- Por uma propriedade share, usando o `vserver cifs share create` comando quando o compartilhamento é criado, ou o `vserver share properties` comando após a criação.
- Por uma propriedade de qtree, usando o `volume qtree create` comando quando a qtree é criada, ou os `volume qtree oplock` comandos após a criação.

Escreva considerações sobre perda de dados de cache ao usar os oplocks

Em algumas circunstâncias, se um processo tem um oplock exclusivo em um arquivo e um segundo processo tenta abrir o arquivo, o primeiro processo deve invalidar dados em cache e flush escreve e bloqueia. O cliente deve então abandonar o oplock e o acesso ao arquivo. Se houver uma falha de rede durante esse flush, os dados de gravação em cache podem ser perdidos.

- Possibilidades de perda de dados

Qualquer aplicativo que tenha dados gravados em cache pode perder esses dados sob o seguinte conjunto de circunstâncias:

- A conexão é feita usando SMB 1,0.
 - Tem um oplock exclusivo no arquivo.
 - É dito para interromper esse oplock ou fechar o arquivo.
 - Durante o processo de limpeza do cache de gravação, a rede ou o sistema de destino gera um erro.
- Erro de manipulação e conclusão de gravação

O cache em si não tem nenhum tratamento de erros - os aplicativos fazem. Quando o aplicativo faz uma gravação no cache, a gravação é sempre concluída. Se o cache, por sua vez, faz uma gravação no sistema de destino em uma rede, ele deve assumir que a gravação é concluída porque, se não fizer, os dados são perdidos.

Ative ou desative os oplocks ao criar compartilhamentos SMB

Oplocks permitem que os clientes bloqueiem arquivos e armazenem conteúdo de cache localmente, o que pode aumentar o desempenho para operações de arquivos. Os Oplocks são ativados em compartilhamentos SMB residentes em máquinas virtuais de armazenamento (SVMs). Em algumas circunstâncias, você pode querer desativar os oplocks. Você pode ativar ou desativar os oplocks em uma base de compartilhamento por compartilhamento.

Sobre esta tarefa

Se os oplocks estiverem ativados no volume que contém uma partilha, mas a propriedade de partilha de oplock para essa partilha estiver desativada, os oplocks serão desativados para essa partilha. A desativação de oplocks em um compartilhamento tem precedência sobre a configuração de volume de oplock. A desativação de oplocks na partilha desativa os oplocks oportunistas e de leasing.

Você pode especificar outras propriedades de compartilhamento além de especificar a propriedade de compartilhamento de oplock usando uma lista delimitada por vírgulas. Você também pode especificar outros parâmetros de compartilhamento.

Passos

1. Execute a ação aplicável:

Se você quiser...	Então...
<p>Ative os oplocks em um compartilhamento durante a criação de compartilhamento</p>	<p>Introduza o seguinte comando: <code>vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks, ...]</code></p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> Se desejar que o compartilhamento tenha apenas as propriedades padrão de compartilhamento, que são <code>oplocks</code>, <code>browsable</code> e <code>changenotify</code> ativadas, não será necessário especificar o <code>-share-properties</code> parâmetro ao criar um compartilhamento SMB. Se você quiser qualquer combinação de propriedades de compartilhamento diferente do padrão, especifique o <code>-share-properties</code> parâmetro com a lista de propriedades de compartilhamento a ser usada para esse compartilhamento.</p> </div>
<p>Desative os oplocks em um compartilhamento durante a criação de compartilhamento</p>	<p>Introduza o seguinte comando: <code>vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property, ...]</code></p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> Ao desativar os oplocks, você deve especificar uma lista de propriedades de compartilhamento ao criar o compartilhamento, mas não deve especificar a <code>oplocks</code> propriedade.</p> </div>

Informações relacionadas

[Ativar ou desativar os oplocks em compartilhamentos SMB existentes](#)

[Monitorização do estado de oplock](#)

Comandos para ativar ou desativar oplocks em volumes e qtrees

Oplocks permitem que os clientes bloqueiem arquivos e armazenem conteúdo de cache localmente, o que pode aumentar o desempenho para operações de arquivos. Você precisa saber os comandos para ativar ou desativar os oplocks em volumes ou qtrees. Você também deve saber quando você pode ativar ou desativar os oplocks em volumes e qtrees.

- Os calços são ativados em volumes por predefinição.
- Não é possível desativar os oplocks ao criar um volume.
- Você pode ativar ou desativar os oplocks em volumes existentes para SVMs a qualquer momento.
- Você pode ativar os oplocks em qtrees para SVMs.

A configuração do modo de oplock é uma propriedade da ID de qtree 0, a qtree padrão que todos os volumes têm. Se você não especificar uma configuração de oplock ao criar uma qtree, a qtree herdará a configuração de oplock do volume pai, que é habilitada por padrão. No entanto, se você especificar uma configuração de oplock na nova qtree, ela terá precedência sobre a configuração de oplock no volume.

Se você quiser...	Use este comando...
Ative os oplocks em volumes ou qtrees	<code>volume qtree oplocks com o -oplock-mode parâmetro definido como enable</code>
Desative os oplocks em volumes ou qtrees	<code>volume qtree oplocks com o -oplock-mode parâmetro definido como disable</code>

Informações relacionadas

[Monitorização do estado de oplock](#)

Ative ou desative os oplocks em compartilhamentos SMB existentes



Os Oplocks são ativados em compartilhamentos SMB em máquinas virtuais de armazenamento (SVMs) por padrão. Em algumas circunstâncias, você pode querer desativar os oplocks; alternativamente, se você tiver desabilitado previamente os oplocks em uma ação, você pode querer reativar os oplocks.

Sobre esta tarefa

Se os oplocks estiverem ativados no volume que contém uma partilha, mas a propriedade de partilha de oplock para essa partilha estiver desativada, os oplocks serão desativados para essa partilha. A desativação de oplocks em um compartilhamento tem precedência sobre a ativação de oplocks no volume. Desativar os oplocks na partilha, desativa os oplocks oportunistas e de leasing. Você pode ativar ou desativar os oplocks em compartilhamentos existentes a qualquer momento.

Passo

1. Execute a ação aplicável:

Se você quiser...	Então...
<p>Ative os oplocks em um compartilhamento modificando um compartilhamento existente</p>	<p>Introduza o seguinte comando: <code>vserver cifs share properties add -vserver <i>vserver_name</i> -share-name <i>share_name</i> -share-properties oplocks</code></p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  <p>Você pode especificar propriedades de compartilhamento adicionais a serem adicionadas usando uma lista delimitada por vírgulas.</p> </div> <p>As propriedades recém-adicionadas são anexadas à lista existente de propriedades de compartilhamento. Quaisquer propriedades de compartilhamento que você especificou anteriormente permanecem em vigor.</p>
<p>Desative os oplocks em um compartilhamento modificando um compartilhamento existente</p>	<p>Introduza o seguinte comando: <code>vserver cifs share properties remove -vserver <i>vserver_name</i> -share-name <i>share_name</i> -share-properties oplocks</code></p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  <p>Você pode especificar propriedades de compartilhamento adicionais para remover usando uma lista delimitada por vírgulas.</p> </div> <p>As propriedades de compartilhamento que você remove são excluídas da lista existente de propriedades de compartilhamento; no entanto, as propriedades de compartilhamento configuradas anteriormente que você não remove permanecem em vigor.</p>

Exemplos

O comando a seguir habilita os oplocks para o compartilhamento chamado "Engenharia" na máquina virtual de armazenamento (SVM, anteriormente conhecido como SVM) VS1:

```
cluster1::> vservers cifs share properties add -vservers vs1 -share-name
Engineering -share-properties oplocks
```

```
cluster1::> vservers cifs share properties show
```

Vserver	Share	Properties
vs1	Engineering	oplocks browsable changenotify showsnapshot

O comando a seguir desativa os oplocks para a ação chamada "Engenharia" no SVM VS1:

```
cluster1::> vservers cifs share properties remove -vservers vs1 -share-name
Engineering -share-properties oplocks
```

```
cluster1::> vservers cifs share properties show
```

Vserver	Share	Properties
vs1	Engineering	browsable changenotify showsnapshot

Informações relacionadas

[Ativar ou desativar os oplocks ao criar compartilhamentos SMB](#)

[Monitorização do estado de oplock](#)

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

Monitorar o status de oplock

Você pode monitorar e exibir informações sobre o status de oplock. Você pode usar essas informações para determinar quais arquivos têm oplocks, quais são o nível de oplock e o nível de estado de oplock e se o leasing de oplock é usado. Você também pode determinar informações sobre bloqueios que você pode precisar quebrar manualmente.

Sobre esta tarefa

Você pode exibir informações sobre todos os oplocks em forma de resumo ou em um formulário de lista detalhado. Você também pode usar parâmetros opcionais para exibir informações sobre um subconjunto menor de bloqueios existentes. Por exemplo, você pode especificar que a saída retorna apenas bloqueios com o endereço IP do cliente especificado ou com o caminho especificado.

Você pode exibir as seguintes informações sobre os oplocks tradicionais e de leasing:

- SVM, nó, volume e LIF em que o oplock
- Bloquear UUID
- Endereço IP do cliente com o oplock
- Caminho no qual o oplock é estabelecido
- Protocolo de bloqueio (SMB) e tipo (oplock)
- Estado de bloqueio
- Nível do calço
- Estado da conexão e tempo de expiração do SMB
- Abra o ID do grupo se for concedida uma locação de oplock

Consulte a `vserver oplocks show` página de manual para obter uma descrição detalhada de cada parâmetro.

Passos

1. Apresentar o estado de oplock utilizando o `vserver locks show` comando.

Exemplos

O comando a seguir exibe informações padrão sobre todos os bloqueios. O oplock no ficheiro apresentado é concedido com um `read-batch` nível de oplock:

```
cluster1::> vserver locks show

Vserver: vs0
Volume   Object Path           LIF           Protocol   Lock Type   Client
-----
voll1    /voll1/notes.txt      node1_data1   cifs       share-level 192.168.1.5
        Sharelock Mode: read_write-deny_delete
        Oplock Level: read-batch
        op-lock    192.168.1.5
```

O exemplo a seguir exibe informações mais detalhadas sobre o bloqueio em um arquivo com o `/data2/data2_2/intro.pptx` caminho . Um leasing de oplock é concedido no arquivo com um `batch` nível de oplock a um cliente com um endereço IP de `10.3.1.3`:



Ao exibir informações detalhadas, o comando fornece saída separada para informações de oplock e sharelock. Este exemplo mostra apenas a saída da secção de oplock

```

cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx

      Vserver: vs1
      Volume: data2_2
Logical Interface: lif2
      Object Path: /data2/data2_2/intro.pptx
      Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
      Lock Protocol: cifs
      Lock Type: op-lock
Node Holding Lock State: node3
      Lock State: granted
Bytelock Starting Offset: -
  Number of Bytes Locked: -
  Bytelock is Mandatory: -
  Bytelock is Exclusive: -
  Bytelock is Superlock: -
    Bytelock is Soft: -
      Oplock Level: batch
Shared Lock Access Mode: -
  Shared Lock is Soft: -
    Delegation Type: -
      Client Address: 10.3.1.3
      SMB Open Type: -
      SMB Connect State: connected
SMB Expiration Time (Secs): -
      SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

```

Informações relacionadas

[Ativar ou desativar os oplocks ao criar compartilhamentos SMB](#)

[Ativar ou desativar os oplocks em compartilhamentos SMB existentes](#)

[Comandos para ativar ou desativar oplocks em volumes e qtrees](#)

Aplique objetos de Diretiva de Grupo a servidores SMB

Aplicar objetos de Diretiva de Grupo à visão geral dos servidores SMB

Seu servidor SMB oferece suporte a objetos de Diretiva de Grupo (GPOs), um conjunto de regras conhecidas como *atributos de diretiva de grupo* que se aplicam a computadores em um ambiente do active Directory. Você pode usar GPOs para gerenciar centralmente as configurações de todas as máquinas virtuais de storage (SVMs) no cluster que pertence ao mesmo domínio do active Directory.

Quando os GPOs estão ativados no servidor SMB, o ONTAP envia consultas LDAP ao servidor do active

Directory solicitando informações de GPO. Se houver definições de GPO aplicáveis ao servidor SMB, o servidor do ativo Directory retornará as seguintes informações de GPO:

- Nome GPO
- Versão GPO atual
- Localização da definição GPO
- Listas de UUIDs (identificadores universalmente exclusivos) para conjuntos de políticas GPO

Informações relacionadas

[Protegendo o acesso aos arquivos usando o controle de acesso dinâmico \(DAC\)](#)

["Auditoria de SMB e NFS e rastreamento de segurança"](#)

GPOs compatíveis

Embora nem todos os objetos de Diretiva de Grupo (GPOs) sejam aplicáveis às máquinas virtuais de storage (SVMs) habilitadas para CIFS, os SVMs podem reconhecer e processar o conjunto relevante de GPOs.

Os GPOs a seguir são compatíveis atualmente com SVMs:

- Definições avançadas de configuração da política de auditoria:

Acesso a objetos: Preparação da Política de Acesso Central

Especifica o tipo de eventos a serem auditados para o estadiamento da política de acesso central (CAP), incluindo as seguintes configurações:

- Não faça auditoria
- Audite apenas eventos de sucesso
- Auditar apenas eventos de falha
- Audite eventos de sucesso e falha



Se qualquer uma das três opções de auditoria estiver definida (auditar apenas eventos de sucesso, auditar apenas eventos de falha, auditar eventos de sucesso e falha), o ONTAP fará a auditoria de eventos de sucesso e falha.

Defina utilizando a `Audit Central Access Policy Staging` definição no `Advanced Audit Policy Configuration/Audit Policies/Object Access GPO`.



Para usar configurações avançadas de GPO de diretiva de auditoria, a auditoria deve ser configurada no SVM habilitado para CIFS ao qual você deseja aplicar essas configurações. Se a auditoria não estiver configurada no SVM, as configurações do GPO não serão aplicadas e serão descartadas.

- Definições do registro:
 - Intervalo de atualização da política de grupo para SVM habilitado para CIFS

Defina utilizando o `Registry GPO`.

- Atualizar desvio aleatório da política de grupo

Defina utilizando o `Registry GPO`.

- Publicação hash para BranchCache

A publicação Hash para o GPO BranchCache corresponde ao modo de operação BranchCache. Os três modos de operação suportados a seguir são suportados:

- Por compartilhamento
- Todos os compartilhamentos
- Desativado definido utilizando o `Registry GPO`.

- Suporte à versão hash para BranchCache

As seguintes três configurações de versão hash são suportadas:

- BranchCache versão 1
- BranchCache versão 2
- BranchCache versões 1 e 2 definidas usando o `Registry GPO`.



Para usar as configurações de GPO do BranchCache, o BranchCache deve ser configurado no SVM habilitado para CIFS ao qual você deseja aplicar essas configurações. Se o BranchCache não estiver configurado no SVM, as configurações do GPO não serão aplicadas e serão descartadas.

- Definições de segurança

- Política de auditoria e log de eventos

- Audite eventos de logon

Especifica o tipo de eventos de logon a serem auditados, incluindo as seguintes configurações:

- Não faça auditoria
- Audite apenas eventos de sucesso
- Auditoria em eventos de falha
- Audite eventos de sucesso e falha definidos usando a `Audit logon events` configuração no `Local Policies/Audit Policy GPO`.



Se qualquer uma das três opções de auditoria estiver definida (auditar apenas eventos de sucesso, auditar apenas eventos de falha, auditar eventos de sucesso e falha), o ONTAP fará a auditoria de eventos de sucesso e falha.

- Auditar o acesso a objeto

Especifica o tipo de acesso a objeto a ser auditado, incluindo as seguintes configurações:

- Não faça auditoria
- Audite apenas eventos de sucesso
- Auditoria em eventos de falha

- Audite eventos de sucesso e falha definidos usando a `Audit object access` configuração no `Local Policies/Audit Policy GPO`.



Se qualquer uma das três opções de auditoria estiver definida (auditar apenas eventos de sucesso, auditar apenas eventos de falha, auditar eventos de sucesso e falha), o ONTAP fará a auditoria de eventos de sucesso e falha.

- Método de retenção de log

Especifica o método de retenção do log de auditoria, incluindo as seguintes configurações:

- Substituir o registo de eventos quando o tamanho do ficheiro de registo exceder o tamanho máximo do registo
- Não substituir o registo de eventos (limpar registo manualmente) definido utilizando a `Retention method for security log` definição no `Event Log GPO`.

- Tamanho máximo do registo

Especifica o tamanho máximo do log de auditoria.

Defina utilizando a `Maximum security log size` definição no `Event Log GPO`.



Para usar a diretiva de auditoria e as configurações de GPO de log de eventos, a auditoria deve ser configurada no SVM habilitado para CIFS ao qual você deseja aplicar essas configurações. Se a auditoria não estiver configurada no SVM, as configurações do GPO não serão aplicadas e serão descartadas.

- Segurança do sistema de arquivos

Especifica uma lista de arquivos ou diretórios nos quais a segurança de arquivos é aplicada por meio de um GPO.

Defina utilizando o `File System GPO`.



O caminho do volume para o qual o GPO de segurança do sistema de arquivos está configurado deve existir na SVM.

- Política Kerberos

- Inclinação máxima do relógio

Especifica a tolerância máxima em minutos para a sincronização do relógio do computador.

Defina utilizando a `Maximum tolerance for computer clock synchronization` definição no `Account Policies/Kerberos Policy GPO`.

- Idade máxima do bilhete

Especifica a vida útil máxima em horas para o ticket de usuário.

Defina utilizando a `Maximum lifetime for user ticket` definição no `Account Policies/Kerberos Policy GPO`.

- Idade máxima de renovação do bilhete

Especifica o tempo de vida máximo em dias para a renovação do ticket do usuário.

Defina utilizando a `Maximum lifetime for user ticket renewal` definição no `Account Policies/Kerberos Policy` GPO.

- Atribuição de direitos de utilizador (direitos de privilégio)

- Assuma a propriedade

Especifica a lista de usuários e grupos que têm o direito de assumir a propriedade de qualquer objeto que possa ser protegido.

Defina utilizando a `Take ownership of files or other objects` definição no `Local Policies/User Rights Assignment` GPO.

- Privilégio de segurança

Especifica a lista de usuários e grupos que podem especificar opções de auditoria para acesso a objetos de recursos individuais, como arquivos, pastas e objetos do `Active Directory`.

Defina utilizando a `Manage auditing and security log` definição no `Local Policies/User Rights Assignment` GPO.

- Privilégio `Change Notify` (verificação de desvio transversal)

Especifica a lista de usuários e grupos que podem atravessar árvores de diretório, mesmo que os usuários e grupos possam não ter permissões no diretório atravessado.

O mesmo privilégio é necessário para que os usuários recebam notificações de alterações em arquivos e diretórios. Defina utilizando a `Bypass traverse checking` definição no `Local Policies/User Rights Assignment` GPO.

- Valores do registo

- Definição de assinatura necessária

Especifica se a assinatura SMB necessária está ativada ou desativada.

Defina utilizando a `Microsoft network server: Digitally sign communications (always)` definição no `Security Options` GPO.

- Restringir o anonimato

Especifica quais são as restrições para usuários anônimos e inclui as seguintes três configurações de GPO:

- Sem enumeração de contas SAM (Security Account Manager):

Esta configuração de segurança determina quais permissões adicionais são concedidas para conexões anônimas ao computador. Esta opção é apresentada como `no-enumeration` no `ONTAP` se estiver ativada.

Defina utilizando a `Network access: Do not allow anonymous enumeration of SAM`

accounts **definição** no Local Policies/Security Options GPO.

- **Nenhuma enumeração de contas e compartilhamentos SAM**

Esta configuração de segurança determina se a enumeração anônima de contas e compartilhamentos SAM é permitida. Esta opção é apresentada como no-enumeration no ONTAP se estiver ativada.

Defina utilizando a Network access: Do not allow anonymous enumeration of SAM accounts and shares **definição** no Local Policies/Security Options GPO.

- **Restringir o acesso anônimo a compartilhamentos e pipes nomeados**

Essa configuração de segurança restringe o acesso anônimo a compartilhamentos e pipes. Esta opção é apresentada como no-access no ONTAP se estiver ativada.

Defina utilizando a Network access: Restrict anonymous access to Named Pipes and Shares **definição** no Local Policies/Security Options GPO.

Ao exibir informações sobre políticas de grupo definidas e aplicadas, o Resultant restriction for anonymous user campo de saída fornece informações sobre a restrição resultante das três configurações de GPO anônimo restrito. As possíveis restrições resultantes são as seguintes:

- no-access

O usuário anônimo tem acesso negado aos compartilhamentos especificados e pipes nomeados e não pode usar enumeração de contas e compartilhamentos SAM. Esta restrição resultante é vista se o Network access: Restrict anonymous access to Named Pipes and Shares GPO estiver ativado.

- no-enumeration

O usuário anônimo tem acesso aos compartilhamentos especificados e pipes nomeados, mas não pode usar enumeração de contas e compartilhamentos SAM. Esta restrição resultante é vista se ambas as seguintes condições forem cumpridas:

- O Network access: Restrict anonymous access to Named Pipes and Shares GPO está desativado.
- Network access: Do not allow anonymous enumeration of SAM accounts`O ou os `Network access: Do not allow anonymous enumeration of SAM accounts and shares GPOs estão ativados.

- no-restriction

O usuário anônimo tem acesso total e pode usar enumeração. Esta restrição resultante é vista se ambas as seguintes condições forem cumpridas:

- O Network access: Restrict anonymous access to Named Pipes and Shares GPO está desativado.
- Network access: Do not allow anonymous enumeration of SAM accounts`Os GPOs e `Network access: Do not allow anonymous enumeration of SAM accounts and shares os GPOs estão desativados.

- Grupos restritos

Você pode configurar grupos restritos para gerenciar centralmente a associação de grupos internos ou definidos pelo usuário. Quando você aplica um grupo restrito por meio de uma política de grupo, a associação de um grupo local de servidor CIFS é definida automaticamente para corresponder às configurações da lista de membros definidas na política de grupo aplicada.

Defina utilizando o `Restricted Groups GPO`.

- Definições da política de acesso central

Especifica uma lista de políticas de acesso central. As políticas de acesso central e as regras de política de acesso central associadas determinam permissões de acesso para vários arquivos no SVM.

Informações relacionadas

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

[Protegendo o acesso aos arquivos usando o controle de acesso dinâmico \(DAC\)](#)

["Auditoria de SMB e NFS e rastreamento de segurança"](#)

[Modificação das configurações de segurança Kerberos do servidor CIFS](#)

[Usando o BranchCache para armazenar em cache conteúdo de compartilhamento SMB em uma filial](#)

[Utilizar a assinatura SMB para melhorar a segurança da rede](#)

[Configuração da verificação transversal de derivação](#)

[Configurando restrições de acesso para usuários anônimos](#)

Requisitos para usar GPOs com seu servidor SMB

Para usar objetos de diretiva de grupo (GPOs) com seu servidor SMB, o sistema deve atender a vários requisitos.

- O SMB deve ser licenciado no cluster. 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.
- Um servidor SMB deve ser configurado e Unido a um domínio do ative Directory do Windows.
- O status de administrador do servidor SMB deve estar ativado.
- Os GPOs devem ser configurados e aplicados à Unidade organizacional do ative Directory (ou) do Windows que contém o objeto de computador servidor SMB.
- O suporte ao GPO deve estar ativado no servidor SMB.

Ative ou desative o suporte de GPO em um servidor CIFS

Você pode ativar ou desativar o suporte de GPO (Group Policy Object) em um servidor CIFS. Se você habilitar o suporte a GPO em um servidor CIFS, os GPOs aplicáveis definidos na diretiva de grupo - a diretiva aplicada à unidade organizacional (ou) que contém o objeto computador servidor CIFS - serão aplicados ao servidor CIFS.



Sobre esta tarefa

Os GPOs não podem ser ativados em servidores CIFS no modo de grupo de trabalho.

Passos

1. Execute uma das seguintes ações:

Se você quiser...	Digite o comando...
Ativar GPOs	<code>vserver cifs group-policy modify -vserver vserver_name -status enabled</code>
Desativar GPOs	<code>vserver cifs group-policy modify -vserver vserver_name -status disabled</code>

2. Verifique se o suporte GPO está no estado desejado: `vserver cifs group-policy show -vserver +vserver_name_`

O status da Diretiva de Grupo para servidores CIFS no modo de grupo de trabalho é exibido como "habilitado".

Exemplo

O exemplo a seguir habilita o suporte a GPO na máquina virtual de storage (SVM) VS1:

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

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

          Vserver: vs1
Group Policy Status: enabled
```

Informações relacionadas

[GPOs compatíveis](#)

[Requisitos para usar GPOs com seu servidor CIFS](#)

[Como os GPOs são atualizados no servidor CIFS](#)

[Atualizar manualmente as definições de GPO no servidor CIFS](#)

[Exibindo informações sobre as configurações do GPO](#)

Como os GPOs são atualizados no servidor SMB

[Como os GPOs são atualizados na visão geral do servidor CIFS](#)

Por padrão, o ONTAP recupera e aplica alterações de Objeto de Diretiva de Grupo (GPO) a cada 90 minutos. As configurações de segurança são atualizadas a cada 16 horas. Se você quiser atualizar os GPOs para aplicar novas configurações de política de

GPO antes que o ONTAP as atualize automaticamente, você pode acionar uma atualização manual em um servidor CIFS com um comando ONTAP.

- Por padrão, todos os GPOs são verificados e atualizados conforme necessário a cada 90 minutos.

Este intervalo é configurável e pode ser definido utilizando as `Refresh interval` definições e `Random offset GPO`.

O ONTAP consulta o ativo Directory quanto a alterações nos GPOs. Se os números de versão do GPO registrados no ativo Directory forem maiores do que os do servidor CIFS, o ONTAP recuperará e aplicará os novos GPOs. Se os números de versão forem os mesmos, os GPOs no servidor CIFS não serão atualizados.

- Os GPOs são atualizados a cada 16 horas.

O ONTAP recupera e aplica GPOs de configurações de segurança a cada 16 horas, independentemente de estes GPOs terem sido alterados ou não.



O valor padrão de 16 horas não pode ser alterado na versão atual do ONTAP. É uma configuração padrão do cliente Windows.

- Todos os GPOs podem ser atualizados manualmente com um comando ONTAP.

Este comando simula o comando Windows `gpupdate.exe /force`.

Informações relacionadas

[Atualizar manualmente as definições de GPO no servidor CIFS](#)

Atualizar manualmente as definições de GPO no servidor CIFS

Se pretender atualizar imediatamente as definições do GPO (Group Policy Object) no servidor CIFS, pode atualizar manualmente as definições. Você pode atualizar apenas as configurações alteradas ou forçar uma atualização para todas as configurações, incluindo as configurações que foram aplicadas anteriormente, mas não foram alteradas.

Passo

1. Execute a ação apropriada:

Se você quiser atualizar...	Digite o comando...
Definições GPO alteradas	<pre>vserver cifs group-policy update -vserver vserver_name</pre>
Todas as definições do GPO	<pre>vserver cifs group-policy update -vserver vserver_name -force-reapply -all-settings true</pre>

Informações relacionadas

[Como os GPOs são atualizados no servidor CIFS](#)

Apresentar informações sobre as configurações do GPO

Você pode exibir informações sobre configurações de GPO (Group Policy Object) definidas no ativo Directory e sobre configurações GPO aplicadas ao servidor CIFS.

Sobre esta tarefa

Você pode exibir informações sobre todas as configurações de GPO definidas no ativo Directory do domínio ao qual o servidor CIFS pertence, ou você pode exibir informações apenas sobre as configurações de GPO aplicadas a um servidor CIFS.

Passos

1. Exiba informações sobre as configurações do GPO executando uma das seguintes ações:

Se você quiser exibir informações sobre todas as configurações de Diretiva de Grupo...	Digite o comando...
Definido no ativo Directory	<code>vserver cifs group-policy show-defined -vserver vserver_name</code>
Aplicado a uma máquina virtual de storage habilitada por CIFS (SVM)	<code>vserver cifs group-policy show-applied -vserver vserver_name</code>

Exemplo

O exemplo a seguir exibe as configurações de GPO definidas no ativo Directory ao qual pertence o SVM habilitado para CIFS chamado VS1:

```
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
Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
```

```
File Security:
  /voll/home
  /voll/dir1
Kerberos:
  Max Clock Skew: 5
  Max Ticket Age: 10
  Max Renew Age: 7
Privilege Rights:
  Take Ownership: usr1, usr2
  Security Privilege: usr1, usr2
  Change Notify: usr1, usr2
Registry Values:
  Signing Required: false
Restrict Anonymous:
  No enumeration of SAM accounts: true
  No enumeration of SAM accounts and shares: false
  Restrict anonymous access to shares and named pipes: true
  Combined restriction for anonymous user: no-access
Restricted Groups:
  gpr1
  gpr2
Central Access Policy Settings:
  Policies: cap1
           cap2

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
Security Settings:
  Event Audit and Event Log:
    Audit Logon Events: none
    Audit Object Access: success
    Log Retention Method: overwrite-as-needed
    Max Log Size: 16384
File Security:
  /voll/home
  /voll/dir1
Kerberos:
  Max Clock Skew: 5
```



```

    Max Ticket Age: 10
    Max Renew Age: 7
Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
Registry Values:
    Signing Required: false
Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
    Policies: cap1
             cap2

```

O exemplo a seguir exibe as configurações de GPO aplicadas ao SVM VS1 habilitado para CIFS:

```

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: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /voll/home

```

```
    /voll/dir1
Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
Registry Values:
    Signing Required: false
Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
    Policies: cap1
           cap2

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: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /voll/home
        /voll/dir1
Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
```

```
Privilege Rights:
  Take Ownership: usr1, usr2
  Security Privilege: usr1, usr2
  Change Notify: usr1, usr2
Registry Values:
  Signing Required: false
Restrict Anonymous:
  No enumeration of SAM accounts: true
  No enumeration of SAM accounts and shares: false
  Restrict anonymous access to shares and named pipes: true
  Combined restriction for anonymous user: no-access
Restricted Groups:
  gpr1
  gpr2
Central Access Policy Settings:
  Policies: cap1
           cap2
```

Informações relacionadas

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

Exibir informações detalhadas sobre GPOs de grupo restrito

Você pode exibir informações detalhadas sobre grupos restritos definidos como objetos de Diretiva de Grupo (GPOs) no ative Directory e aplicados ao servidor CIFS.

Sobre esta tarefa

Por padrão, as seguintes informações são exibidas:

- Nome da política de grupo
- Versão da política de grupo
- Link

Especifica o nível no qual a diretiva de grupo está configurada. Os possíveis valores de saída incluem o seguinte:

- `Local` Quando a política de grupo é configurada no ONTAP
 - `Site` quando a política de grupo é configurada no nível do site no controlador de domínio
 - `Domain` quando a política de grupo é configurada no nível do domínio no controlador de domínio
 - `OrganizationalUnit` Quando a política de grupo é configurada no nível de unidade organizacional (ou) no controlador de domínio
 - `RSOP` para o conjunto resultante de políticas derivadas de todas as políticas de grupo definidas em vários níveis
- Nome do grupo restrito
 - Os usuários e grupos que pertencem e que não pertencem ao grupo restrito

- A lista de grupos aos quais o grupo restrito é adicionado

Um grupo pode ser membro de grupos que não sejam os listados aqui.

Passo

1. Exiba informações sobre todos os GPOs de grupo restrito executando uma das seguintes ações:

Se você quiser exibir informações sobre todos os GPOs de grupo restrito...	Digite o comando...
Definido no ative Directory	<code>vserver cifs group-policy restricted-group show-defined -vserver vserver_name</code>
Aplicado a um servidor CIFS	<code>vserver cifs group-policy restricted-group show-applied -vserver vserver_name</code>

Exemplo

O exemplo a seguir exibe informações sobre GPOs de grupo restrito definidos no domínio do ative Directory ao qual pertence o SVM habilitado para CIFS chamado VS1:

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

```
Vserver: vs1
```

```
-----
```

```
Group Policy Name: gp01
Version: 16
Link: OrganizationalUnit
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9
```

```
Group Policy Name: Resultant Set of Policy
Version: 0
Link: RSOP
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9
```

O exemplo a seguir exibe informações sobre GPOs de grupos restritos aplicados ao SVM VS1 habilitado para CIFS:

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

```
Vserver: vs1
```

```
-----
```

```
Group Policy Name: gp01
Version: 16
Link: OrganizationalUnit
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9
```

```
Group Policy Name: Resultant Set of Policy
Version: 0
Link: RSOP
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9
```

Informações relacionadas

[Exibindo informações sobre as configurações do GPO](#)

Exibir informações sobre políticas de acesso centrais

Você pode exibir informações detalhadas sobre as políticas de acesso central definidas no Active Directory. Você também pode exibir informações sobre as políticas de acesso central aplicadas ao servidor CIFS por meio de objetos de diretiva de grupo (GPOs).

Sobre esta tarefa

Por padrão, as seguintes informações são exibidas:

- Nome do SVM
- Nome da política de acesso central
- SID
- Descrição
- Tempo de criação
- Tempo de modificação
- Regras dos membros



Os servidores CIFS no modo de grupo de trabalho não são exibidos porque não suportam GPOs.

Passo

1. Exiba informações sobre políticas de acesso central executando uma das seguintes ações:

Se você quiser exibir informações sobre todas as políticas de acesso central...	Digite o comando...
Definido no ative Directory	<code>vserver cifs group-policy central-access-policy show-defined -vserver vserver_name</code>
Aplicado a um servidor CIFS	<code>vserver cifs group-policy central-access-policy show-applied -vserver vserver_name</code>

Exemplo

O exemplo a seguir exibe informações de todas as políticas de acesso central definidas no ative Directory:

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver  Name          SID
-----  -
vs1      p1                S-1-17-3386172923-1132988875-3044489393-3993546205
        Description: policy #1
        Creation Time: Tue Oct 22 09:34:13 2013
        Modification Time: Wed Oct 23 08:59:15 2013
        Member Rules: r1

vs1      p2                S-1-17-1885229282-1100162114-134354072-822349040
        Description: policy #2
        Creation Time: Tue Oct 22 10:28:20 2013
        Modification Time: Thu Oct 31 10:25:32 2013
        Member Rules: r1
                   r2
```

O exemplo a seguir exibe informações de todas as políticas de acesso central aplicadas às máquinas virtuais de armazenamento (SVMs) no cluster:

```
cluster1::> vserver cifs group-policy central-access-policy show-applied
```

```
Vserver      Name                               SID
-----
-----
vs1          p1                                  S-1-17-3386172923-1132988875-3044489393-
3993546205
      Description: policy #1
      Creation Time: Tue Oct 22 09:34:13 2013
      Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1          p2                                  S-1-17-1885229282-1100162114-134354072-
822349040
      Description: policy #2
      Creation Time: Tue Oct 22 10:28:20 2013
      Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                  r2
```

Informações relacionadas

[Protegendo o acesso aos arquivos usando o controle de acesso dinâmico \(DAC\)](#)

[Exibindo informações sobre as configurações do GPO](#)

[Exibindo informações sobre as regras da política de acesso central](#)

Exibir informações sobre as regras da política de acesso central

Você pode exibir informações detalhadas sobre regras de política de acesso central associadas a políticas de acesso centrais definidas no Active Directory. Você também pode exibir informações sobre regras de políticas de acesso centrais aplicadas ao servidor CIFS por meio de GPOs de diretiva de acesso central (objetos de diretiva de grupo).

Sobre esta tarefa

Você pode exibir informações detalhadas sobre regras de política de acesso central definidas e aplicadas. Por padrão, as seguintes informações são exibidas:

- Nome do SVM
- Nome da regra de acesso central
- Descrição
- Tempo de criação
- Tempo de modificação
- Permissões atuais

- Permissões propostas
- Direcionar recursos

Se você quiser exibir informações sobre todas as regras de política de acesso central associadas às políticas de acesso central...	Digite o comando...
Definido no ative Directory	<code>vserver cifs group-policy central-access-rule show-defined -vserver vserver_name</code>
Aplicado a um servidor CIFS	<code>vserver cifs group-policy central-access-rule show-applied -vserver vserver_name</code>

Exemplo

O exemplo a seguir exibe informações de todas as regras de política de acesso central associadas às políticas de acesso central definidas no ative Directory:

```
cluster1::> vserver cifs group-policy central-access-rule show-defined
```

```
Vserver      Name
-----
vs1          r1
             Description: rule #1
             Creation Time: Tue Oct 22 09:33:48 2013
             Modification Time: Tue Oct 22 09:33:48 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1          r2
             Description: rule #2
             Creation Time: Tue Oct 22 10:27:57 2013
             Modification Time: Tue Oct 22 10:27:57 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

O exemplo a seguir exibe informações de todas as regras de política de acesso central associadas às políticas de acesso central aplicadas a máquinas virtuais de armazenamento (SVMs) no cluster:


```
cluster1::> vserver cifs group-policy central-access-rule show-applied
```

```
Vserver      Name
-----
vs1          r1
             Description: rule #1
             Creation Time: Tue Oct 22 09:33:48 2013
             Modification Time: Tue Oct 22 09:33:48 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1          r2
             Description: rule #2
             Creation Time: Tue Oct 22 10:27:57 2013
             Modification Time: Tue Oct 22 10:27:57 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

Informações relacionadas

[Protegendo o acesso aos arquivos usando o controle de acesso dinâmico \(DAC\)](#)

[Exibindo informações sobre as configurações do GPO](#)

[Exibindo informações sobre políticas de acesso central](#)

Comandos para gerenciar senhas de contas de computador de servidores SMB

Você precisa saber os comandos para alterar, redefinir e desativar senhas e para configurar agendas de atualização automática. Você também pode configurar um agendamento no servidor SMB para atualizá-lo automaticamente.

Se você quiser...	Use este comando...
Altere a senha da conta de domínio quando o ONTAP estiver sincronizado com os serviços do AD	<code>vserver cifs domain password change</code>
Redefina a senha da conta de domínio quando o ONTAP não estiver sincronizado com os serviços do AD	<code>vserver cifs domain password reset</code>
Configurar servidores SMB para alterações automáticas de senha de conta de computador	<code>vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true</code>

Se você quiser...	Use este comando...
Desativar alterações automáticas de senha de conta de computador em servidores SMB	<code>vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false</code>

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

Gerenciar conexões do controlador de domínio

Exibir informações sobre servidores descobertos

Você pode exibir informações relacionadas a servidores LDAP e controladores de domínio descobertos em seu servidor CIFS.

Passo

1. Para exibir informações relacionadas aos servidores descobertos, digite o seguinte comando: `vserver cifs domain discovered-servers show`

Exemplo

O exemplo a seguir mostra os servidores descobertos para o SVM VS1:

```
cluster1::> vserver cifs domain discovered-servers show
```

```
Node: node1
Vserver: vs1
```

Domain Name	Type	Preference	DC-Name	DC-Address	Status
example.com	MS-LDAP	adequate	DC-1	1.1.3.4	OK
example.com	MS-LDAP	adequate	DC-2	1.1.3.5	OK
example.com	MS-DC	adequate	DC-1	1.1.3.4	OK
example.com	MS-DC	adequate	DC-2	1.1.3.5	OK

Informações relacionadas

[Redefinir e redescobrir servidores](#)

[Parar ou iniciar o servidor CIFS](#)

Redefinir e redescobrir servidores

Redefinir e redescobrir servidores no servidor CIFS permite que o servidor CIFS descarte informações armazenadas sobre servidores LDAP e controladores de domínio. Depois de descartar as informações do servidor, o servidor CIFS readquire as informações atuais sobre esses servidores externos. Isso pode ser útil quando os servidores conectados não estão respondendo adequadamente.

Passos

1. Introduza o seguinte comando: `vserver cifs domain discovered-servers reset-servers -vserver vserver_name`
2. Exibir informações sobre os servidores recém-redescobertos: `vserver cifs domain discovered-servers show -vserver vserver_name`

Exemplo

O exemplo a seguir redefine e redescobre servidores para máquina virtual de armazenamento (SVM, anteriormente conhecido como SVM) VS1:

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver vs1
```

```
cluster1::> vserver cifs domain discovered-servers show
```

```
Node: node1  
Vserver: vs1
```

Domain Name	Type	Preference	DC-Name	DC-Address	Status
example.com	MS-LDAP	adequate	DC-1	1.1.3.4	OK
example.com	MS-LDAP	adequate	DC-2	1.1.3.5	OK
example.com	MS-DC	adequate	DC-1	1.1.3.4	OK
example.com	MS-DC	adequate	DC-2	1.1.3.5	OK

Informações relacionadas

[Exibindo informações sobre servidores descobertos](#)

[Parar ou iniciar o servidor CIFS](#)

Gerenciar a descoberta do controlador de domínio

A partir do ONTAP 9.3, você pode modificar o processo padrão pelo qual controladores de domínio (DCs) são descobertos. Isso permite limitar a descoberta ao seu site ou a um pool de DCs preferenciais, o que pode levar a melhorias de desempenho, dependendo do ambiente.

Sobre esta tarefa

Por padrão, o processo de descoberta dinâmica descobre todos os DCs disponíveis, incluindo todos os DCs preferenciais, todos os DCs no local e todos os DCs remotos. Essa configuração pode levar à latência na autenticação e ao acesso a compartilhamentos em determinados ambientes. Se você já determinou o pool de DCs que deseja usar, ou se os DCs remotos são inadequados ou inacessíveis, você pode alterar o método de descoberta.

No ONTAP 9.3 e versões posteriores, o `discovery-mode` parâmetro `cifs domain discovered-servers` do comando permite selecionar uma das seguintes opções de descoberta:

- Todos os DCs no domínio são descobertos.

- Apenas DCs no local são descobertos.

O `default-site` parâmetro para o servidor SMB pode ser definido para usar esse modo com LIFs que não são atribuídos a um site em sites e serviços.

- A detecção de servidor não é realizada, a configuração do servidor SMB depende apenas de DCs preferenciais.

Para utilizar este modo, tem de definir primeiro os DCs preferidos para o servidor SMB.

Antes de começar

Você deve estar no nível de privilégio avançado.

Passo

1. Especifique a opção de descoberta desejada: `vserver cifs domain discovered-servers discovery-mode modify -vserver vserver_name -mode {all|site|none}`

Opções para o `mode` parâmetro:

- `all`

Descubra todos os DCs disponíveis (padrão).

- `site`

Limite a descoberta DC ao seu site.

- `none`

Use apenas DCs preferenciais e não execute a descoberta.

Adicione controladores de domínio preferenciais

O ONTAP descobre automaticamente controladores de domínio através do DNS. Opcionalmente, você pode adicionar um ou mais controladores de domínio à lista de controladores de domínio preferenciais para um domínio específico.

Sobre esta tarefa

Se já existir uma lista de controlador de domínio preferencial para o domínio especificado, a nova lista será mesclada com a lista existente.

Passo

1. Para adicionar à lista de controladores de domínio preferenciais, digite o seguinte comando `vserver cifs domain preferred-dc add -vserver vserver_name -domain domain_name -preferred-dc IP_address, ...+`

`-vserver vserver_name` Especifica o nome da máquina virtual de storage (SVM).

`-domain domain_name` Especifica o nome totalmente qualificado do ative Directory do domínio ao qual pertencem os controladores de domínio especificados.

`-preferred-dc IP_address,...` especifica um ou mais endereços IP dos controladores de domínio preferidos, como uma lista delimitada por vírgulas, por ordem de preferência.

Exemplo

O comando a seguir adiciona controladores de domínio 172.17.102.25 e 172.17.102.24 à lista de controladores de domínio preferenciais que o servidor SMB no SVM VS1 usa para gerenciar o acesso externo ao domínio `cifs.lab.example.com`.

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

Informações relacionadas

[Comandos para gerenciar controladores de domínio preferenciais](#)

Comandos para gerenciar controladores de domínio preferenciais

Você precisa saber os comandos para adicionar, exibir e remover controladores de domínio preferenciais.

Se você quiser...	Use este comando...
Adicione um controlador de domínio preferido	<code>vserver cifs domain preferred-dc add</code>
Exibir controladores de domínio preferenciais	<code>vserver cifs domain preferred-dc show</code>
Remova um controlador de domínio preferido	<code>vserver cifs domain preferred-dc remove</code>

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

Informações relacionadas

[Adicionando controladores de domínio preferenciais](#)

Ative as conexões SMB2 aos controladores de domínio

A partir do ONTAP 9.1, você pode habilitar o SMB versão 2,0 para se conectar a um controlador de domínio. Isso é necessário se você desativou o SMB 1,0 em controladores de domínio. A partir do ONTAP 9.2, o SMB2 é ativado por predefinição.

Sobre esta tarefa

A `smb2-enabled-for-dc-connections` opção de comando ativa o padrão do sistema para o lançamento do ONTAP que você está usando. O padrão do sistema para o ONTAP 9.1 está ativado para o SMB 1,0 e desativado para o SMB 2,0. O padrão do sistema para o ONTAP 9.2 está habilitado para o SMB 1,0 e habilitado para o SMB 2,0. Se o controlador de domínio não puder negociar o SMB 2,0 inicialmente, ele usará o SMB 1,0.

O SMB 1,0 pode ser desativado do ONTAP para um controlador de domínio. No ONTAP 9.1, se o SMB 1,0 tiver sido desativado, o SMB 2,0 deve ser ativado para se comunicar com um controlador de domínio.

Saiba mais sobre:

- ["Verificando versões SMB ativadas"](#).
- ["Versões e funcionalidade SMB compatíveis"](#).



Se `-smb1-enabled-for-dc-connections` estiver definido como `false` enquanto `-smb1-enabled` estiver definido como `true`, o ONTAP nega conexões SMB 1,0 como cliente, mas continua a aceitar conexões SMB 1,0 de entrada como servidor.

Passos

1. Antes de alterar as configurações de segurança SMB, verifique quais versões SMB estão ativadas:
`vserver cifs security show`
2. Role a lista para baixo para ver as versões SMB.
3. Execute o comando apropriado, usando a `smb2-enabled-for-dc-connections` opção.

Se você quiser que SMB2 seja...	Digite o comando...
Ativado	<pre>vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc -connections true</pre>
Desativado	<pre>vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc -connections false</pre>

Ative conexões criptografadas para controladores de domínio

A partir do ONTAP 9.8, você pode especificar que as conexões aos controladores de domínio sejam criptografadas.

Sobre esta tarefa

O ONTAP requer criptografia para comunicações de controlador de domínio (DC) quando a `-encryption-required-for-dc-connection` opção está definida como `true`; o padrão é `false`. Quando a opção está definida, apenas o protocolo SMB3 será utilizado para ligações ONTAP-DC, uma vez que a encriptação é suportada apenas pelo SMB3.

Quando as comunicações CC criptografadas são necessárias, a `-smb2-enabled-for-dc-connections` opção é ignorada, porque o ONTAP negocia somente conexões SMB3. Se um DC não suportar SMB3 e criptografia, o ONTAP não se conetará a ele.

Passo

1. Ative a comunicação encriptada com o DC: `vserver cifs security modify -vserver svm_name -encryption-required-for-dc-connection true`

Use sessões nulas para acessar o armazenamento em ambientes não Kerberos

Use sessões nulas para acessar o armazenamento na visão geral de ambientes não Kerberos

O acesso de sessão nula fornece permissões para recursos de rede, como dados do sistema de armazenamento de dados, e para serviços baseados em cliente executados no sistema local. Uma sessão nula ocorre quando um processo de cliente usa a conta "system" para acessar um recurso de rede. A configuração de sessão nula é específica para autenticação não Kerberos.

Como o sistema de armazenamento fornece acesso nulo à sessão

Como compartilhamentos de sessão nulos não exigem autenticação, os clientes que exigem acesso de sessão null devem ter seus endereços IP mapeados no sistema de armazenamento.

Por padrão, os clientes de sessão nula não mapeados podem acessar determinados serviços do sistema ONTAP, como enumeração de compartilhamento, mas eles são restritos a acessar quaisquer dados do sistema de storage.



O ONTAP suporta os valores de configuração do Registro anônimo do Windows com a `-restrict-anonymous` opção. Isso permite controlar até que ponto os usuários nulos não mapeados podem exibir ou acessar recursos do sistema. Por exemplo, você pode desativar a enumeração de compartilhamento e o acesso ao compartilhamento IPC (o compartilhamento de pipe nomeado oculto). As `vserver cifs options modify` páginas de manual e `vserver cifs options show` fornecem mais informações sobre a `-restrict-anonymous` opção.

A menos que configurado de outra forma, um cliente executando um processo local que solicita acesso ao sistema de armazenamento por meio de uma sessão nula é membro apenas de grupos não restritivos, como "todos". Para limitar o acesso de sessão nula a recursos selecionados do sistema de armazenamento, você pode querer criar um grupo ao qual todos os clientes de sessão nula pertencem; a criação deste grupo permite restringir o acesso ao sistema de armazenamento e definir permissões de recursos do sistema de armazenamento que se aplicam especificamente a clientes de sessão nula.

O ONTAP fornece uma sintaxe de mapeamento no `vserver name-mapping` conjunto de comandos para especificar o endereço IP dos clientes que têm acesso permitido aos recursos do sistema de armazenamento usando uma sessão de usuário nula. Depois de criar um grupo para usuários nulos, você pode especificar restrições de acesso para recursos do sistema de armazenamento e permissões de recursos que se aplicam somente a sessões nulas. O usuário nulo é identificado como logon anônimo. Os usuários nulos não têm acesso a nenhum diretório home.

Qualquer usuário nulo que acesse o sistema de armazenamento a partir de um endereço IP mapeado recebe permissões de usuário mapeadas. Considere as precauções apropriadas para evitar o acesso não autorizado aos sistemas de armazenamento mapeados com usuários nulos. Para máxima proteção, coloque o sistema de armazenamento e todos os clientes que necessitem de acesso nulo ao sistema de armazenamento de utilizadores numa rede separada, para eliminar a possibilidade de "spoofing" de endereço IP.

Informações relacionadas

[Configurando restrições de acesso para usuários anônimos](#)

Conceder acesso a usuários nulos a compartilhamentos de sistema de arquivos

Você pode permitir o acesso aos recursos do seu sistema de armazenamento por clientes de sessão nulos, atribuindo um grupo a ser usado por clientes de sessão nulos e

registrando os endereços IP de clientes de sessão nulos para adicionar à lista de clientes com permissão para acessar dados usando sessões nulas.

Passos

1. Use o `vserver name-mapping create` comando para mapear o usuário nulo para qualquer usuário válido do Windows, com um qualificador IP.

O comando a seguir mapeia o usuário nulo para `user1` com um nome de host válido `google.com`:

```
vserver name-mapping create -direction win-unix -position 1 -pattern
"ANONYMOUS LOGON" -replacement user1 - hostname google.com
```

O comando a seguir mapeia o usuário nulo para `user1` com um endereço IP válido `10.238.2.54/32`:

```
vserver name-mapping create -direction win-unix -position 2 -pattern
"ANONYMOUS LOGON" -replacement user1 -address 10.238.2.54/32
```

2. Use o `vserver name-mapping show` comando para confirmar o mapeamento de nomes.

```
vserver name-mapping show

Vserver:    vs1
Direction: win-unix
Position Hostname      IP Address/Mask
-----
1          -            10.72.40.83/32      Pattern: anonymous logon
                                     Replacement: user1
```

3. Use o `vserver cifs options modify -win-name-for-null-user` comando para atribuir a associação do Windows ao usuário nulo.

Essa opção é aplicável somente quando há um mapeamento de nome válido para o usuário nulo.

```
vserver cifs options modify -win-name-for-null-user user1
```

4. Use o `vserver cifs options show` comando para confirmar o mapeamento do usuário nulo para o usuário ou grupo do Windows.

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```


Gerencie aliases NetBIOS para servidores SMB

Gerenciar aliases NetBIOS para servidores SMB

Os aliases NetBIOS são nomes alternativos para o servidor SMB que os clientes SMB podem usar ao se conectar ao servidor SMB. A configuração de aliases NetBIOS para um servidor SMB pode ser útil quando você está consolidando dados de outros servidores de arquivos para o servidor SMB e deseja que o servidor SMB responda aos nomes dos servidores de arquivos originais.

Você pode especificar uma lista de aliases NetBIOS ao criar o servidor SMB ou a qualquer momento depois de criar o servidor SMB. Você pode adicionar ou remover aliases NetBIOS da lista a qualquer momento. Você pode se conectar ao servidor SMB usando qualquer um dos nomes na lista de alias do NetBIOS.

Informações relacionadas

[Exibindo informações sobre NetBIOS sobre conexões TCP](#)

Adicione uma lista de aliases NetBIOS ao servidor SMB

Se você quiser que os clientes SMB se conectem ao servidor SMB usando um alias, você pode criar uma lista de aliases NetBIOS ou adicionar aliases NetBIOS a uma lista existente de aliases NetBIOS.

Sobre esta tarefa

- O nome de alias NetBIOS pode ter 15 até caracteres de comprimento.
- Você pode configurar até 200 aliases NetBIOS no servidor SMB.
- Não são permitidos os seguintes caracteres:
- `()[]|;: ", > / ?`

Passos

1. Adicione os aliases NetBIOS `vserver cifs add-netbios-aliases -vserver vserver_name -netbios-aliases NetBIOS_alias,...`

```
vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases
alias_1,alias_2,alias_3
```

- Você pode especificar um ou mais aliases NetBIOS usando uma lista delimitada por vírgulas.
- Os aliases NetBIOS especificados são adicionados à lista existente.
- Uma nova lista de aliases NetBIOS é criada se a lista estiver vazia no momento.

2. Verifique se os aliases NetBIOS foram adicionados corretamente: `vserver cifs show -vserver vserver_name -display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1
```

```
Server Name: CIFS_SERVER  
NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

Informações relacionadas

[Removendo aliases NetBIOS da lista de alias NetBIOS](#)

[Exibindo a lista de aliases NetBIOS em servidores CIFS](#)

Remova os aliases NetBIOS da lista de alias NetBIOS

Se você não precisar de aliases NetBIOS específicos para um servidor CIFS, você poderá remover esses aliases NetBIOS da lista. Você também pode remover todos os aliases NetBIOS da lista.

Sobre esta tarefa

Você pode remover mais de um alias NetBIOS usando uma lista delimitada por vírgulas. Você pode remover todos os aliases NetBIOS em um servidor CIFS especificando - como o valor para o `-netbios-aliases` parâmetro.

Passos

1. Execute uma das seguintes ações:

Se você quiser remover...	Digite...
Aliases NetBIOS específicos da lista	<pre>vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios -aliases _NetBIOS_alias_,...</pre>
Todos os aliases NetBIOS da lista	<pre>vserver cifs remove-netbios-aliases -vserver vserver_name -netbios-aliases -</pre>

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
```

2. Verifique se os aliases NetBIOS especificados foram removidos: `vserver cifs show -vserver vserver_name -display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1
```

```
Server Name: CIFS_SERVER  
NetBIOS Aliases: ALIAS_2, ALIAS_3
```

Exiba a lista de aliases NetBIOS em servidores CIFS

Você pode exibir a lista de aliases NetBIOS. Isso pode ser útil quando você deseja determinar a lista de nomes sobre os quais clientes SMB podem fazer conexões com o servidor CIFS.

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre...	Digite...
Os aliases NetBIOS de um servidor CIFS	<code>vserver cifs show -display-netbios -aliases</code>
A lista de aliases NetBIOS como parte das informações detalhadas do servidor CIFS	<code>vserver cifs show -instance</code>

O exemplo a seguir exibe informações sobre os aliases NetBIOS de um servidor CIFS:

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1  
  
    Server Name: CIFS_SERVER  
    NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

O exemplo a seguir exibe a lista de aliases NetBIOS como parte das informações detalhadas do servidor CIFS:

```
vserver cifs show -instance
```

```
                                Vserver: vs1  
                                CIFS Server NetBIOS Name: CIFS_SERVER  
                                NetBIOS Domain/Workgroup Name: EXAMPLE  
                                Fully Qualified Domain Name: EXAMPLE.COM  
Default Site Used by LIFs Without Site Membership:  
                                Authentication Style: domain  
                                CIFS Server Administrative Status: up  
                                CIFS Server Description:  
                                List of NetBIOS Aliases: ALIAS_1, ALIAS_2,  
ALIAS_3
```

Consulte a página de manual para obter mais informações.

Informações relacionadas

[Adicionando uma lista de aliases NetBIOS ao servidor CIFS](#)

Determine se os clientes SMB estão conectados usando aliases NetBIOS

Você pode determinar se os clientes SMB estão conectados usando aliases NetBIOS e, em caso afirmativo, qual alias NetBIOS é usado para fazer a conexão. Isso pode ser útil ao solucionar problemas de conexão.

Sobre esta tarefa

Você deve usar o `-instance` parâmetro para exibir o alias NetBIOS (se houver) associado a uma conexão SMB. Se o nome do servidor CIFS ou um endereço IP for usado para fazer a conexão SMB, a saída para o `NetBIOS Name` campo é `-` (hífen).

Passo

1. Execute a ação desejada:

Se você quiser exibir informações do NetBIOS para...	Digite...
Conexões SMB	<code>vserver cifs session show -instance</code>
Conexões usando um alias NetBIOS especificado:	<code>vserver cifs session show -instance -netbios-name <i>netbios_name</i></code>

O exemplo a seguir exibe informações sobre o alias NetBIOS usado para fazer a conexão SMB com o Session ID 1:

```
vserver cifs session show -session-id 1 -instance
```

```

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
Workstation: 10.2.2.50
Authentication Mechanism: NTLMv2
Windows User: EXAMPLE\user1
UNIX User: user1
Open Shares: 2
Open Files: 2
Open Other: 0
Connected Time: 1d 1h 10m 5s
Idle Time: 22s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: ALIAS1
SMB Encryption Status: Unencrypted

```

Gerenciar diversas tarefas de servidor SMB

Pare ou inicie o servidor CIFS

Você pode parar o servidor CIFS em uma SVM, que pode ser útil na execução de tarefas enquanto os usuários não acessam dados por compartilhamentos SMB. Você pode reiniciar o acesso SMB iniciando o servidor CIFS. Ao parar o servidor CIFS, você também pode modificar os protocolos permitidos na máquina virtual de storage (SVM).

Passos

1. Execute uma das seguintes ações:

Se você quiser...	Digite o comando...
Pare o servidor CIFS	<code>`vserver cifs stop -vserver <i>vserver_name</i> [-foreground {true</code>
<code>false}]`</code>	Inicie o servidor CIFS
<code>`vserver cifs start -vserver <i>vserver_name</i> [-foreground {true</code>	<code>false}]`</code>

`-foreground` especifica se o comando deve ser executado em primeiro plano ou em segundo plano. Se você não inserir esse parâmetro, ele será definido como `true`, e o comando será executado em primeiro

plano.

2. Verifique se o status administrativo do servidor CIFS está correto usando o `vserver cifs show` comando.

Exemplo

Os comandos a seguir iniciam o servidor CIFS no SVM VS1:

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

                                Vserver: vs1
                                CIFS Server NetBIOS Name: VS1
                                NetBIOS Domain/Workgroup Name: DOMAIN
                                Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
                                Authentication Style: domain
                                CIFS Server Administrative Status: up
```

Informações relacionadas

[Exibindo informações sobre servidores descobertos](#)

[Redefinir e redescobrir servidores](#)

Mova servidores CIFS para diferentes OUs

O processo de criação do servidor CIFS usa a unidade organizacional padrão (ou) CN de computadores durante a configuração, a menos que você especifique uma ou diferente. Você pode mover servidores CIFS para diferentes OUs após a configuração.

Passos

1. No servidor Windows, abra a árvore **usuários e computadores do ativo Directory**.
2. Localize o objeto do ativo Directory da máquina virtual de storage (SVM).
3. Clique com o botão direito do rato no objeto e selecione **mover**.
4. Selecione a UO que você deseja associar ao SVM

Resultados

O objeto SVM é colocado na UO selecionada.

Modifique o domínio DNS dinâmico na SVM antes de mover o servidor SMB

Se desejar que o servidor DNS integrado ao ativo Directory Registre dinamicamente os Registros DNS do servidor SMB no DNS ao mover o servidor SMB para outro domínio, você deve modificar DNS dinâmico (DDNS) na máquina virtual de armazenamento (SVM) antes de mover o servidor SMB.

Antes de começar

Os serviços de nomes DNS devem ser modificados no SVM para usar o domínio DNS que contém os Registros de localização do serviço para o novo domínio que conterá a conta de computador do servidor SMB. Se você estiver usando DDNS seguro, você deve usar servidores de nomes DNS integrados ao active Directory.

Sobre esta tarefa

Embora o DDNS (se configurado no SVM) adicione automaticamente os Registros DNS para LIFs de dados ao novo domínio, os Registros DNS para o domínio original não são excluídos automaticamente do servidor DNS original. Você deve excluí-los manualmente.

Para concluir as modificações do DDNS antes de mover o servidor SMB, consulte o seguinte tópico:

["Configurar serviços DNS dinâmicos"](#)

Ingressar em um SVM em um domínio do active Directory

É possível associar uma máquina virtual de armazenamento (SVM) a um domínio do active Directory sem excluir o servidor SMB existente, modificando o domínio usando o `vserver cifs modify` comando. Você pode ingressar novamente no domínio atual ou ingressar em um novo.

Antes de começar

- O SVM já deve ter uma configuração de DNS.
- A configuração DNS do SVM deve ser capaz de servir o domínio de destino.

Os servidores DNS têm de conter os registros de localização de serviço (SRV) para os servidores LDAP de domínio e controlador de domínio.

Sobre esta tarefa

- O status administrativo do servidor CIFS deve ser definido como "próprio" para prosseguir com a modificação de domínio do active Directory.
- Se o comando for concluído com êxito, o status administrativo será automaticamente definido como "up".
- Ao ingressar em um domínio, esse comando pode levar vários minutos para ser concluído.

Passos

1. Junte-se ao SVM ao domínio do servidor CIFS: `vserver cifs modify -vserver vserver_name -domain domain_name -status-admin down`

Para obter mais informações, consulte a página man para o `vserver cifs modify` comando. Se você precisar reconfigurar o DNS para o novo domínio, consulte a página de manual do `vserver dns modify` comando.

Para criar uma conta de máquina do active Directory para o servidor SMB, você deve fornecer o nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores ao `ou=example` ou contentor dentro do `example` domínio .com.

A partir do ONTAP 9.7, o administrador do AD pode fornecer um URI para um arquivo keytab como alternativa para fornecer um nome e uma senha para uma conta privilegiada do Windows. Quando receber o URI, inclua-o `-keytab-uri` no parâmetro com os `vserver cifs` comandos.

2. Verifique se o servidor CIFS está no domínio desejado do ativo Directory: `vserver cifs show`

Exemplo

No exemplo a seguir, o servidor SMB "CIFSSERVER1" no SVM VS1 junta o domínio `example.com` usando autenticação keytab:

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab
```

```
cluster1::> vserver cifs show
```

	Server	Status	Domain/Workgroup	Authentication
Vserver	Name	Admin	Name	Style
-----	-----	-----	-----	-----
vs1	CIFSSERVER1	up	EXAMPLE	domain

Exibir informações sobre NetBIOS sobre conexões TCP

Você pode exibir informações sobre conexões NetBIOS sobre TCP (NBT). Isso pode ser útil ao solucionar problemas relacionados ao NetBIOS.

Passo

1. Use o `vserver cifs nbtstat` comando para exibir informações sobre NetBIOS sobre conexões TCP.



O serviço de nomes NetBIOS (NBNS) em IPv6 não é suportado.

Exemplo

O exemplo a seguir mostra as informações do serviço de nomes NetBIOS exibidas para "cluster1":


```

cluster1::> vserver cifs nbtstat

Vserver: vs1
Node:    cluster1-01
Interfaces:
          10.10.10.32
          10.10.10.33
Servers:
          17.17.1.2 (active )
NBT Scope:
          [ ]
NBT Mode:
          [h]
NBT Name      NetBIOS Suffix  State   Time Left  Type
-----
CLUSTER_1    00                          wins    57
CLUSTER_1    20                          wins    57

Vserver: vs1
Node:    cluster1-02
Interfaces:
          10.10.10.35
Servers:
          17.17.1.2 (active )
CLUSTER_1    00                          wins    58
CLUSTER_1    20                          wins    58
4 entries were displayed.

```

Comandos para gerenciar servidores SMB

Você precisa saber os comandos para criar, exibir, modificar, parar, iniciar e excluir servidores SMB. Há também comandos para redefinir e redescobrir servidores, alterar ou redefinir senhas de conta de máquina, agendar alterações para senhas de conta de máquina e adicionar ou remover aliases NetBIOS.

Se você quiser...	Use este comando...
Crie um servidor SMB	<code>vserver cifs create</code>
Exibir informações sobre um servidor SMB	<code>vserver cifs show</code>
Modifique um servidor SMB	<code>vserver cifs modify</code>
Mova um servidor SMB para outro domínio	<code>vserver cifs modify</code>

Parar um servidor SMB	<code>vserver cifs stop</code>
Inicie um servidor SMB	<code>vserver cifs start</code>
Excluir um servidor SMB	<code>vserver cifs delete</code>
Redefinir e redescobrir servidores para o servidor SMB	<code>vserver cifs domain discovered-servers reset-servers</code>
Altere a senha da conta de máquina do servidor SMB	<code>vserver cifs domain password change</code>
Redefina a senha da conta da máquina do servidor SMB	<code>vserver cifs domain password change</code>
Agendar alterações automáticas de senha para a conta de máquina do servidor SMB	<code>vserver cifs domain password schedule modify</code>
Adicione aliases NetBIOS para o servidor SMB	<code>vserver cifs add-netbios-aliases</code>
Remova os aliases NetBIOS para o servidor SMB	<code>vserver cifs remove-netbios-aliases</code>

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

Informações relacionadas

["O que acontece com usuários e grupos locais ao excluir servidores SMB"](#)

Ative o serviço de nomes NetBIOS

Começando com ONTAP 9, o serviço de nomes NetBIOS (NBNS, às vezes chamado de Serviço de nomes de Internet do Windows ou WINS) é desativado por padrão.

Anteriormente, as máquinas virtuais de armazenamento (SVMs) habilitadas por CIFS enviavam transmissões de Registro de nomes, independentemente de o WINS estar habilitado em uma rede. Para limitar tais transmissões a configurações em que o NBNS é necessário, você deve habilitar o NBNS explicitamente para novos servidores CIFS.

Antes de começar

- Se você já estiver usando NBNS e atualizar para o ONTAP 9, não é necessário concluir esta tarefa. NBNS continuará a funcionar como antes.
- O NBNS é ativado por UDP (porta 137).
- NBNS sobre IPv6 não é suportado.

Passos

1. Defina o nível de privilégio como avançado.

```
set -privilege advanced
```

2. Ative NBNS em um servidor CIFS.

```
vserver cifs options modify -vserver <vserver name> -is-nbns-enabled  
true
```

3. Retorne ao nível de privilégio de administrador.

```
set -privilege admin
```

Use o IPv6 para acesso SMB e serviços SMB

Requisitos para usar IPv6

Antes de poder usar o IPv6 no servidor SMB, você precisa saber quais versões do ONTAP e SMB o suportam e quais são os requisitos de licença.

Requisitos de licença do ONTAP

Nenhuma licença especial é necessária para o IPv6 quando o SMB é licenciado. 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 IPv6 em todas as versões do protocolo SMB.



O serviço de nomes NetBIOS (NBNS) em IPv6 não é suportado.

Suporte para IPv6 com acesso SMB e serviços CIFS

Se você quiser usar o IPv6 em seu servidor CIFS, você precisa estar ciente de como o ONTAP suporta o IPv6 para acesso SMB e comunicação de rede para serviços CIFS.

Suporte ao cliente e servidor Windows

O ONTAP fornece suporte para servidores e clientes Windows que suportam IPv6. A seguir descreve o suporte ao cliente e servidor Microsoft Windows IPv6:

- O Windows 7, Windows 8, Windows Server 2008, Windows Server 2012 e posterior suportam o IPv6 para serviços de partilha de ficheiros SMB e ative Directory, incluindo DNS, LDAP, CLDAP e Kerberos.

Se os endereços IPv6 estiverem configurados, o Windows 7 e o Windows Server 2008 e versões posteriores usam o IPv6 por padrão para serviços do ative Directory. Tanto a autenticação NTLM como Kerberos através de conexões IPv6 são suportadas.

Todos os clientes Windows suportados pelo ONTAP podem se conectar a compartilhamentos SMB usando endereços IPv6.

Para obter as informações mais recentes sobre quais clientes Windows ONTAP suportam, consulte "[Matriz de interoperabilidade](#)".



Os domínios NT não são suportados para IPv6.

Suporte adicional a serviços CIFS

Além do suporte IPv6 para compartilhamentos de arquivos SMB e serviços do Active Directory, o ONTAP oferece suporte IPv6 para o seguinte:

- Serviços do lado do cliente, incluindo pastas offline, perfis de roaming, redirecionamento de pastas e versões anteriores
- Serviços do lado do servidor, incluindo diretórios base dinâmicos (recurso Home Directory), links simbólicos e Widelinks, BranchCache, descarga de cópia ODX, referências automáticas de nós e versões anteriores
- Serviços de gerenciamento de acesso a arquivos, incluindo o uso de usuários e grupos locais do Windows para controle de acesso e gerenciamento de direitos, configuração de permissões de arquivos e políticas de auditoria usando a CLI, rastreamento de segurança, gerenciamento de bloqueios de arquivos e monitoramento de atividades SMB
- Auditoria multiprotocolo nas
- FPolicy
- Compartilhamentos continuamente disponíveis, protocolo de testemunha e VSS remoto (usado com configurações Hyper-V em SMB)

Serviço de nomes e suporte de serviços de autenticação

A comunicação com os seguintes serviços de nome é suportada com o IPv6:

- Controladores de domínio
- Servidores DNS
- Servidores LDAP
- Servidores KDC
- Servidores NIS

Como os servidores CIFS usam o IPv6 para se conectar a servidores externos

Para criar uma configuração que atenda aos seus requisitos, você deve estar ciente de como os servidores CIFS usam o IPv6 ao fazer conexões com servidores externos.

- Seleção do endereço de origem

Se for feita uma tentativa de ligação a um servidor externo, o endereço de origem selecionado tem de ser do mesmo tipo que o endereço de destino. Por exemplo, se estiver conectando a um endereço IPv6, a máquina virtual de armazenamento (SVM) que hospeda o servidor CIFS deve ter um LIF de dados ou LIF de gerenciamento que tenha um endereço IPv6 para usar como endereço de origem. Da mesma forma, se estiver conectando a um endereço IPv4, o SVM precisa ter um LIF de dados ou um LIF de gerenciamento

que tenha um endereço IPv4 para usar como endereço de origem.

- Para servidores dinamicamente descobertos usando DNS, a descoberta do servidor é executada da seguinte forma:
 - Se o IPv6 estiver desativado no cluster, apenas serão detetados IPv4 endereços de servidores.
 - Se IPv6 estiver ativado no cluster, os endereços de servidor IPv4 e IPv6 serão descobertos. Qualquer tipo pode ser usado dependendo da adequação do servidor ao qual o endereço pertence e da disponibilidade de dados IPv6 ou IPv4 ou LIFs de gerenciamento. A descoberta dinâmica de servidor é usada para descobrir controladores de domínio e seus serviços associados, como LSA, NETLOGON, Kerberos e LDAP.
- Conetividade do servidor DNS

Se o SVM usa IPv6 ao se conectar a um servidor DNS depende da configuração dos serviços de nome DNS. Se os serviços DNS estiverem configurados para usar endereços IPv6, as conexões serão feitas usando IPv6. Se desejar, a configuração dos serviços de nomes DNS pode usar endereços IPv4 para que as conexões com servidores DNS continuem a usar endereços IPv4. Combinações de endereços IPv4 e IPv6 podem ser especificadas ao configurar serviços de nomes DNS.

- Conetividade do servidor LDAP

Se o SVM usa IPv6 ao se conectar a um servidor LDAP depende da configuração do cliente LDAP. Se o cliente LDAP estiver configurado para usar endereços IPv6, as conexões serão feitas usando IPv6. Se desejar, a configuração do cliente LDAP pode usar endereços IPv4 para que as conexões com servidores LDAP continuem a usar endereços IPv4. Combinações de endereços IPv4 e IPv6 podem ser especificadas ao configurar a configuração do cliente LDAP.



A configuração do cliente LDAP é usada ao configurar o LDAP para serviços de nome de usuário, grupo e netgroup UNIX.

- Conetividade do servidor NIS

Se o SVM usa IPv6 ao conectar-se a um servidor NIS depende da configuração dos serviços de nome NIS. Se os serviços NIS estiverem configurados para usar endereços IPv6, as conexões serão feitas usando IPv6. Se desejar, a configuração dos serviços de nomes NIS pode usar endereços IPv4 para que as conexões com servidores NIS continuem a usar endereços IPv4. Combinações de endereços IPv4 e IPv6 podem ser especificadas ao configurar serviços de nomes NIS.



Os serviços de nomes NIS são usados para armazenar e gerenciar objetos de nome de usuário, grupo, netgroup e host UNIX.

Informações relacionadas

[Habilitação do IPv6 para SMB \(somente administradores de cluster\)](#)

[Monitoramento e exibição de informações sobre IPv6 sessões SMB](#)

Ativar o IPv6 para SMB (somente administradores de cluster)

As redes IPv6 não estão ativadas durante a configuração do cluster. Um administrador de cluster deve habilitar o IPv6 após a conclusão da configuração do cluster para usar o IPv6 para SMB. Quando o administrador do cluster ativa o IPv6, ele é ativado para todo o cluster.

Passo

1. Ativar IPv6: `network options ipv6 modify -enabled true`

Para obter mais informações sobre como ativar o IPv6 no cluster e configurar LIFs IPv6, consulte o *Network Management Guide*.

IPv6 está ativado. LIFs de dados IPv6 para acesso SMB podem ser configurados.

Informações relacionadas

[Monitoramento e exibição de informações sobre IPv6 sessões SMB](#)

["Gerenciamento de rede"](#)

Desativar IPv6 para SMB

Mesmo que IPv6 esteja habilitado no cluster usando uma opção de rede, você não pode desabilitar IPv6 para SMB usando o mesmo comando. Em vez disso, o ONTAP desativa o IPv6 quando o administrador do cluster desativa a última interface habilitada para IPv6 no cluster. Você deve se comunicar com o administrador do cluster sobre o gerenciamento de suas interfaces IPv6 habilitadas.

Para obter mais informações sobre a desativação do IPv6 no cluster, consulte o *Network Management Guide*.

Informações relacionadas

["Gerenciamento de rede"](#)

Monitore e exiba informações sobre IPv6 sessões SMB

Você pode monitorar e exibir informações sobre sessões SMB conetadas usando redes IPv6G. Essas informações são úteis para determinar quais clientes estão se conetando usando o IPv6, bem como outras informações úteis sobre sessões SMB do IPv6.

Passo

1. Execute a ação desejada:

Se você quiser determinar se...	Digite o comando...
As sessões de SMB a uma máquina virtual de storage (SVM) são conetadas usando o IPv6	<pre>vserver cifs session show -vserver vserver_name -instance</pre>
IPv6 é usado para sessões SMB através de um endereço LIF especificado	<pre>vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address -instance</pre> <p><i>LIF_IP_address</i> É o endereço IPv6 do LIF de dados.</p>

Configure o acesso a arquivos usando SMB

Configurar estilos de segurança

Como os estilos de segurança afetam o acesso aos dados

Estilos de segurança e seus efeitos

Existem quatro estilos de segurança diferentes: UNIX, NTFS, misto e unificado. Cada estilo de segurança tem um efeito diferente sobre como as permissões são tratadas para os dados. Você deve entender os diferentes efeitos para garantir que você selecione o estilo de segurança apropriado para seus propósitos.

É importante entender que os estilos de segurança não determinam quais tipos de clientes podem ou não acessar dados. Os estilos de segurança determinam apenas o tipo de permissões que o ONTAP usa para controlar o acesso aos dados e que tipo de cliente pode modificar essas permissões.

Por exemplo, se um volume usa estilo de segurança UNIX, os clientes SMB ainda podem acessar dados (desde que autentiquem e autorizem adequadamente) devido à natureza multiprotocolo do ONTAP. No entanto, o ONTAP usa permissões UNIX que somente clientes UNIX podem modificar usando ferramentas nativas.

Estilo de segurança	Cientes que podem modificar permissões	Permissões que os clientes podem usar	Estilo de segurança eficaz resultante	Cientes que podem acessar arquivos
UNIX	NFS	NFSv3 bits de modo	UNIX	NFS e SMB
		ACLs NFSv4.x		
NTFS	SMB	ACLs NTFS	NTFS	
Misto	NFS ou SMB	NFSv3 bits de modo	UNIX	
		NFSv4.ACLs		
		ACLs NTFS	NTFS	
Unificado (somente para volumes infinitos, no ONTAP 9.4 e versões anteriores).	NFS ou SMB	NFSv3 bits de modo	UNIX	
		ACLs NFSv4,1		
		ACLs NTFS	NTFS	

Os volumes FlexVol suportam estilos de segurança UNIX, NTFS e mistos. Quando o estilo de segurança é misto ou unificado, as permissões efetivas dependem do tipo de cliente que modificou as permissões pela última vez porque os usuários definem o estilo de segurança individualmente. Se o último cliente que modificou permissões fosse um cliente NFSv3, as permissões são bits do modo UNIX NFSv3. Se o último cliente foi um cliente NFSv4, as permissões são NFSv4 ACLs. Se o último cliente foi um cliente SMB, as permissões são ACLs do Windows NTFS.

O estilo de segurança unificado só está disponível com volumes infinitos, que não são mais suportados no ONTAP 9.5 e versões posteriores. Para obter mais informações, [Visão geral do gerenciamento do FlexGroup volumes](#) consulte .

A partir do ONTAP 9.2, o `show-effective-permissions` parâmetro para o `vserver security file-directory` comando permite exibir permissões efetivas concedidas a um usuário Windows ou UNIX no caminho especificado de arquivo ou pasta. Além disso, o parâmetro opcional `-share-name` permite exibir a permissão de compartilhamento efetivo.



O ONTAP define inicialmente algumas permissões de arquivo padrão. Por padrão, o estilo de segurança eficaz em todos os dados em UNIX, volumes mistos e de estilo de segurança unificado é UNIX e o tipo de permissões efetivas é bits de modo UNIX (0755 a menos que especificado de outra forma) até ser configurado por um cliente como permitido pelo estilo de segurança padrão. Por padrão, o estilo de segurança eficaz em todos os dados em volumes de estilo de segurança NTFS é NTFS e tem uma ACL que permite o controle total para todos.

Onde e quando definir estilos de segurança

Os estilos de segurança podem ser definidos em volumes FlexVol (raiz ou volumes de dados) e qtrees. Os estilos de segurança podem ser definidos manualmente no momento da criação, herdados automaticamente ou alterados posteriormente.

Decida qual estilo de segurança usar em SVMs

Para ajudá-lo a decidir qual estilo de segurança usar em um volume, você deve considerar dois fatores. O fator principal é o tipo de administrador que gerencia o sistema de arquivos. O fator secundário é o tipo de usuário ou serviço que acessa os dados no volume.

Ao configurar o estilo de segurança em um volume, você deve considerar as necessidades do seu ambiente para garantir que você selecione o melhor estilo de segurança e evite problemas com o gerenciamento de permissões. As seguintes considerações podem ajudá-lo a decidir:

Estilo de segurança	Escolha se...
UNIX	<ul style="list-style-type: none">• O sistema de arquivos é gerenciado por um administrador UNIX.• A maioria dos usuários são clientes NFS.• Um aplicativo que acessa os dados usa um usuário UNIX como a conta de serviço.
NTFS	<ul style="list-style-type: none">• O sistema de arquivos é gerenciado por um administrador do Windows.• A maioria dos usuários são clientes SMB.• Um aplicativo que acessa os dados usa um usuário do Windows como a conta de serviço.
Misto	O sistema de arquivos é gerenciado por administradores UNIX e Windows e os usuários consistem em clientes NFS e SMB.

Como a herança de estilo de segurança funciona

Se você não especificar o estilo de segurança ao criar um novo FlexVol volume ou uma qtree, ele herdará seu estilo de segurança de maneiras diferentes.

Os estilos de segurança são herdados da seguinte maneira:

- Um FlexVol volume herda o estilo de segurança do volume raiz do SVM.
- Uma qtree herda o estilo de segurança do seu que contém FlexVol volume.
- Um arquivo ou diretório herda o estilo de segurança dele contendo FlexVol volume ou qtree.

Como o ONTAP preserva as permissões UNIX

Quando os arquivos em um FlexVol volume que atualmente têm permissões UNIX são editados e salvos por aplicativos do Windows, o ONTAP pode preservar as permissões UNIX.

Quando os aplicativos em clientes do Windows editam e salvam arquivos, eles leem as propriedades de segurança do arquivo, criam um novo arquivo temporário, aplicam essas propriedades ao arquivo temporário e dão ao arquivo temporário o nome do arquivo original.

Quando os clientes Windows executam uma consulta para as propriedades de segurança, eles recebem uma ACL construída que representa exatamente as permissões UNIX. O único propósito desta ACL construída é preservar as permissões UNIX do arquivo, pois os arquivos são atualizados por aplicativos do Windows para garantir que os arquivos resultantes tenham as mesmas permissões UNIX. O ONTAP não define nenhuma ACLs NTFS usando a ACL construída.

Gerenciar permissões UNIX usando a guia Segurança do Windows

Se você quiser manipular permissões UNIX de arquivos ou pastas em volumes mistos de estilo de segurança ou qtrees em SVMs, você pode usar a guia Segurança em clientes Windows. Como alternativa, você pode usar aplicativos que podem consultar e definir ACLs do Windows.

- Modificação de permissões UNIX

Você pode usar a guia Segurança do Windows para exibir e alterar permissões UNIX para um volume ou qtree misto de estilo de segurança. Se você usar a guia principal de Segurança do Windows para alterar permissões UNIX, primeiro remova o ACE existente que deseja editar (isso define os bits de modo como 0) antes de fazer as alterações. Como alternativa, você pode usar o editor avançado para alterar permissões.

Se as permissões de modo forem usadas, você pode alterar diretamente as permissões de modo para o UID listado, GID e outros (todos os outros com uma conta no computador). Por exemplo, se o UID exibido tiver permissões r-x, você pode alterar as permissões UID para rwx.

- Alterando permissões UNIX para permissões NTFS

Você pode usar a guia Segurança do Windows para substituir objetos de segurança UNIX por objetos de segurança do Windows em um volume de estilo de segurança misto ou qtree onde os arquivos e pastas têm um estilo de segurança eficaz UNIX.

Você deve primeiro remover todas as entradas de permissão UNIX listadas antes de poder substituí-las

pelos objetos de Usuário e Grupo do Windows desejados. Em seguida, você pode configurar ACLs baseadas em NTFS nos objetos Usuário e Grupo do Windows. Removendo todos os objetos de segurança UNIX e adicionando apenas usuários e grupos do Windows a um arquivo ou pasta em um volume ou qtree misto de estilo de segurança, você altera o estilo de segurança efetivo no arquivo ou pasta de UNIX para NTFS.

Ao alterar permissões em uma pasta, o comportamento padrão do Windows é propagar essas alterações para todas as subpastas e arquivos. Portanto, você deve alterar a opção de propagação para a configuração desejada se não quiser propagar uma alteração no estilo de segurança para todas as pastas, subpastas e arquivos filhos.

Configurar estilos de segurança em volumes raiz do SVM

Você configura o estilo de segurança do volume raiz da máquina virtual de storage (SVM) para determinar o tipo de permissões usado para dados no volume raiz do SVM.

Passos

1. Use o `vserver create` comando com o `-rootvolume-security-style` parâmetro para definir o estilo de segurança.

As opções possíveis para o estilo de segurança do volume raiz são `unix`, `ntfs` ou `mixed`.

2. Exiba e verifique a configuração, incluindo o estilo de segurança do volume raiz do SVM criado: `vserver show -vserver vserver_name`

Configurar estilos de segurança no FlexVol volumes

Você configura o estilo de segurança do FlexVol volume para determinar o tipo de permissões usadas para dados nos volumes do FlexVol da máquina virtual de storage (SVM).

Passos

1. Execute uma das seguintes ações:

Se o FlexVol volume...	Use o comando...
Ainda não existe	<code>volume create</code> e inclua o <code>-security-style</code> parâmetro para especificar o estilo de segurança.
Já existe	<code>volume modify</code> e inclua o <code>-security-style</code> parâmetro para especificar o estilo de segurança.

As opções possíveis para o estilo de segurança do FlexVol volume são `unix`, `ntfs` ou `mixed`.

Se você não especificar um estilo de segurança ao criar um FlexVol volume, o volume herdará o estilo de segurança do volume raiz.

Para obter mais informações sobre os `volume create` comandos ou `volume modify`, "[Gerenciamento de storage lógico](#)" consulte .

2. Para exibir a configuração, incluindo o estilo de segurança do FlexVol volume criado, digite o seguinte

comando:

```
volume show -volume volume_name -instance
```

Configurar estilos de segurança no qtrees

Você configura o estilo de segurança do volume de qtree para determinar o tipo de permissões usadas para dados no qtrees.

Passos

1. Execute uma das seguintes ações:

Se a qtree...	Use o comando...
Ainda não existe	<code>volume qtree create</code> e inclua o <code>-security -style</code> parâmetro para especificar o estilo de segurança.
Já existe	<code>volume qtree modify</code> e inclua o <code>-security -style</code> parâmetro para especificar o estilo de segurança.

As opções possíveis para o estilo de segurança de qtree são `unix`, `ntfs`, ou `mixed`.

Se você não especificar um estilo de segurança ao criar uma qtree, o estilo de segurança padrão será `mixed`.

Para obter mais informações sobre os `volume qtree create` comandos ou `volume qtree modify`, "[Gerenciamento de storage lógico](#)" consulte .

2. Para exibir a configuração, incluindo o estilo de segurança da qtree que você criou, digite o seguinte comando: `volume qtree show -qtree qtree_name -instance`

Crie e gerencie volumes de dados em namespaces nas

Criar e gerenciar volumes de dados na visão geral dos namespaces nas

Para gerenciar o acesso a arquivos em um ambiente nas, você precisa gerenciar volumes de dados e pontos de junção na máquina virtual de storage (SVM). Isso inclui Planejar sua arquitetura de namespace, criar volumes com ou sem pontos de junção, montar ou desmontar volumes e exibir informações sobre volumes de dados e namespaces de servidor NFS ou CIFS.

Crie volumes de dados com pontos de junção especificados

Pode especificar o ponto de junção quando cria um volume de dados. O volume resultante é montado automaticamente no ponto de junção e está imediatamente disponível para configurar para acesso nas.

Antes de começar

O agregado no qual você deseja criar o volume já deve existir.



Os seguintes caracteres não podem ser usados no caminho de junção: * *

Além disso, o comprimento do caminho de junção não pode ter mais de 255 caracteres.

Passos

1. Crie o volume com um ponto de junção: `volume create -vserver vs1 -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -junction-path junction_path`

O caminho de junção deve começar com a raiz (/) e pode conter diretórios e volumes juntados. O caminho de junção não precisa conter o nome do volume. Os caminhos de junção são independentes do nome do volume.

Especificar um estilo de segurança de volume é opcional. Se você não especificar um estilo de segurança, o ONTAP criará o volume com o mesmo estilo de segurança aplicado ao volume raiz da máquina virtual de storage (SVM). No entanto, o estilo de segurança do volume raiz pode não ser o estilo de segurança que você deseja aplicar ao volume de dados criado. A recomendação é especificar o estilo de segurança quando você cria o volume para minimizar problemas de acesso a arquivos difíceis de solucionar.

O caminho de junção é insensível a maiúsculas e minúsculas; /ENG é o mesmo que /eng. Se você criar um compartilhamento CIFS, o Windows tratará o caminho de junção como se ele fosse sensível a maiúsculas e minúsculas. Por exemplo, se a junção for /ENG, o caminho de um compartilhamento CIFS deve começar com /ENG, não /eng.

Há muitos parâmetros opcionais que você pode usar para personalizar um volume de dados. Para saber mais sobre eles, consulte as páginas de manual do `volume create` comando.

2. Verifique se o volume foi criado com o ponto de junção desejado: `volume show -vserver vs1 -volume volume_name -junction`

Exemplo

O exemplo a seguir cria um volume chamado "home4" localizado na SVM VS1 que tem um caminho de junção /eng/home :

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -volume home4 -junction
```

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

Crie volumes de dados sem especificar pontos de junção

Você pode criar um volume de dados sem especificar um ponto de junção. O volume resultante não é montado automaticamente e não está disponível para configuração para acesso nas. É necessário montar o volume antes de configurar compartilhamentos SMB ou exportações NFS para esse volume.

Antes de começar

O agregado no qual você deseja criar o volume já deve existir.

Passos

1. Crie o volume sem um ponto de junção usando o seguinte comando: `volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed}`

Especificar um estilo de segurança de volume é opcional. Se você não especificar um estilo de segurança, o ONTAP criará o volume com o mesmo estilo de segurança aplicado ao volume raiz da máquina virtual de storage (SVM). No entanto, o estilo de segurança do volume raiz pode não ser o estilo de segurança que você deseja aplicar ao volume de dados. A recomendação é especificar o estilo de segurança quando você cria o volume para minimizar problemas de acesso a arquivos difíceis de solucionar.

Há muitos parâmetros opcionais que você pode usar para personalizar um volume de dados. Para saber mais sobre eles, consulte as páginas de manual do `volume create` comando.

2. Verifique se o volume foi criado sem um ponto de junção: `volume show -vserver vserver_name -volume volume_name -junction`

Exemplo

O exemplo a seguir cria um volume chamado "vendas" localizado no SVM VS1 que não está montado em um ponto de junção:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	data	true	/data	RW_volume
vs1	home4	true	/eng/home	RW_volume
vs1	vs1_root	-	/	-
vs1	sales	-	-	-

Montar ou desmontar volumes existentes no namespace nas

Um volume deve ser montado no namespace nas antes de poder configurar o acesso do cliente nas aos dados contidos nos volumes de máquina virtual de storage (SVM). Você

pode montar um volume em um ponto de junção se ele não estiver montado no momento. Você também pode desmontar volumes.

Sobre esta tarefa

Se você desmontar e colocar um volume off-line, todos os dados dentro do ponto de junção, incluindo dados em volumes com pontos de junção contidos no namespace do volume não montado, ficarão inacessíveis para clientes nas.



Para interromper o acesso de cliente nas a um volume, não é suficiente simplesmente desmontar o volume. Você deve colocar o volume off-line ou tomar outras medidas para garantir que os caches de manipulação de arquivos do lado do cliente sejam invalidados. Para obter mais informações, consulte o seguinte artigo da base de dados de Conhecimento: ["Os clientes NFSv3 ainda têm acesso a um volume depois de serem removidos do namespace no ONTAP"](#)

Quando você desmontar e colocar um volume off-line, os dados dentro do volume não são perdidos. Além disso, políticas de exportação de volume existentes e compartilhamentos SMB criados no volume ou em diretórios e pontos de junção dentro do volume não montado são retidos. Se você remontar o volume não montado, os clientes nas poderão acessar os dados contidos no volume usando políticas de exportação e compartilhamentos SMB existentes.

Passos

1. Execute a ação desejada:

Se você quiser...	Digite os comandos...
Monte um volume	<pre>volume mount -vserver <i>svm_name</i> -volume <i>volume_name</i> -junction-path <i>junction_path</i></pre>
Desmontar um volume	<pre>volume unmount -vserver <i>svm_name</i> -volume <i>volume_name</i> volume offline -vserver <i>svm_name</i> -volume <i>volume_name</i></pre>

2. Verifique se o volume está no estado de montagem desejado:

```
volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active
```

Exemplos

O exemplo a seguir monta um volume chamado "vendas" localizado na SVM "VS1" no ponto de junção ""/vendas":

```

cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver    volume      state      junction-path  junction-active
-----
vs1        data        online     /data          true
vs1        home4       online     /eng/home      true
vs1        sales       online     /sales         true

```

O exemplo a seguir desmonta e coloca offline um volume chamado "data" localizado na SVM "VS1":

```

cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver    volume      state      junction-path  junction-active
-----
vs1        data        offline    -              -
vs1        home4       online     /eng/home      true
vs1        sales       online     /sales         true

```

Apresentar informações sobre a montagem do volume e o ponto de junção

Você pode exibir informações sobre volumes montados para máquinas virtuais de armazenamento (SVMs) e os pontos de junção para os quais os volumes são montados. Você também pode determinar quais volumes não estão montados em um ponto de junção. Use essas informações para entender e gerenciar seu namespace SVM.

Passos

1. Execute a ação desejada:

Se você quiser exibir...	Digite o comando...
Informações resumidas sobre volumes montados e não montados no SVM	<code>volume show -vserver vs1 -junction</code>
Informações detalhadas sobre volumes montados e não montados no SVM	<code>volume show -vserver vs1 -volume volume_name -instance</code>

Se você quiser exibir...	Digite o comando...
Informações específicas sobre volumes montados e não montados no SVM	<p>a. Se necessário, você pode exibir campos válidos para o <code>-fields</code> parâmetro usando o seguinte comando: <code>volume show -fields ?</code></p> <p>b. Exiba as informações desejadas usando o <code>-fields</code> parâmetro: <code>Volume show -vserver vs1 -fieldname,...</code></p>

Exemplos

O exemplo a seguir exibe um resumo dos volumes montados e não montados no SVM VS1:

```
cluster1::> volume show -vserver vs1 -junction
          Junction
Vserver  Volume  Active  Junction Path  Junction
-----  -
vs1      data    true    /data          RW_volume
vs1      home4   true    /eng/home      RW_volume
vs1      vs1_root -        /              -
vs1      sales   true    /sales         RW_volume
```

O exemplo a seguir exibe informações sobre campos especificados para volumes localizados no SVM VS2:


```

cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume    aggregate size state  type security-style junction-path
junction-parent node
-----
vs2      data1      aggr3    2GB  online RW   unix          -          -
node3
vs2      data2      aggr3    1GB  online RW   ntfs          /data2
vs2_root node3
vs2      data2_1    aggr3    8GB  online RW   ntfs          /data2/d2_1
data2    node3
vs2      data2_2    aggr3    8GB  online RW   ntfs          /data2/d2_2
data2    node3
vs2      pubs      aggr1    1GB  online RW   unix          /publications
vs2_root node1
vs2      images    aggr3    2TB  online RW   ntfs          /images
vs2_root node3
vs2      logs      aggr1    1GB  online RW   unix          /logs
vs2_root node1
vs2      vs2_root  aggr3    1GB  online RW   ntfs          /          -
node3

```

Configurar mapeamentos de nomes

Configure a visão geral dos mapeamentos de nomes

O ONTAP usa mapeamento de nomes para mapear identidades CIFS para identidades UNIX, identidades Kerberos para identidades UNIX e identidades UNIX para identidades CIFS. Ele precisa dessas informações para obter credenciais de usuário e fornecer acesso adequado aos arquivos, independentemente de estarem se conectando a partir de um cliente NFS ou de um cliente CIFS.

Há duas exceções em que você não precisa usar o mapeamento de nomes:

- Você configura um ambiente UNIX puro e não planeja usar o acesso CIFS ou o estilo de segurança NTFS em volumes.
- Em vez disso, você configura o usuário padrão a ser usado.

Nesse cenário, o mapeamento de nomes não é necessário porque, em vez de mapear cada credencial de cliente individual, todas as credenciais de cliente são mapeadas para o mesmo usuário padrão.

Observe que você pode usar o mapeamento de nomes somente para usuários, não para grupos.

No entanto, você pode mapear um grupo de usuários individuais para um usuário específico. Por exemplo,

você pode mapear todos os usuários do AD que começam ou terminam com a palavra VENDAS para um usuário UNIX específico e para o UID do usuário.

Como o mapeamento de nomes funciona

Quando o ONTAP tem que mapear credenciais para um usuário, ele primeiro verifica o banco de dados de mapeamento de nomes local e o servidor LDAP para um mapeamento existente. Verifique uma ou ambas e em que ordem é determinada pela configuração do serviço de nomes do SVM.

- Para mapeamento do Windows para UNIX

Se nenhum mapeamento for encontrado, o ONTAP verifica se o nome de usuário do Windows em minúsculas é um nome de usuário válido no domínio UNIX. Se isso não funcionar, ele usará o usuário UNIX padrão desde que esteja configurado. Se o usuário UNIX padrão não estiver configurado e o ONTAP também não puder obter um mapeamento dessa maneira, o mapeamento falhará e um erro será retornado.

- Para mapeamento UNIX para Windows

Se nenhum mapeamento for encontrado, o ONTAP tentará encontrar uma conta do Windows que corresponda ao nome UNIX no domínio SMB. Se isso não funcionar, ele usará o usuário SMB padrão, desde que esteja configurado. Se o usuário CIFS padrão não estiver configurado e o ONTAP também não puder obter um mapeamento dessa maneira, o mapeamento falhará e um erro será retornado.

As contas de máquina são mapeadas para o usuário UNIX padrão especificado por padrão. Se nenhum usuário UNIX padrão for especificado, mapeamentos de contas de máquina falharão.

- A partir do ONTAP 9.5, você pode mapear contas de máquina para usuários que não sejam o usuário UNIX padrão.
- No ONTAP 9.4 e anteriores, você não pode mapear contas de máquina para outros usuários.

Mesmo que os mapeamentos de nomes para contas de máquinas sejam definidos, os mapeamentos serão ignorados.

Procura multidomínio para mapeamentos de nome de usuário do UNIX para o Windows

O ONTAP oferece suporte a pesquisas de vários domínios ao mapear usuários UNIX para usuários do Windows. Todos os domínios confiáveis descobertos são pesquisados por correspondências ao padrão de substituição até que um resultado correspondente seja retornado. Como alternativa, você pode configurar uma lista de domínios confiáveis preferenciais, que é usada em vez da lista de domínios confiáveis descobertos e é pesquisada em ordem até que um resultado correspondente seja retornado.

Como as relações de confiança de domínio afetam as pesquisas de mapeamento de nomes de usuário do Windows

Para entender como o mapeamento de nomes de usuário de vários domínios funciona, você deve entender como as relações de confiança de domínio funcionam com o ONTAP. As relações de confiança do Active Directory com o domínio home do servidor CIFS podem ser uma confiança bidirecional ou podem ser um dos dois tipos de confiança unidirecionais, uma confiança de entrada ou uma confiança de saída. O domínio inicial é o domínio ao qual pertence o servidor CIFS na SVM.

- *Confiança bidirecional*

Com trusts bidirecionais, ambos os domínios confiam uns nos outros. Se o domínio home do servidor CIFS tiver uma confiança bidirecional com outro domínio, o domínio home pode autenticar e autorizar um usuário pertencente ao domínio confiável e vice-versa.

As pesquisas de mapeamento de nome de usuário do UNIX para o Windows podem ser realizadas apenas em domínios com confiança bidirecional entre o domínio inicial e o outro domínio.

- *Outbound Trust*

Com uma confiança de saída, o domínio home confia no outro domínio. Nesse caso, o domínio home pode autenticar e autorizar um usuário pertencente ao domínio confiável de saída.

Um domínio com uma confiança de saída com o domínio inicial é *not* pesquisado ao executar pesquisas de mapeamento de nomes de usuário do UNIX para o Windows.

- *Confiança inbound*


Com uma confiança de entrada, o outro domínio confia no domínio home do servidor CIFS. Neste caso, o domínio inicial não pode autenticar ou autorizar um usuário pertencente ao domínio confiável de entrada.

Um domínio com uma confiança de entrada com o domínio inicial é *not* pesquisado ao executar pesquisas de mapeamento de nomes de usuário do UNIX para o Windows.

Como os curingas (*) são usados para configurar pesquisas de vários domínios para mapeamento de nomes

As pesquisas de mapeamento de nomes de vários domínios são facilitadas pelo uso de curingas na seção domínio do nome de usuário do Windows. A tabela a seguir ilustra como usar curingas na parte de domínio de uma entrada de mapeamento de nomes para habilitar pesquisas de vários domínios:

Padrão	Substituição	Resultado
raiz	<ul style="list-style-type: none">• administrador	O usuário UNIX "root" é mapeado para o usuário chamado "administrador". Todos os domínios confiáveis são pesquisados em ordem até que o primeiro usuário correspondente chamado "administrador" seja encontrado.

Padrão	Substituição	Resultado
*	• *	<p>Os usuários UNIX válidos são mapeados para os usuários do Windows correspondentes. Todos os domínios confiáveis são pesquisados em ordem até que o primeiro usuário correspondente com esse nome seja encontrado.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>O padrão* é válido apenas para mapeamento de nomes do UNIX para o Windows, e não para o contrário.</p> </div>

Como as pesquisas de nomes de vários domínios são realizadas

Você pode escolher um dos dois métodos para determinar a lista de domínios confiáveis usados para pesquisas de nomes de vários domínios:

- Use a lista de confiança bidirecional descoberta automaticamente compilada pelo ONTAP
- Use a lista de domínio confiável preferida que você compila

Se um usuário UNIX for mapeado para um usuário do Windows com um curinga usado para a seção de domínio do nome de usuário, o usuário do Windows será pesquisado em todos os domínios confiáveis da seguinte forma:

- Se uma lista de domínio confiável preferencial estiver configurada, o usuário mapeado do Windows será pesquisado somente nesta lista de pesquisa, em ordem.
- Se uma lista preferencial de domínios confiáveis não estiver configurada, o usuário do Windows será pesquisado em todos os domínios confiáveis bidirecionais do domínio doméstico.
- Se não houver domínios bidirecionalmente confiáveis para o domínio home, o usuário será pesquisado no domínio home.

Se um usuário UNIX for mapeado para um usuário do Windows sem uma seção de domínio no nome de usuário, o usuário do Windows será pesquisado no domínio inicial.

Regras de conversão de mapeamento de nomes

Um sistema ONTAP mantém um conjunto de regras de conversão para cada SVM. Cada regra consiste em duas partes: Um *pattern* e um *replacement*. As conversões começam no início da lista apropriada e executam uma substituição com base na primeira regra de correspondência. O padrão é uma expressão regular estilo UNIX. A substituição é uma cadeia de caracteres contendo sequências de escape que representam subexpressões do padrão, como no programa UNIX `sed`.

Crie um mapeamento de nomes

Você pode usar o `vserver name-mapping create` comando para criar um mapeamento de nomes. Use mapeamentos de nomes para permitir que os usuários do Windows acessem volumes de estilo de segurança UNIX e o inverso.

Sobre esta tarefa

Para cada SVM, o ONTAP oferece suporte a até 12.500 mapeamentos de nomes para cada direção.

Passo

1. Criar um mapeamento de nomes: `vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-unix|unix-win} -position integer -pattern text -replacement text`



As `-pattern` declarações e `-replacement` podem ser formuladas como expressões regulares. Você também pode usar a `-replacement` instrução para negar explicitamente um mapeamento para o usuário usando a cadeia de substituição nula " " (o caractere de espaço). Consulte a `vserver name-mapping create` página de manual para obter detalhes.

Quando os mapeamentos do Windows para UNIX são criados, todos os clientes SMB que tenham conexões abertas ao sistema ONTAP no momento em que os novos mapeamentos são criados devem fazer logout e fazer login novamente para ver os novos mapeamentos.

Exemplos

O comando a seguir cria um mapeamento de nomes no SVM chamado VS1. O mapeamento é um mapeamento do UNIX para o Windows na posição 1 na lista de prioridades. O mapeamento mapeia o usuário UNIX johnd para o usuário do Windows Eng.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

O comando a seguir cria outro mapeamento de nomes no SVM chamado VS1. O mapeamento é um mapeamento do Windows para o UNIX na posição 1 na lista de prioridades. Aqui o padrão e a substituição incluem expressões regulares. O mapeamento mapeia cada usuário CIFS no domínio ENG para usuários no domínio LDAP associado ao SVM.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\\1"
```

O comando a seguir cria outro mapeamento de nomes no SVM chamado VS1. Aqui, o padrão inclui "" como um elemento no nome de usuário do Windows que deve ser escapado. O mapeamento mapeia as operações do usuário do Windows para o usuário do UNIX John_OPS.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$\ops
-replacement john_ops
```

Configure o usuário padrão

Você pode configurar um usuário padrão para usar se todas as outras tentativas de mapeamento falharem para um usuário ou se não quiser mapear usuários individuais entre UNIX e Windows. Alternativamente, se você quiser que a autenticação de usuários não mapeados falhe, você não deve configurar um usuário padrão.

Sobre esta tarefa

Para autenticação CIFS, se você não quiser mapear cada usuário do Windows para um usuário UNIX individual, você pode especificar um usuário UNIX padrão.

Para autenticação NFS, se você não quiser mapear cada usuário UNIX para um usuário individual do Windows, você pode especificar um usuário padrão do Windows.

Passos


1. Execute uma das seguintes ações:

Se você quiser...	Digite o seguinte comando...
Configure o usuário UNIX padrão	<code>vserver cifs options modify -default -unix-user <i>user_name</i></code>
Configure o usuário padrão do Windows	<code>vserver nfs modify -default-win-user <i>user_name</i></code>

Comandos para gerenciar mapeamentos de nomes

Existem comandos ONTAP específicos para gerenciar mapeamentos de nomes.

Se você quiser...	Use este comando...
Crie um mapeamento de nomes	<code>vserver name-mapping create</code>
Insira um mapeamento de nomes em uma posição específica	<code>vserver name-mapping insert</code>
Exibir mapeamentos de nomes	<code>vserver name-mapping show</code>

Se você quiser...	Use este comando...
Troque a posição de dois mapeamentos de nomes <div style="display: flex; align-items: center; margin-top: 10px;">  <p>Uma troca não é permitida quando o mapeamento de nomes é configurado com uma entrada de qualificador ip.</p> </div>	<code>vserver name-mapping swap</code>
Modificar um mapeamento de nomes	<code>vserver name-mapping modify</code>
Eliminar um mapeamento de nomes	<code>vserver name-mapping delete</code>
Valide o mapeamento de nomes correto	<code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code>

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

Configurar pesquisas de mapeamento de nomes de vários domínios

Ative ou desative pesquisas de mapeamento de nomes de vários domínios

Com pesquisas de mapeamento de nomes de vários domínios, você pode usar um cartão selvagem (*) **na parte de domínio de um nome do Windows ao configurar o usuário UNIX para o mapeamento de nome de usuário do Windows. O uso de um cartão selvagem (*) na parte do domínio do nome permite que o ONTAP pesquise todos os domínios que tenham uma confiança bidirecional com o domínio que contém a conta do computador do servidor CIFS.**

Sobre esta tarefa

Como alternativa à pesquisa de todos os domínios bidirecionalmente confiáveis, você pode configurar uma lista de domínios confiáveis preferenciais. Quando uma lista de domínios confiáveis preferenciais é configurada, o ONTAP usa a lista de domínios confiáveis preferenciais em vez dos domínios confiáveis bidirecionais descobertos para realizar pesquisas de mapeamento de nomes de vários domínios.

- As pesquisas de mapeamento de nomes de vários domínios são ativadas por padrão.
- Esta opção está disponível no nível de privilégio avançado.

Passos

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

Se você deseja que as pesquisas de mapeamento de nomes de vários domínios sejam...	Digite o comando...
Ativado	<pre>vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled true</pre>
Desativado	<pre>vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled false</pre>

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

Informações relacionadas

[Opções de servidor SMB disponíveis](#)

Redefinir e redescobrir domínios confiáveis

Você pode forçar a redescoberta de todos os domínios confiáveis. Isso pode ser útil quando os servidores de domínio confiáveis não estão respondendo adequadamente ou as relações de confiança foram alteradas. Somente domínios com confiança bidirecional com o domínio home, que é o domínio que contém a conta de computador do servidor CIFS, são descobertos.

Passo

1. Redefina e redescubra domínios confiáveis usando o `vserver cifs domain trusts rediscover` comando.

```
vserver cifs domain trusts rediscover -vserver vs1
```

Informações relacionadas

[Exibindo informações sobre domínios confiáveis descobertos](#)

Exibir informações sobre domínios confiáveis descobertos

Você pode exibir informações sobre os domínios confiáveis descobertos para o domínio doméstico do servidor CIFS, que é o domínio que contém a conta de computador do servidor CIFS. Isso pode ser útil quando você quiser saber quais domínios confiáveis são descobertos e como eles são solicitados na lista de domínios confiáveis descobertos.

Sobre esta tarefa

Apenas os domínios com confiança bidirecional com o domínio home são descobertos. Como o controlador de domínio (DC) do domínio home retorna a lista de domínios confiáveis em uma ordem determinada pelo DC, a ordem dos domínios dentro da lista não pode ser prevista. Ao exibir a lista de domínios confiáveis, você pode determinar a ordem de pesquisa para pesquisas de mapeamento de nomes de vários domínios.

As informações de domínio confiável exibidas são agrupadas por nó e máquina virtual de armazenamento (SVM).

Passo

1. Exiba informações sobre domínios confiáveis descobertos usando o `vserver cifs domain trusts show` comando.

```
vserver cifs domain trusts show -vserver vs1
```

```
Node: node1
Vserver: vs1

Home Domain          Trusted Domain
-----
EXAMPLE.COM          CIFS1.EXAMPLE.COM,
                     CIFS2.EXAMPLE.COM
                     EXAMPLE.COM

Node: node2
Vserver: vs1

Home Domain          Trusted Domain
-----
EXAMPLE.COM          CIFS1.EXAMPLE.COM,
                     CIFS2.EXAMPLE.COM
                     EXAMPLE.COM
```

Informações relacionadas

[Redefinir e redescobrir domínios confiáveis](#)

Adicione, remova ou substitua domínios confiáveis em listas de domínios confiáveis preferenciais

Pode adicionar ou remover domínios fidedignos da lista de domínios fidedignos preferidos para o servidor SMB ou pode modificar a lista atual. Se você configurar uma lista de domínio confiável preferencial, essa lista será usada em vez dos domínios confiáveis bidirecionais descobertos ao executar pesquisas de mapeamento de nomes de vários domínios.

Sobre esta tarefa

- Se você estiver adicionando domínios confiáveis a uma lista existente, a nova lista será mesclada com a lista existente com as novas entradas colocadas no final. Os domínios confiáveis são pesquisados na ordem em que aparecem na lista de domínios confiáveis.
- Se você estiver removendo domínios confiáveis da lista existente e não especificar uma lista, toda a lista de domínio confiável para a máquina virtual de armazenamento especificada (SVM) será removida.
- Se você modificar a lista existente de domínios confiáveis, a nova lista substituirá a lista existente.



Você deve inserir apenas domínios bidirecionalmente confiáveis na lista de domínios confiáveis preferidos. Mesmo que você possa inserir domínios confiáveis de saída ou entrada na lista de domínios preferidos, eles não são usados ao realizar pesquisas de mapeamento de nomes de vários domínios. O ONTAP pula a entrada do domínio unidirecional e passa para o próximo domínio confiável bidirecional na lista.

Passo

1. Execute uma das seguintes ações:

Se você quiser fazer o seguinte com a lista de domínios confiáveis preferenciais...	Use o comando...
Adicione domínios confiáveis à lista	<code>vserver cifs domain name-mapping-search add -vserver _vserver_name_-trusted-domains FQDN, ...</code>
Remova domínios confiáveis da lista	<code>vserver cifs domain name-mapping-search remove -vserver _vserver_name_-trusted-domains FQDN, ...]</code>
Modifique a lista existente	<code>vserver cifs domain name-mapping-search modify -vserver _vserver_name_-trusted-domains FQDN, ...</code>

Exemplos

O comando a seguir adiciona dois domínios confiáveis (cifs1.example.com e cifs2.example.com) à lista de domínios confiáveis preferida usada pelo SVM VS1:

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

O comando a seguir remove dois domínios confiáveis da lista usada pelo SVM VS1:

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

O comando a seguir modifica a lista de domínio confiável usada pelo SVM VS1. A nova lista substitui a lista original:

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

Informações relacionadas

[Exibindo informações sobre a lista de domínio confiável preferencial](#)

Exibir informações sobre a lista de domínios confiáveis preferencial

Você pode exibir informações sobre quais domínios confiáveis estão na lista de domínios confiáveis preferenciais e a ordem em que eles são pesquisados se as pesquisas de mapeamento de nomes de vários domínios estiverem ativadas. Você pode configurar uma lista de domínio confiável preferida como alternativa ao uso da lista de domínio confiável descoberta automaticamente.

Passos

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre o seguinte...	Use o comando...
Todos os domínios confiáveis preferenciais no cluster agrupados por máquina virtual de armazenamento (SVM)	<code>vserver cifs domain name-mapping-search show</code>
Todos os domínios confiáveis preferenciais para um SVM especificado	<code>vserver cifs domain name-mapping-search show -vserver vserver_name</code>

O comando a seguir exibe informações sobre todos os domínios confiáveis preferenciais no cluster:

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver          Trusted Domains
-----
vs1              CIFS1.EXAMPLE.COM
```

Informações relacionadas

[Adicionar, remover ou substituir domínios confiáveis em listas de domínios confiáveis preferenciais](#)

Crie e configure compartilhamentos SMB

Crie e configure a visão geral de compartilhamentos SMB

Para que usuários e aplicativos possam acessar dados no servidor CIFS em SMB, você deve criar e configurar compartilhamentos SMB, que é um ponto de acesso nomeado em um volume. Você pode personalizar compartilhamentos especificando parâmetros de compartilhamento e propriedades de compartilhamento. Você pode modificar um compartilhamento existente a qualquer momento.

Quando você cria um compartilhamento SMB, o ONTAP cria uma ACL padrão para as permissões de compartilhamento com controle total para todos.

Os compartilhamentos SMB estão vinculados ao servidor CIFS na máquina virtual de storage (SVM). Os compartilhamentos de SMB serão excluídos se o SVM for excluído ou se o servidor CIFS ao qual ele está associado for excluído do SVM. Se você recriar o servidor CIFS na SVM, será necessário recriar os

compartilhamentos SMB.

Informações relacionadas

[Gerencie o acesso a arquivos usando SMB](#)

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

[Configure o mapeamento de caracteres para a tradução de nomes de arquivo SMB em volumes](#)

Quais são os compartilhamentos administrativos padrão

Quando você cria um servidor CIFS na máquina virtual de storage (SVM), os compartilhamentos administrativos padrão são criados automaticamente. Você deve entender o que são esses compartilhamentos padrão e como eles são usados.

O ONTAP cria os seguintes compartilhamentos administrativos padrão quando você cria o servidor CIFS:



A partir do ONTAP 9.8, o compartilhamento admin não é mais criado por padrão.

- ipc
- (Somente ONTAP 9.7 e versões anteriores)
- c

Como os compartilhamentos que terminam com o caractere dólar são compartilhamentos ocultos, os compartilhamentos administrativos padrão não são visíveis em meu computador, mas você pode visualizá-los usando pastas compartilhadas.

Como os compartilhamentos padrão do ipc e do admin são usados

As ações do ONTAP são usadas pelos administradores do Windows e não podem ser usadas pelos administradores do Windows para acessar dados residentes no SVM.

- compartilhar

A ação ipc é um recurso que compartilha os pipes nomeados que são essenciais para a comunicação entre programas. O compartilhamento ipc é usado durante a administração remota de um computador e ao visualizar os recursos compartilhados de um computador. Não é possível alterar as configurações de compartilhamento, propriedades de compartilhamento ou ACLs do compartilhamento ipc. Você também não pode renomear ou excluir o compartilhamento ipc.

- Compartilhar (somente ONTAP 9.7 e anteriores)



A partir do ONTAP 9.8, o compartilhamento admin não é mais criado por padrão.

O compartilhamento admin é usado durante a administração remota do SVM. O caminho desse recurso é sempre o caminho para a raiz do SVM. Você não pode alterar as configurações de compartilhamento, propriedades de compartilhamento ou ACLs para o compartilhamento admin. Você também não pode renomear ou excluir o compartilhamento admin.

Como o compartilhamento padrão c

O compartilhamento de CAD é um compartilhamento administrativo que o cluster ou o administrador do SVM

pode usar para acessar e gerenciar o volume raiz do SVM.

A seguir estão as características da participação:

- O caminho para esse compartilhamento é sempre o caminho para o volume raiz da SVM e não pode ser modificado.
- ACL padrão para o compartilhamento c

Este utilizador é o administrador. Por padrão, o administrador do BUILTIN pode mapear para o compartilhamento e exibição, criar, modificar ou excluir arquivos e pastas no diretório raiz mapeado. Cuidado deve ser exercido ao gerenciar arquivos e pastas neste diretório.

- Você pode alterar a ACL do compartilhamento.
- Você pode alterar as configurações de compartilhamento e as propriedades de compartilhamento.
- Não é possível eliminar a partilha c
- O administrador do SVM pode acessar o restante do namespace SVM a partir do compartilhamento mapeado por meio do cruzamento das junções do namespace.
- O compartilhamento c pode ser acessado usando o Console de Gerenciamento da Microsoft.

Informações relacionadas

[Configurando permissões avançadas de arquivos NTFS usando a guia Segurança do Windows](#)

Requisitos de nomenclatura para compartilhamento de SMB

Você deve manter os requisitos de nomenclatura do compartilhamento do ONTAP em mente ao criar compartilhamentos SMB no seu servidor SMB.

As convenções de nomes de compartilhamento para ONTAP são as mesmas que para o Windows e incluem os seguintes requisitos:

- O nome de cada compartilhamento deve ser exclusivo para o servidor SMB.
- Nomes de compartilhamento não diferenciam maiúsculas de minúsculas.
- O comprimento máximo do nome da partilha é de 80 caracteres.
- Nomes de compartilhamento Unicode são suportados.
- Nomes de compartilhamento que terminam com o caractere dólar são compartilhamentos ocultos.
- Para o ONTAP 9.7 e anteriores, os compartilhamentos administrativos são criados automaticamente em todos os servidores CIFS e são nomes de compartilhamento reservados. A partir do ONTAP 9.8, o compartilhamento admin não é mais criado automaticamente.
- Você não pode usar o nome de compartilhamento ONTAP_ADMIN ao criar um compartilhamento.
- Nomes de compartilhamento que contêm espaços são suportados:
 - Você não pode usar um espaço como o primeiro caractere ou como o último caractere em um nome de compartilhamento.
 - Você deve incluir nomes de compartilhamento contendo um espaço entre aspas.



As aspas simples são consideradas parte do nome da partilha e não podem ser utilizadas no lugar das aspas.

- Os seguintes caracteres especiais são suportados quando você nomeia compartilhamentos SMB:
! A % e ' _ - . Clique em "OK"
- Os seguintes caracteres especiais não são suportados quando você nomeia compartilhamentos SMB:
 - " / : ; | > , ? *

Requisitos de sensibilidade de caso de diretório ao criar compartilhamentos em um ambiente multiprotocolo

Se você criar compartilhamentos em um SVM em que o esquema de nomenclatura 8,3 seja usado para distinguir entre nomes de diretórios onde haja apenas diferenças de casos entre os nomes, você deve usar o nome 8,3 no caminho de compartilhamento para garantir que o cliente se conecte ao caminho de diretório desejado.

No exemplo a seguir, dois diretórios chamados "testdir" e "TESTDIR" foram criados em um cliente Linux. O caminho de junção do volume que contém os diretórios é /home. A primeira saída é de um cliente Linux e a segunda saída é de um cliente SMB.

```
ls -l
drwxrwxr-x 2 user1 group1 4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1 4096 Apr 17 11:24 TESTDIR
```

```
dir

Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

Ao criar um compartilhamento no segundo diretório, você deve usar o nome 8,3 no caminho de compartilhamento. Neste exemplo, o caminho de compartilhamento para o primeiro diretório é /home/testdir e o caminho de compartilhamento para o segundo diretório é /home/TESTDI~1.

Use propriedades de compartilhamento SMB

Use a visão geral das propriedades de compartilhamento SMB

Você pode personalizar as propriedades dos compartilhamentos SMB.

As propriedades de compartilhamento disponíveis são as seguintes:

Compartilhar propriedades	Descrição
oplocks	Esta propriedade especifica que o compartilhamento usa bloqueios oportunistas, também conhecidos como cache do lado do cliente.

Compartilhar propriedades	Descrição
browsable	Esta propriedade permite que os clientes Windows naveguem na partilha.
showsnapshot	Essa propriedade especifica que as cópias Snapshot podem ser visualizadas e atravessadas por clientes.
changenotify	Esta propriedade especifica que o compartilhamento suporta solicitações Change Notify. Para compartilhamentos em um SVM, esta é uma propriedade inicial padrão.
attributecache	Essa propriedade permite que o cache de atributos de arquivo no compartilhamento SMB forneça acesso mais rápido aos atributos. O padrão é desabilitar o cache de atributos. Esta propriedade só deve ser ativada se houver clientes conetando-se a compartilhamentos sobre SMB 1,0. Essa propriedade de compartilhamento não se aplica se os clientes estiverem se conetando a compartilhamentos em SMB 2.x ou SMB 3,0.
continuously-available	Esta propriedade permite que clientes SMB que a suportam para abrir arquivos de forma persistente. Os arquivos abertos desta maneira são protegidos contra eventos disruptivos, como failover e giveback.
branchcache	Esta propriedade especifica que o compartilhamento permite que os clientes solicitem hashes BranchCache nos arquivos desse compartilhamento. Esta opção é útil somente se você especificar "per-share" como o modo operacional na configuração do CIFS BranchCache.
access-based-enumeration	Esta propriedade especifica que <i>Access Based Enumeração</i> (ABE) está ativada neste compartilhamento. As pastas compartilhadas filtradas por ABE são visíveis para um usuário com base nos direitos de acesso desse usuário individual, impedindo a exibição de pastas ou outros recursos compartilhados que o usuário não tem direitos de acesso.

Compartilhar propriedades	Descrição
namespace-caching	Esta propriedade especifica que os clientes SMB que se conetam a esse compartilhamento podem armazenar em cache os resultados da enumeração de diretórios retornados pelos servidores CIFS, o que pode fornecer melhor desempenho. Por padrão, os clientes SMB 1 não armazenam em cache os resultados da enumeração de diretórios. Como os clientes SMB 2 e SMB 3 armazenam resultados de enumeração de diretório em cache por padrão, especificar essa propriedade de compartilhamento fornece benefícios de desempenho apenas para conexões de cliente SMB 1.
encrypt-data	Esta propriedade especifica que a criptografia SMB deve ser usada ao acessar esse compartilhamento. Os clientes SMB que não suportam encriptação ao acessar a dados SMB não poderão acessar a esta partilha.

Adicione ou remova propriedades de compartilhamento em um compartilhamento SMB existente

Você pode personalizar um compartilhamento SMB existente adicionando ou removendo propriedades de compartilhamento. Isso pode ser útil se você quiser alterar a configuração de compartilhamento para atender às mudanças nos requisitos do seu ambiente.

Antes de começar

O compartilhamento cujas propriedades você deseja modificar deve existir.

Sobre esta tarefa

Diretrizes para adicionar propriedades de compartilhamento:

- Você pode adicionar uma ou mais propriedades de compartilhamento usando uma lista delimitada por vírgulas.
- Quaisquer propriedades de compartilhamento que você especificou anteriormente permanecem em vigor.

As propriedades recém-adicionadas são anexadas à lista existente de propriedades de compartilhamento.

- Se você especificar um novo valor para as propriedades de compartilhamento que já são aplicadas ao compartilhamento, o valor recém-especificado substituirá o valor original.
- Não é possível remover propriedades de compartilhamento usando o `vserver cifs share properties add` comando.

Você pode usar o `vserver cifs share properties remove` comando para remover propriedades de compartilhamento.

Diretrizes para remover propriedades de compartilhamento:

- Você pode remover uma ou mais propriedades de compartilhamento usando uma lista delimitada por vírgulas.
- Todas as propriedades de compartilhamento que você especificou anteriormente, mas não as remove, permanecem em vigor.

Passos

1. Introduza o comando adequado:

Se você quiser...	Digite o comando...
Adicione propriedades de compartilhamento	<pre>vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...</pre>
Remover propriedades de compartilhamento	<pre>vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...</pre>

2. Verifique as configurações da propriedade de compartilhamento: `vserver cifs share show -vserver vserver_name -share-name share_name`

Exemplos

O comando a seguir adiciona a `showsnapshot` propriedade share a uma ação chamada "hare1" no SVM VS1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot
```

```
cluster1::> vserver cifs share show -vserver vs1
Vserver      Share      Path        Properties      Comment      ACL
-----      -
vs1          share1    /share1     oplocks        -            Everyone / Full
Control
                browsable
                changenotify
                showsnapshot
```

O comando a seguir remove a `browsable` propriedade share de um compartilhamento chamado "hare2" no SVM VS1:

```

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver      Share      Path        Properties  Comment     ACL
-----      -
vs1          share2    /share2     oplocks    -           Everyone / Full
Control
                                changenotify

```

Informações relacionadas

[Comandos para gerenciar compartilhamentos SMB](#)

Otimize o acesso do usuário SMB com a configuração de compartilhamento de grupo de força

Quando você cria um compartilhamento da linha de comando ONTAP para dados com segurança efetiva UNIX, você pode especificar que todos os arquivos criados por usuários SMB nesse compartilhamento pertencem ao mesmo grupo, conhecido como *force-group*, que deve ser um grupo predefinido no banco de dados de grupos UNIX. O uso de um grupo de força torna mais fácil garantir que os arquivos possam ser acessados por usuários SMB pertencentes a vários grupos.

Especificar um grupo de força é significativo apenas se o compartilhamento estiver em um UNIX ou em uma *qtree* misto. Não há necessidade de definir um grupo de força para compartilhamentos em um volume NTFS ou *qtree* porque o acesso a arquivos nesses compartilhamentos é determinado pelas permissões do Windows, não GIDs UNIX.

Se um grupo de força tiver sido especificado para uma ação, o seguinte se tornará verdadeiro para a partilha:

- Os usuários SMB no grupo de força que acessam esse compartilhamento são temporariamente alterados para o GID do grupo de força.

Este GID permite que eles acessem arquivos neste compartilhamento que não são acessíveis normalmente com seu GID principal ou UID.

- Todos os arquivos neste compartilhamento criados por usuários SMB pertencem ao mesmo grupo de força, independentemente do GID principal do proprietário do arquivo.

Quando os usuários SMB tentam acessar um arquivo criado pelo NFS, os GIDs principais dos usuários SMB determinam os direitos de acesso.

O grupo *force* não afeta a forma como os usuários NFS acessam arquivos neste compartilhamento. Um arquivo criado por NFS adquire o GID do proprietário do arquivo. A determinação das permissões de acesso é baseada no UID e GID principal do usuário NFS que está tentando acessar o arquivo.

O uso de um grupo de força torna mais fácil garantir que os arquivos possam ser acessados por usuários SMB pertencentes a vários grupos. Por exemplo, se você quiser criar um compartilhamento para armazenar as páginas da Web da empresa e dar acesso de gravação a usuários nos departamentos de Engenharia e Marketing, você pode criar um compartilhamento e dar acesso de gravação a um grupo de força chamado "webgroup1". Devido ao grupo *force*, todos os arquivos criados por usuários SMB neste compartilhamento

são de propriedade do grupo "webgroup1". Além disso, os usuários recebem automaticamente o GID do grupo "webgroup1" ao acessar o compartilhamento. Como resultado, todos os usuários podem escrever para esse compartilhamento sem que você precise gerenciar os direitos de acesso dos usuários nos departamentos de Engenharia e Marketing.

Informações relacionadas

[Criando um compartilhamento SMB com a configuração de compartilhamento de grupo de força](#)

Crie um compartilhamento SMB com a configuração de compartilhamento de grupo de força

Você pode criar um compartilhamento SMB com a configuração de compartilhamento de grupo de força se desejar que os usuários de SMB que acessam dados em volumes ou qtrees com segurança de arquivos UNIX sejam considerados pelo ONTAP como pertencentes ao mesmo grupo UNIX.

Passo

1. Crie o compartilhamento SMB: `vserver cifs share create -vserver vserver_name -share -name share_name -path path -force-group-for-create UNIX_group_name`

Se o caminho UNC (\\servername\sharename\filepath) do compartilhamento contiver mais de 256 caracteres (excluindo o " " inicial\ no caminho UNC), a guia **Segurança** na caixa Propriedades do Windows não estará disponível. Este é um problema de cliente do Windows em vez de um problema de ONTAP. Para evitar esse problema, não crie compartilhamentos com caminhos UNC com mais de 256 caracteres.

Se você quiser remover o grupo de força depois que o compartilhamento é criado, você pode modificar o compartilhamento a qualquer momento e especificar uma string vazia ("") como o valor para o `-force-group-for-create` parâmetro. Se você remover o grupo de força modificando o compartilhamento, todas as conexões existentes a esse compartilhamento continuarão tendo o grupo de força definido anteriormente como GID principal.

Exemplo

O comando a seguir cria um compartilhamento "webpages" que é acessível na Web no /corp/companyinfo diretório no qual todos os arquivos criados pelos usuários SMB são atribuídos ao grupo webgroup1:

```
vserver cifs share create -vserver vs1 -share-name webpages -path /corp/companyinfo -force-group-for-create webgroup1
```

Informações relacionadas

[Otimize o acesso do usuário SMB com a configuração de compartilhamento de grupo de força](#)

Exibir informações sobre compartilhamentos SMB usando o MMC

Você pode exibir informações sobre compartilhamentos SMB no SVM e executar algumas tarefas de gerenciamento usando o Console de Gerenciamento da Microsoft (MMC). Antes de poder visualizar os compartilhamentos, você precisa conectar o MMC ao SVM.

Sobre esta tarefa

Você pode executar as seguintes tarefas em compartilhamentos contidos em SVMs usando o MMC:

- Ver compartilhamentos
- Ver sessões ativas
- Exibir arquivos abertos
- Enumerar a lista de sessões, ficheiros e ligações em árvore no sistema
- Feche os ficheiros abertos no sistema
- Feche as sessões abertas
- Criar/gerenciar compartilhamentos



As visualizações exibidas pelos recursos anteriores são específicas de nós e não específicas de cluster. Portanto, quando você usa o MMC para se conectar ao nome do host do servidor SMB (ou seja, cifs01.domain.local), você é encaminhado, com base em como configurou o DNS, para um único LIF dentro do cluster.

As seguintes funções não são suportadas no MMC para ONTAP:

- Criando novos usuários/grupos locais
- Gerir/visualizar utilizadores/grupos locais existentes
- Visualização de eventos ou registos de desempenho
- Armazenamento
- Serviços e aplicações

Nos casos em que a operação não é suportada, você pode ter `remote procedure call failed` erros.

["Perguntas frequentes: Usando o Windows MMC com ONTAP"](#)

Passos

1. Para abrir o MMC de Gerenciamento de computador em qualquer servidor Windows, no **Painel de Controle**, selecione **Ferramentas administrativas > Gerenciamento de computador**.
2. Selecione **Ação > ligar a outro computador**.

A caixa de diálogo Selecionar computador é exibida.

3. Digite o nome do sistema de armazenamento ou clique em **Procurar** para localizar o sistema de armazenamento.
4. Clique em **OK**.

O MMC se conecta ao SVM.

5. No painel de navegação, clique em **pastas compartilhadas > compartilhamentos**.

Uma lista de compartilhamentos no SVM é exibida no painel de exibição direito.

6. Para exibir as propriedades de compartilhamento de um compartilhamento, clique duas vezes no compartilhamento para abrir a caixa de diálogo **Propriedades**.
7. Se você não puder se conectar ao sistema de armazenamento usando o MMC, você poderá adicionar o usuário ao grupo BUILTIN ou BUILTIN/Power Users usando um dos seguintes comandos no sistema de armazenamento:

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

Comandos para gerenciar compartilhamentos SMB

Use os `vserver cifs share` comandos e `vserver cifs share properties` para gerenciar compartilhamentos SMB.

Se você quiser...	Use este comando...
Crie um compartilhamento SMB	<code>vserver cifs share create</code>
Exibir compartilhamentos SMB	<code>vserver cifs share show</code>
Modificar um compartilhamento SMB	<code>vserver cifs share modify</code>
Excluir um compartilhamento SMB	<code>vserver cifs share delete</code>
Adicione propriedades de compartilhamento a um compartilhamento existente	<code>vserver cifs share properties add</code>
Remover propriedades de compartilhamento de um compartilhamento existente	<code>vserver cifs share properties remove</code>
Exibir informações sobre as propriedades de compartilhamento	<code>vserver cifs share properties show</code>

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

Proteja o acesso a arquivos usando ACLs de compartilhamento SMB

Diretrizes para gerenciar ACLs de nível de compartilhamento SMB

Você pode alterar ACLs de nível de compartilhamento para dar aos usuários mais ou menos direitos de acesso ao compartilhamento. Você pode configurar ACLs de nível de compartilhamento usando usuários e grupos do Windows ou usuários e grupos UNIX.

Por padrão, a ACL de nível de compartilhamento dá controle total ao grupo padrão chamado Everyone. Controle total na ACL significa que todos os usuários no domínio e todos os domínios confiáveis têm acesso total ao compartilhamento. Você pode controlar o nível de acesso de uma ACL de nível de compartilhamento usando o ["Console de Gerenciamento Microsoft \(MMC\) em um cliente Windows ou na linha de comando ONTAP"](#).

As diretrizes a seguir se aplicam quando você usa o MMC:

- Os nomes de usuário e grupo especificados devem ser nomes do Windows.
- Você pode especificar apenas permissões do Windows.

As diretrizes a seguir se aplicam quando você usa a linha de comando ONTAP:

- Os nomes de usuário e grupo especificados podem ser nomes do Windows ou nomes UNIX.

Se um tipo de usuário e grupo não for especificado ao criar ou modificar ACLs, o tipo padrão será usuários e grupos do Windows.

- Você pode especificar apenas permissões do Windows.

Criar listas de controle de acesso de compartilhamento SMB

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

Sobre esta tarefa

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

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

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

Passos

1. Exclua a ACL de compartilhamento padrão: `vserver cifs share access-control delete -vserver <vserver_name> -share <share_name> -user-or-group everyone`
2. Configure a nova ACL:

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

Se você quiser configurar ACLs usando um...	Digite o comando...
Utilizador UNIX	<pre>vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix- user> -user-or-group <UNIX_user_name> -permission <access_right></pre>
Grupo UNIX	<pre>vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix- group> -user-or-group <UNIX_group_name> -permission <access_right></pre>

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

Exemplo

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

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

cluster1:~> vserver cifs share access-control show -vserver
vs1.example.com
```

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

O comando a seguir `Read` dá permissão ao grupo UNIX "Engineering" para o compartilhamento "eng" no SVM "vs2.example.com":

```

cluster1::> vsserver cifs share access-control create -vsserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vsserver cifs share access-control show -vsserver
vs2.example.com

```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs2.example.com	c\$	BUILTIN\Administrators	windows	Full_Control
vs2.example.com	eng	engineering	unix-group	Read

Os comandos a seguir Change dão permissão ao grupo local do Windows chamado "Tiger Team" e Full_Control permissão ao usuário local do Windows chamado "Sue Chang" para o compartilhamento "datavol5" no SVM "VS1":

```

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

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

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

```

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

Comandos para gerenciar listas de controle de acesso de compartilhamento SMB

Você precisa saber os comandos para gerenciar listas de controle de acesso (ACLs) SMB, o que inclui criar, exibir, modificar e excluir.

Se você quiser...	Use este comando...
Crie uma nova ACL	<code>vserver cifs share access-control create</code>
Exibir ACLs	<code>vserver cifs share access-control show</code>
Modificar uma ACL	<code>vserver cifs share access-control modify</code>
Eliminar uma ACL	<code>vserver cifs share access-control delete</code>

Proteja o acesso aos arquivos usando permissões de arquivo

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

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

Antes de começar

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

Sobre esta tarefa

A configuração de permissões de arquivos NTFS é feita em um host do Windows adicionando entradas a listas de controle de acesso discricionárias (DACLS) NTFS associadas a um descritor de segurança NTFS. O descritor de segurança é então aplicado a arquivos e diretórios NTFS. Essas tarefas são tratadas automaticamente pela GUI do Windows.

Passos

1. No menu **Ferramentas** no Windows Explorer, selecione **Mapear unidade de rede**.
2. Preencha a caixa de diálogo **Map Network Drive**:
 - a. Selecione uma letra **Drive**.
 - b. Na caixa **pasta**, digite o nome do servidor CIFS que contém o compartilhamento que contém os dados aos quais você deseja aplicar permissões e o nome do compartilhamento.

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



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

- a. Clique em **Finish**.

A unidade selecionada está montada e pronta com a janela do Windows Explorer exibindo arquivos e pastas contidos no compartilhamento.

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

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

6. Clique em **Avançado**.

A janela Propriedades do Windows exibe informações sobre permissões de arquivo existentes atribuídas a usuários e grupos.

7. Clique em **alterar permissões**.

A janela permissões é aberta.

8. Execute as ações desejadas:

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

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

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

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

10. Na caixa **Permissions**, selecione as caixas **allow** ou **deny** para as permissões avançadas que você deseja definir neste objeto.
 - Para permitir o acesso especificado, selecione a caixa **permitir**.

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

◦ * Controle total*

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

◦ * Traverse pasta / executar arquivo *

◦ **Lista de pastas / dados de leitura**

◦ **Leia atributos**

◦ **Leia atributos estendidos**

◦ * Criar arquivos / escrever dados *

◦ * Criar pastas / anexar dados*

◦ * Escrever atributos*

◦ **Escreva atributos estendidos**

◦ **Excluir subpastas e arquivos**

◦ **Excluir**

◦ **Permissões de leitura**

◦ **Alterar permissões**

◦ **Assuma a propriedade**



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

11. Se você quiser que subpastas e arquivos desse objeto herdem essas permissões, marque a caixa **aplicar essas permissões a objetos e/ou contentores dentro desse contentor somente**.

12. Clique em **OK**.

13. Depois de terminar de adicionar, remover ou editar permissões NTFS, especifique a configuração de herança para este objeto:

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

Este é o padrão.

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

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



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

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

14. Clique em **OK** para fechar a caixa **permissões**.

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

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

Informações relacionadas

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

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

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

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

Configurar permissões de arquivos NTFS usando a CLI do ONTAP

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

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

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

Passos

1. Crie um descritor de segurança NTFS.

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

2. Adicione DACLS ao descritor de segurança NTFS.

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

```
{this-folder|sub-folders|files}
```

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

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

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

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

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

- Permissões de exportação

Configurar permissões de exportação para o acesso SMB é opcional.

- Permissões de compartilhamento
- Permissões de arquivo

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

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

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



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

Acesso seguro a arquivos usando o controle de acesso dinâmico (DAC)

Proteja o acesso a ficheiros utilizando a visão geral do controlo de acesso dinâmico (DAC)

Você pode proteger o acesso usando o Controle de Acesso Dinâmico e criando políticas de acesso centrais no ative Directory e aplicando-as a arquivos e pastas em SVMs por meio de objetos de Diretiva de Grupo aplicados (GPOs). Você pode configurar a auditoria para usar eventos de preparação de políticas de acesso central para ver os efeitos das alterações nas políticas de acesso central antes de aplicá-las.

Adições às credenciais CIFS

Antes do Controle de Acesso Dinâmico, uma credencial CIFS incluía a identidade de um responsável de segurança (o usuário) e a associação de grupo do Windows. Com o Dynamic Access Control, mais três tipos de informações são adicionados à identidade do dispositivo, às declarações do dispositivo e às declarações do usuário:

- Identidade do dispositivo

O análogo das informações de identidade do usuário, exceto se for a identidade e associação de grupo do dispositivo do qual o usuário está fazendo login.

- Reclamações do dispositivo

Afirmações sobre um dispositivo principal de segurança. Por exemplo, uma alegação de dispositivo pode ser que ela seja membro de uma ou específica.

- Reclamações do utilizador

Afirmações sobre um responsável de segurança do usuário. Por exemplo, uma alegação de usuário pode ser que sua conta do AD seja membro de uma ou específica.

Políticas de acesso central

As políticas de acesso central para arquivos permitem que as organizações implantem e gerenciem centralmente políticas de autorização que incluem expressões condicionais usando grupos de usuários, reivindicações de usuários, declarações de dispositivos e propriedades de recursos.

Por exemplo, para acessar dados de alto impacto nos negócios, um usuário precisa ser um funcionário em tempo integral e ter acesso apenas aos dados de um dispositivo gerenciado. As políticas de acesso central são definidas no ative Directory e distribuídas para servidores de arquivos através do mecanismo GPO.

Preparação de políticas de acesso central com auditoria avançada

As políticas de acesso central podem ser "envelhecidas", caso em que são avaliadas de forma "What-if" durante as verificações de acesso ao arquivo. Os resultados do que teria acontecido se a política estivesse em vigor e como isso difere do que está configurado atualmente são registrados como um evento de auditoria. Dessa forma, os administradores podem usar logs de eventos de auditoria para estudar o impacto de uma alteração de política de acesso antes de realmente colocar a política em jogo. Depois de avaliar o impacto de uma alteração de política de acesso, a política pode ser implantada via GPOs nos SVMs desejados.

Informações relacionadas

[GPOs compatíveis](#)

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

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

[Exibindo informações sobre as configurações do GPO](#)

[Exibindo informações sobre políticas de acesso central](#)

[Exibindo informações sobre as regras da política de acesso central](#)

[Configuração de políticas de acesso central para proteger dados em servidores CIFS](#)

Funcionalidade de controle de acesso dinâmico suportada

Se você quiser usar o controle de acesso dinâmico (DAC) em seu servidor CIFS, você precisa entender como o ONTAP suporta a funcionalidade de controle de acesso dinâmico em ambientes do Active Directory.

Suportado para controle de acesso dinâmico

O ONTAP suporta a seguinte funcionalidade quando o controle de acesso dinâmico está ativado no servidor CIFS:

Funcionalidade	Comentários
Reclamações no sistema de arquivos	Reivindicações são pares simples de nome e valor que afirmam alguma verdade sobre um usuário. As credenciais do usuário contêm informações de reclamação, e os descritores de segurança nos arquivos podem executar verificações de acesso que incluem verificações de reclamações. Isso dá aos administradores um nível mais alto de controle sobre quem pode acessar arquivos.
Expressões condicionais para verificações de acesso a arquivos	Ao modificar os parâmetros de segurança de um arquivo, os usuários podem adicionar expressões condicionais arbitrariamente complexas ao descritor de segurança do arquivo. A expressão condicional pode incluir verificações para reclamações.
Controle central do acesso a arquivos através de políticas de acesso central	As políticas de acesso central são um tipo de ACL armazenada no Active Directory que pode ser marcada para um arquivo. O acesso ao arquivo só é concedido se as verificações de acesso do descritor de segurança no disco e da diretiva de acesso central marcada permitirem o acesso. Isso dá aos administradores a capacidade de controlar o acesso a arquivos de um local central (AD) sem ter que modificar o descritor de segurança no disco.
Preparação da política de acesso central	Adiciona a capacidade de testar alterações de segurança sem afetar o acesso real aos arquivos, "definindo" uma alteração nas políticas de acesso central e vendo o efeito da alteração em um relatório de auditoria.
Suporte para exibir informações sobre a segurança da diretiva de acesso central usando a CLI do ONTAP	Estende o <code>vserver security file-directory show</code> comando para exibir informações sobre políticas de acesso centrais aplicadas.

Funcionalidade	Comentários
Rastreamento de segurança que inclui políticas de acesso central	Estende a <code>vserver security trace</code> família de comandos para exibir resultados que incluem informações sobre políticas de acesso central aplicadas.

Não suportado para o controle de acesso dinâmico

O ONTAP não suporta a seguinte funcionalidade quando o controle de acesso dinâmico está ativado no servidor CIFS:

Funcionalidade	Comentários
Classificação automática de objetos do sistema de arquivos NTFS	Esta é uma extensão para a infra-estrutura de classificação de ficheiros do Windows que não é suportada no ONTAP.
Auditoria avançada que não a preparação de políticas de acesso central	Somente o estadiamento da política de acesso central é suportado para auditoria avançada.

Considerações ao usar o Controle de Acesso Dinâmico e políticas de Acesso Central com servidores CIFS

Há certas considerações que você deve ter em mente ao usar o controle de acesso dinâmico (DAC) e as políticas de acesso central para proteger arquivos e pastas em servidores CIFS.

O acesso NFS pode ser negado ao root se a regra de política se aplicar ao usuário do domínio/administrador

Em determinadas circunstâncias, o acesso NFS à raiz pode ser negado quando a segurança da diretiva de acesso central é aplicada aos dados que o usuário raiz está tentando acessar. O problema ocorre quando a política de acesso central contém uma regra que é aplicada ao domínio/administrador e a conta raiz é mapeada para a conta de domínio/administrador.

Em vez de aplicar uma regra ao utilizador de domínio/administrador, deve aplicar a regra a um grupo com Privileges administrativo, como o grupo de domínio/administradores. Desta forma, pode mapear a raiz para a conta de domínio/administrador sem que a raiz seja afetada por este problema.

O grupo BUILTIN/Administradores do servidor CIFS tem acesso a recursos quando a diretiva de acesso central aplicado não é encontrada no ative Directory

É possível que os recursos contidos no servidor CIFS tenham políticas de acesso central aplicadas a eles, mas quando o servidor CIFS usa o SID da política de acesso central para tentar recuperar informações do ative Directory, o SID não corresponde a nenhum SIDs de política de acesso central existente no ative Directory. Nestas circunstâncias, o servidor CIFS aplica a política de recuperação padrão local para esse recurso.

A política de recuperação padrão local permite o acesso do grupo BUILTIN/Administradores do servidor CIFS a esse recurso.

Ativar ou desativar a descrição geral do controle de Acesso Dinâmico

A opção que permite utilizar o controle de Acesso Dinâmico (DAC) para proteger objetos no servidor CIFS está desativada por predefinição. Você deve ativar a opção se quiser usar o Controle de Acesso Dinâmico no servidor CIFS. Se decidir mais tarde que não pretende utilizar o controle de Acesso Dinâmico para proteger objetos armazenados no servidor CIFS, pode desativar a opção.

Sobre esta tarefa

Uma vez que o Controle de Acesso Dinâmico esteja ativado, o sistema de arquivos pode conter ACLs com entradas relacionadas ao Controle de Acesso Dinâmico. Se o controle de Acesso Dinâmico estiver desativado, as entradas atuais do controle de Acesso Dinâmico serão ignoradas e as novas não serão permitidas.

Esta opção está disponível apenas no nível de privilégio avançado.

Passo

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

Se você quiser que o Controle de Acesso Dinâmico seja...	Digite o comando...
Ativado	<code>vserver cifs options modify -vserver vserver_name -is-dac-enabled true</code>
Desativado	<code>vserver cifs options modify -vserver vserver_name -is-dac-enabled false</code>

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

Informações relacionadas

[Configuração de políticas de acesso central para proteger dados em servidores CIFS](#)

Gerencie ACLs que contêm ACEs de controle de acesso dinâmico quando o controle de acesso dinâmico estiver desativado

Se você tiver recursos que têm ACLs aplicadas com ACEs de controle de acesso dinâmico e desativar o controle de acesso dinâmico na máquina virtual de armazenamento (SVM), remova os ACEs de controle de acesso dinâmico antes de gerenciar os ACEs de controle de acesso não dinâmico nesse recurso.

Sobre esta tarefa

Depois de o controle de acesso dinâmico ser desativado, não é possível remover os ACEs de controle de acesso não dinâmico existentes nem adicionar novos ACEs de controle de acesso não dinâmico até ter removido os ACEs de controle de acesso dinâmico existentes.

Você pode usar qualquer ferramenta usada normalmente para gerenciar ACLs para executar essas etapas.

Passos

1. Determine quais ACEs do controle de acesso dinâmico são aplicados ao recurso.
2. Remova os ACEs de controle de acesso dinâmico do recurso.
3. Adicione ou remova ACEs não-Dynamic Access Control conforme desejado do recurso.

Configurar políticas de acesso central para proteger dados em servidores CIFS

Há várias etapas que você deve seguir para proteger o acesso aos dados no servidor CIFS usando políticas de acesso central, incluindo habilitar o DAC (Dynamic Access Control) no servidor CIFS, configurar políticas de acesso central no active Directory, aplicar as políticas de acesso central a contentores do active Directory com GPOs e habilitar GPOs no servidor CIFS.

Antes de começar

- O active Directory deve ser configurado para usar políticas de acesso central.
- Você precisa ter acesso suficiente nos controladores de domínio do active Directory para criar políticas de acesso centrais e para criar e aplicar GPOs aos contêineres que contêm os servidores CIFS.
- Você precisa ter acesso administrativo suficiente na máquina virtual de storage (SVM) para executar os comandos necessários.

Sobre esta tarefa

As políticas de acesso central são definidas e aplicadas a objetos de diretiva de grupo (GPOs) no active Directory. Você pode consultar a Biblioteca Microsoft TechNet para obter instruções sobre como configurar políticas de acesso central e GPOs.

["Microsoft TechNet Library"](#)

Passos

1. Ative o controle de acesso dinâmico na SVM se ele ainda não estiver habilitado usando o `vserver cifs options modify` comando.

```
vserver cifs options modify -vserver vs1 -is-dac-enabled true
```

2. Habilite os objetos de diretiva de grupo (GPOs) no servidor CIFS se eles ainda não estiverem habilitados usando o `vserver cifs group-policy modify` comando.

```
vserver cifs group-policy modify -vserver vs1 -status enabled
```

3. Crie regras de acesso central e políticas de acesso central no active Directory.
4. Crie um objeto de diretiva de grupo (GPO) para implantar as políticas de acesso central no active Directory.
5. Aplique o GPO ao recipiente onde a conta do computador do servidor CIFS está localizada.
6. Atualize manualmente os GPOs aplicados ao servidor CIFS usando o `vserver cifs group-policy update` comando.

```
vserver cifs group-policy update -vserver vs1
```

7. Verifique se a diretiva de acesso central GPO é aplicada aos recursos no servidor CIFS usando o `vserver cifs group-policy show-applied` comando.

O exemplo a seguir mostra que a Diretiva de domínio padrão tem duas diretivas de acesso central

aplicadas ao servidor CIFS:

```
vserver cifs group-policy show-applied
```

```
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: all-versions
```

```
Security Settings:
```

```
  Event Audit and Event Log:
```

```
    Audit Logon Events: none
```

```
    Audit Object Access: success
```

```
    Log Retention Method: overwrite-as-needed
```

```
    Max Log Size: 16384
```

```
File Security:
```

```
  /voll/home
```

```
  /voll/dir1
```

```
Kerberos:
```

```
  Max Clock Skew: 5
```

```
  Max Ticket Age: 10
```

```
  Max Renew Age: 7
```

```
Privilege Rights:
```

```
  Take Ownership: usr1, usr2
```

```
  Security Privilege: usr1, usr2
```

```
  Change Notify: usr1, usr2
```

```
Registry Values:
```

```
  Signing Required: false
```

```
Restrict Anonymous:
```

```
  No enumeration of SAM accounts: true
```

```
  No enumeration of SAM accounts and shares: false
```

```
  Restrict anonymous access to shares and named pipes: true
```

```
  Combined restriction for anonymous user: no-access
```

```
Restricted Groups:
```

```
  gpr1
```

```
  gpr2
```

```
Central Access Policy Settings:
```

```
  Policies: cap1
```

cap2

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: all-versions

Security Settings:

Event Audit and Event Log:

Audit Logon Events: none

Audit Object Access: success

Log Retention Method: overwrite-as-needed

Max Log Size: 16384

File Security:

/voll/home

/voll/dir1

Kerberos:

Max Clock Skew: 5

Max Ticket Age: 10

Max Renew Age: 7

Privilege Rights:

Take Ownership: usr1, usr2

Security Privilege: usr1, usr2

Change Notify: usr1, usr2

Registry Values:

Signing Required: false

Restrict Anonymous:

No enumeration of SAM accounts: true

No enumeration of SAM accounts and shares: false

Restrict anonymous access to shares and named pipes: true

Combined restriction for anonymous user: no-access

Restricted Groups:

gpr1

gpr2

Central Access Policy Settings:

Policies: cap1

cap2

2 entries were displayed.

Informações relacionadas

[Exibindo informações sobre as configurações do GPO](#)

[Exibindo informações sobre políticas de acesso central](#)

[Exibindo informações sobre as regras da política de acesso central](#)

[Ativar ou desativar o controle de acesso dinâmico](#)

Apresentar informações sobre a segurança do controle de acesso dinâmico

Pode apresentar informações sobre a segurança do controle de acesso dinâmico (DAC) em volumes NTFS e em dados com segurança eficaz NTFS em volumes mistos de estilo de segurança. Isso inclui informações sobre ACEs condicionais, ACEs de recursos e ACEs de política de acesso central. Você pode usar os resultados para validar sua configuração de segurança ou para solucionar problemas de acesso a arquivos.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os dados cujas informações de segurança de arquivo ou pasta você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

Passo

1. Exiba as configurações de segurança de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações...	Digite o seguinte comando...
Em forma de resumo	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>
Com detalhes expandidos	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>
Onde a saída é exibida com SIDs de grupo e usuário	<pre>vserver security file-directory show -vserver vserver_name -path path -lookup-names false</pre>
Sobre segurança de arquivos e diretórios para arquivos e diretórios onde a máscara de bits hexadecimal é traduzida para o formato textual	<pre>vserver security file-directory show -vserver vserver_name -path path -textual-mask true</pre>

Exemplos

O exemplo a seguir exibe informações de segurança do Dynamic Access Control sobre o caminho /vol11 no SVM VS1:

```

cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
          Vserver: vs1
          File Path: /vol1
    File Inode Number: 112
      Security Style: mixed
    Effective Style: ntfs
      DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attribute: -
      Unix User Id: 0
      Unix Group Id: 1
      Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
          ACLs: NTFS Security Descriptor
              Control:0xbf14
              Owner:CIFS1\Administrator
              Group:CIFS1\Domain Admins
              SACL - ACEs
                  ALL-Everyone-0xf01ff-OI|CI|SA|FA
                  RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
          POLICY ID-All resources - No Write-
0x0-OI|CI
          DACL - ACEs
              ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
              ALLOW-Everyone-0x1f01ff-OI|CI
              ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)

```

Informações relacionadas

[Exibindo informações sobre as configurações do GPO](#)

[Exibindo informações sobre políticas de acesso central](#)

[Exibindo informações sobre as regras da política de acesso central](#)

Considerações de reversão para o Controle de Acesso Dinâmico

Você deve estar ciente do que acontece ao reverter para uma versão do ONTAP que não suporta o controle de acesso dinâmico (DAC) e o que você deve fazer antes e depois de reverter.

Se você quiser reverter o cluster para uma versão do ONTAP que não suporte o Controle de Acesso Dinâmico e o Controle de Acesso Dinâmico estiver ativado em uma ou mais máquinas virtuais de armazenamento (SVMs), faça o seguinte antes de reverter:

- Você deve desativar o Controle de Acesso Dinâmico em todos os SVMs que o tenham ativado no cluster.
- É necessário modificar qualquer configuração de auditoria no cluster que contenha o `cap-staging` tipo de evento para usar somente o `file-op` tipo de evento.

Você deve entender e agir sobre algumas considerações importantes de reversão para arquivos e pastas com ACEs de Controle de Acesso Dinâmico:

- Se o cluster for revertido, os ACEs de Controle de Acesso Dinâmico existentes não serão removidos; no entanto, eles serão ignorados nas verificações de acesso ao arquivo.
- Uma vez que os ACEs do controle de Acesso Dinâmico são ignorados após a reversão, o acesso aos arquivos será alterado nos arquivos com ACEs do controle de Acesso Dinâmico.

Isso poderia permitir que os usuários acessem arquivos que eles anteriormente não podiam, ou não poderiam acessar arquivos que anteriormente poderiam.

- Você deve aplicar ACEs não-Dynamic Access Control aos arquivos afetados para restaurar seu nível anterior de segurança.

Isso pode ser feito antes de reverter ou imediatamente após a reversão ser concluída.



Uma vez que os ACEs do controle de Acesso Dinâmico são ignorados após a reversão, não é necessário removê-los ao aplicar ACEs do controle de Acesso não Dinâmico aos arquivos afetados. No entanto, se desejado, você pode removê-los manualmente.

Onde encontrar informações adicionais sobre como configurar e usar o Controle de Acesso Dinâmico e as políticas de Acesso Central

Recursos adicionais estão disponíveis para ajudá-lo a configurar e usar o controle de acesso dinâmico e as políticas de acesso central.

Você pode encontrar informações sobre como configurar o Controle de Acesso Dinâmico e as políticas de Acesso Central no ative Directory na Biblioteca Microsoft TechNet.

["Microsoft TechNet: Visão geral do cenário Dynamic Access Control"](#)

["Microsoft TechNet: Cenário de Política de Acesso Central"](#)

As referências a seguir podem ajudá-lo a configurar o servidor SMB para usar e dar suporte ao Controle de Acesso Dinâmico e às políticas de Acesso Central:

- **Usando GPOs no servidor SMB**

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

- **Configurando a auditoria nas no servidor SMB**

["Auditoria de SMB e NFS e rastreamento de segurança"](#)

Acesso SMB seguro usando políticas de exportação

Como as políticas de exportação são usadas com o acesso SMB

Se as políticas de exportação para acesso SMB estiverem habilitadas no servidor SMB, as políticas de exportação serão usadas ao controlar o acesso a volumes SVM por clientes SMB. Para acessar dados, você pode criar uma política de exportação que permita o acesso SMB e, em seguida, associá-la aos volumes que contêm compartilhamentos SMB.

Uma política de exportação tem uma ou mais regras aplicadas a ela que especifica quais clientes têm permissão de acesso aos dados e quais protocolos de autenticação são suportados para acesso somente leitura e gravação. Você pode configurar políticas de exportação para permitir o acesso por SMB a todos os clientes, uma sub-rede de clientes ou um cliente específico e para permitir a autenticação usando autenticação Kerberos, autenticação NTLM ou autenticação Kerberos e NTLM ao determinar o acesso somente leitura e gravação aos dados.

Depois de processar todas as regras de exportação aplicadas à política de exportação, o ONTAP pode determinar se o cliente recebe acesso e que nível de acesso é concedido. As regras de exportação se aplicam a máquinas cliente, não a usuários e grupos do Windows. As regras de exportação não substituem a autenticação e autorização baseadas em grupo e no utilizador do Windows. As regras de exportação fornecem outra camada de segurança de acesso, além das permissões de compartilhamento e acesso a arquivos.

Você associa exatamente uma política de exportação a cada volume para configurar o acesso do cliente ao volume. Cada SVM pode conter várias políticas de exportação. Isso permite que você faça o seguinte para SVMs com vários volumes:

- Atribua diferentes políticas de exportação a cada volume do SVM para controle de acesso de cliente individual a cada volume no SVM.
- Atribua a mesma política de exportação a vários volumes do SVM para controle de acesso de cliente idêntico sem precisar criar uma nova política de exportação para cada volume.

Cada SVM tem pelo menos uma política de exportação chamada "falha", que não contém regras. Não é possível excluir esta política de exportação, mas você pode renomeá-la ou modificá-la. Por padrão, cada volume no SVM está associado à política de exportação padrão. Se as políticas de exportação para acesso SMB estiverem desativadas no SVM, a política de exportação "falha" não terá efeito no acesso SMB.

Você pode configurar regras que fornecem acesso a hosts NFS e SMB e associar essa regra a uma política de exportação, que pode ser associada ao volume que contém dados ao qual hosts NFS e SMB precisam acessar. Alternativamente, se houver alguns volumes em que apenas clientes SMB exigem acesso, você poderá configurar uma política de exportação com regras que só permitem acesso usando o protocolo SMB e que usa apenas Kerberos ou NTLM (ou ambos) para autenticação para acesso somente leitura e gravação. A política de exportação é então associada aos volumes em que apenas o acesso SMB é desejado.

Se as políticas de exportação para SMB estiverem ativadas e um cliente fizer uma solicitação de acesso não permitida pela política de exportação aplicável, a solicitação falhará com uma mensagem de permissão negada. Se um cliente não corresponder a nenhuma regra na política de exportação do volume, o acesso será negado. Se uma política de exportação estiver vazia, todos os acessos serão implicitamente negados. Isso é verdade mesmo se as permissões de compartilhamento e arquivo permitissem o acesso. Isso significa que você deve configurar sua política de exportação para permitir minimamente o seguinte em volumes que contêm compartilhamentos SMB:

- Permitir o acesso a todos os clientes ou ao subconjunto apropriado de clientes
- Permitir acesso através de SMB
- Permitir acesso apropriado somente leitura e gravação usando a autenticação Kerberos ou NTLM (ou ambas)

Saiba mais "[configuração e gerenciamento de políticas de exportação](#)" sobre .

Como funcionam as regras de exportação

As regras de exportação são os elementos funcionais de uma política de exportação. As regras de exportação correspondem às solicitações de acesso do cliente a um volume em relação aos parâmetros específicos que você configura para determinar como lidar com as solicitações de acesso do cliente.

Uma política de exportação deve conter pelo menos uma regra de exportação para permitir o acesso aos clientes. Se uma política de exportação contiver mais de uma regra, as regras serão processadas na ordem em que aparecem na política de exportação. A ordem da regra é ditada pelo número do índice da regra. Se uma regra corresponder a um cliente, as permissões dessa regra serão usadas e nenhuma outra regra será processada. Se nenhuma regra corresponder, o cliente é negado o acesso.

Você pode configurar regras de exportação para determinar permissões de acesso do cliente usando os seguintes critérios:

- O protocolo de acesso ao arquivo usado pelo cliente que envia a solicitação, por exemplo, NFSv4 ou SMB.
- Um identificador de cliente, por exemplo, nome de host ou endereço IP.

O tamanho máximo para o `-clientmatch` campo é de 4096 caracteres.

- O tipo de segurança usado pelo cliente para autenticar, por exemplo, Kerberos v5, NTLM ou AUTH_SYS.

Se uma regra especificar vários critérios, o cliente deve corresponder a todos eles para que a regra seja aplicada.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

A solicitação de acesso do cliente é enviada usando o protocolo NFSv3 e o cliente tem o endereço IP 10,1.17,37.

Mesmo que o protocolo de acesso do cliente corresponda, o endereço IP do cliente está em uma sub-rede diferente da especificada na regra de exportação. Portanto, a correspondência do cliente falha e esta regra não se aplica a este cliente.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

A solicitação de acesso do cliente é enviada usando o protocolo NFSv4 e o cliente tem o endereço IP 10,1.16,54.

O protocolo de acesso do cliente corresponde e o endereço IP do cliente está na sub-rede especificada. Portanto, a correspondência do cliente é bem-sucedida e esta regra se aplica a este cliente. O cliente obtém acesso de leitura e gravação independentemente do seu tipo de segurança.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

O cliente nº 1 tem o endereço IP 10,1.16,207, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com Kerberos v5.

O cliente nº 2 tem o endereço IP 10,1.16,211, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com AUTH_SYS.

O protocolo de acesso do cliente e o endereço IP correspondem a ambos os clientes. O parâmetro somente leitura permite o acesso somente leitura a todos os clientes, independentemente do tipo de segurança com o qual eles autenticaram. Portanto, ambos os clientes recebem acesso somente leitura. No entanto, somente o cliente nº 1 obtém acesso de leitura e gravação porque usou o tipo de segurança aprovado Kerberos v5 para autenticar. O cliente nº 2 não obtém acesso de leitura e gravação.

Exemplos de regras de política de exportação que restringem ou permitem acesso através de SMB

Os exemplos mostram como criar regras de política de exportação que restringem ou permitem o acesso ao SMB em um SVM que tenha políticas de exportação para acesso ao SMB ativadas.

As políticas de exportação para o acesso SMB estão desativadas por predefinição. Você precisa configurar regras de política de exportação que restrinjam ou permitam acesso ao SMB somente se você tiver ativado políticas de exportação para acesso ao SMB.

Regra de exportação apenas para acesso SMB

O comando a seguir cria uma regra de exportação no SVM chamado "VS1" que tem a seguinte configuração:

- Nome da política: `cifs1`
- Número de índice: 1

- Correspondência de cliente: Corresponde apenas a clientes na rede 192.168.1.0/24
- Protocolo: Ativa apenas o acesso SMB
- Acesso somente leitura: Para clientes que usam autenticação NTLM ou Kerberos
- Acesso de leitura-gravação: Para clientes que usam a autenticação Kerberos

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

Regra de exportação para SMB e acesso NFS

O comando a seguir cria uma regra de exportação no SVM chamado "VS1" que tem a seguinte configuração:

- Nome da política: cifs nfs1
- Número de índice: 2
- Correspondência do cliente: Corresponde a todos os clientes
- Protocolo: Acesso SMB e NFS
- Acesso somente leitura: Para todos os clientes
- Acesso de leitura e gravação: Para clientes que usam Kerberos (NFS e SMB) ou autenticação NTLM (SMB)
- Mapeamento para ID de usuário UNIX 0 (zero): Mapeado para ID de usuário 65534 (que normalmente mapeia para o nome de usuário ninguém)
- Acesso suid e sgid: Permite

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs nfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule any
-rwrule krb5,ntlm -anon 65534 -allow-suid true
```

Regra de exportação para acesso SMB usando apenas NTLM

O comando a seguir cria uma regra de exportação no SVM chamado "VS1" que tem a seguinte configuração:

- Nome da política: ntlm1
- Número de índice: 1
- Correspondência do cliente: Corresponde a todos os clientes
- Protocolo: Ativa apenas o acesso SMB
- Acesso somente leitura: Somente para clientes que usam NTLM
- Acesso de leitura e gravação: Apenas para clientes que utilizam NTLM



Se você configurar a opção somente leitura ou a opção leitura-gravação para acesso somente NTLM, você deverá usar entradas baseadas em endereço IP na opção correspondência do cliente. Caso contrário, você recebe `access denied` erros. Isso ocorre porque o ONTAP usa os nomes principais do Serviço Kerberos (SPN) ao usar um nome de host para verificar os direitos de acesso do cliente. A autenticação NTLM não suporta nomes SPN.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

Ativar ou desativar políticas de exportação para acesso SMB

Você pode ativar ou desativar políticas de exportação para acesso SMB em máquinas virtuais de armazenamento (SVMs). O uso de políticas de exportação para controlar o acesso SMB a recursos é opcional.

Antes de começar

A seguir estão os requisitos para ativar políticas de exportação para SMB:

- O cliente deve ter um Registro "PTR" no DNS antes de criar as regras de exportação para esse cliente.
- Um conjunto adicional de Registros "A" e "PTR" para nomes de host é necessário se o SVM fornecer acesso a clientes NFS e o nome de host que você deseja usar para acesso NFS for diferente do nome do servidor CIFS.

Sobre esta tarefa

Ao configurar um novo servidor CIFS na SVM, o uso de políticas de exportação para acesso SMB é desativado por padrão. Você pode habilitar políticas de exportação para acesso SMB se quiser controlar o acesso com base no protocolo de autenticação ou em endereços IP de cliente ou nomes de host. Você pode ativar ou desativar políticas de exportação para acesso SMB a qualquer momento.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Ativar ou desativar políticas de exportação:
 - Ativar políticas de exportação: `vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled true`
 - Desativar políticas de exportação: `vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled false`
3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exemplo

O exemplo a seguir permite o uso de políticas de exportação para controlar o acesso de clientes SMB a recursos 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 -is-exportpolicy
-enabled true

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

Proteja o acesso aos arquivos usando o Storage-Level Access Guard

Proteja o acesso aos arquivos usando o Storage-Level Access Guard

Além de proteger o acesso usando a segurança nativa em nível de arquivo e exportar e compartilhar, você pode configurar o Storage-Level Access Guard, uma terceira camada de segurança aplicada pelo ONTAP no nível de volume. O Storage-Level Access Guard se aplica ao acesso de todos os protocolos nas ao objeto de storage ao qual ele é aplicado.

Apenas as permissões de acesso NTFS são suportadas. Para que o ONTAP execute verificações de segurança em usuários UNIX para obter acesso a dados em volumes para os quais o Guarda de Acesso em nível de storage foi aplicado, o usuário do UNIX deve mapear para um usuário do Windows na SVM que possua o volume.

Comportamento do Access Guard no nível de storage

- O Storage-Level Access Guard aplica-se a todos os arquivos ou a todos os diretórios em um objeto de armazenamento.

Como todos os arquivos ou diretórios em um volume estão sujeitos às configurações do Storage-Level Access Guard, a herança através da propagação não é necessária.

- Você pode configurar o Storage-Level Access Guard para se aplicar apenas a arquivos, apenas a diretórios ou a arquivos e diretórios dentro de um volume.

- Segurança de arquivos e diretórios

Aplica-se a cada diretório e arquivo dentro do objeto de armazenamento. Esta é a configuração padrão.

- Segurança de arquivos

Aplica-se a todos os arquivos dentro do objeto de armazenamento. A aplicação dessa segurança não afeta o acesso ou a auditoria de diretórios.

- Segurança do diretório

Aplica-se a todos os diretórios dentro do objeto de armazenamento. A aplicação dessa segurança não afeta o acesso ou a auditoria de arquivos.

- O Access Guard no nível de storage é usado para restringir permissões.

Ele nunca dará permissões de acesso extra.

- Se você exibir as configurações de segurança em um arquivo ou diretório de um cliente NFS ou SMB, não verá a segurança Storage-Level Access Guard.

Ele é aplicado no nível do objeto de armazenamento e armazenado nos metadados usados para determinar as permissões efetivas.

- A segurança no nível do storage não pode ser revogada de um cliente, mesmo por um administrador do sistema (Windows ou UNIX).

Ele foi desenvolvido para ser modificado apenas por administradores de storage.

- Você pode aplicar o Storage-Level Access Guard a volumes com NTFS ou estilo de segurança misto.
- Você pode aplicar o Storage-Level Access Guard a volumes com estilo de segurança UNIX, desde que o SVM que contém o volume tenha um servidor CIFS configurado.
- Quando os volumes são montados sob um caminho de junção de volume e se o Storage-Level Access Guard estiver presente nesse caminho, ele não será propagado para volumes montados sob ele.
- O descritor de segurança do Access Guard em nível de storage é replicado com a replicação de dados do SnapMirror e com replicação SVM.
- Há dispensação especial para scanners de vírus.

Acesso excepcional é permitido a esses servidores para exibir arquivos e diretórios, mesmo que o Storage-Level Access Guard negue acesso ao objeto.

- As notificações FPolicy não são enviadas se o acesso for negado devido ao Storage-Level Access Guard.

Verificações de ordem de acesso

O acesso a um arquivo ou diretório é determinado pelo efeito combinado das permissões de exportação ou compartilhamento, as permissões de guarda de acesso em nível de armazenamento definidas em volumes e as permissões de arquivo nativo aplicadas a arquivos e/ou diretórios. Todos os níveis de segurança são avaliados para determinar quais as permissões efetivas de um arquivo ou diretório. As verificações de acesso de segurança são realizadas na seguinte ordem:

1. Permissões de compartilhamento SMB ou nível de exportação NFS
2. Proteção de acesso no nível de storage
3. Listas de controle de acesso (ACLs) de arquivos/pastas NTFS, ACLs NFSv4 ou bits de modo UNIX

Casos de uso para usar o Storage-Level Access Guard

O Storage-Level Access Guard fornece segurança adicional no nível de armazenamento, que não é visível do lado do cliente; portanto, ele não pode ser revogado por nenhum dos usuários ou administradores de seus desktops. Há certos casos de uso em que a capacidade de controlar o acesso no nível de storage é benéfica.

Os casos de uso típicos para esse recurso incluem os seguintes cenários:

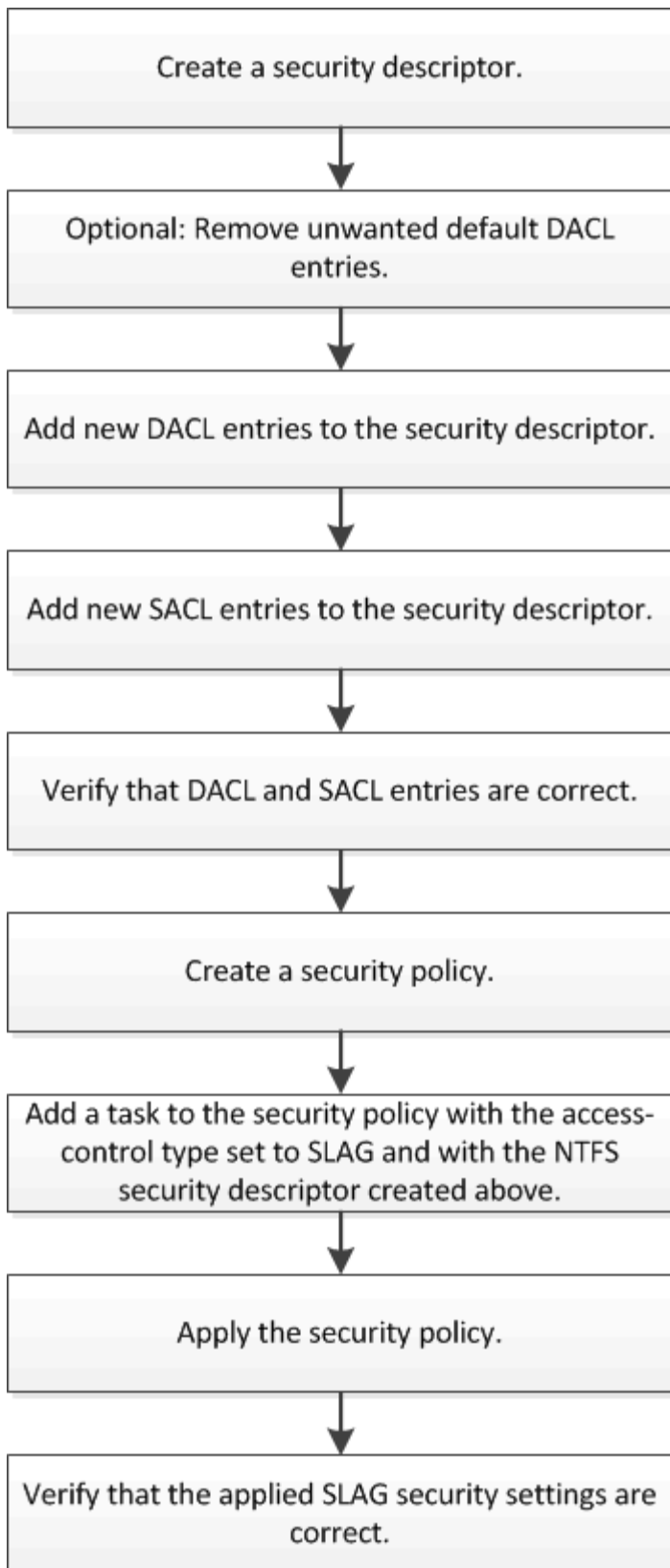
- Proteção da propriedade intelectual através da auditoria e controle do acesso de todos os utilizadores ao

nível do armazenamento

- Armazenamento para empresas de serviços financeiros, incluindo bancos e grupos de negociação
- Serviços governamentais dos EUA com storage de arquivos separado para departamentos individuais
- Universidades protegendo todos os arquivos dos alunos

Fluxo de trabalho para configurar o Storage-Level Access Guard

O fluxo de trabalho para configurar o guarda de acesso em nível de armazenamento (SLAG) usa os mesmos comandos CLI do ONTAP que você usa para configurar permissões de arquivos NTFS e políticas de auditoria. Em vez de configurar o acesso a arquivos e diretórios em um destino designado, você configura O SLAG no volume designado de máquina virtual de armazenamento (SVM).



Informações relacionadas

[Configurando o Storage-Level Access Guard](#)

Configurar o Storage-Level Access Guard

Há uma série de etapas que você precisa seguir para configurar o Storage-Level Access Guard em um volume ou qtree. O Storage-Level Access Guard fornece um nível de segurança de acesso definido no nível de armazenamento. Ele fornece segurança que se aplica a todos os acessos de todos os protocolos nas ao objeto de storage ao qual foi aplicado.

Passos

1. Crie um descritor de segurança usando o `vserver security file-directory ntfs create` comando.

```
vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1 vserver
security file-directory ntfs show -vserver vs1
```

```
Vserver: vs1
```

NTFS Security Descriptor Name	Owner Name
-----	-----
sd1	-

Um descritor de segurança é criado com as quatro entradas de controle de acesso (ACEs) padrão a seguir:

```
Vserver: vs1
```

```
NTFS Security Descriptor Name: sd1
```

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
BUILTIN\Administrators	allow	full-control	this-folder, sub-folders, files
BUILTIN\Users	allow	full-control	this-folder, sub-folders, files
CREATOR OWNER	allow	full-control	this-folder, sub-folders, files
NT AUTHORITY\SYSTEM	allow	full-control	this-folder, sub-folders, files

Se você não quiser usar as entradas padrão ao configurar o Storage-Level Access Guard, você pode removê-las antes de criar e adicionar seus próprios ACEs ao descritor de segurança.

2. Remova qualquer um dos ACEs DACL padrão do descritor de segurança que você não deseja configurar

com segurança Storage-Level Access Guard:

- a. Remova quaisquer ACEs DACL indesejados usando o `vserver security file-directory ntfs dacl remove` comando.

Neste exemplo, três ACEs DACL padrão são removidos do descritor de segurança: BUILTIN/Administrators, BUILTIN/Users e CREATOR OWNER.

```
vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
-access-type allow -account builtin\users vserver security file-directory
ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
builtin\administrators vserver security file-directory ntfs dacl remove
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
```

- b. Verifique se os ACEs DACL que você não deseja usar para a segurança Storage-Level Access Guard são removidos do descritor de segurança usando o `vserver security file-directory ntfs dacl show` comando.

Neste exemplo, a saída do comando verifica se três ACEs DACL padrão foram removidos do descritor de segurança, deixando apenas a entrada DCAACE padrão DA AUTORIDADE NT/SISTEMA:

```
vserver security file-directory ntfs dacl show -vserver vs1
```

```
Vserver: vs1
NTFS Security Descriptor Name: sd1

Account Name      Access  Access  Apply To
                  Type   Rights
-----
NT AUTHORITY\SYSTEM
                  allow   full-control  this-folder, sub-folders,
files
```

3. Adicione uma ou mais entradas DACL a um descritor de segurança usando o `vserver security file-directory ntfs dacl add` comando.

Neste exemplo, dois ACEs DACL são adicionados ao descritor de segurança:

```
vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
-access-type allow -account example\engineering -rights full-control -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs dacl add
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
-rights read -apply-to this-folder,sub-folders,files
```

4. Adicione uma ou mais entradas SACL a um descritor de segurança usando o `vserver security file-directory ntfs sacl add` comando.

Neste exemplo, dois ACEs SACL são adicionados ao descritor de segurança:

```
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
```

```
-access-type failure -account "example\Domain Users" -rights read -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. Verifique se os ACEs DACL e SACL estão configurados corretamente utilizando os `vserver security file-directory ntfs dacl show` comandos e `vserver security file-directory ntfs sacl show`, respectivamente.

Neste exemplo, o comando a seguir exibe informações sobre entradas DACL para descritor de segurança "D1":

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
NTFS Security Descriptor Name: sd1

Account Name      Access  Access  Apply To
                  Type   Rights
-----
EXAMPLE\Domain Users
                  allow   read    this-folder, sub-folders,
files
EXAMPLE\engineering
                  allow   full-control  this-folder, sub-folders,
files
NT AUTHORITY\SYSTEM
                  allow   full-control  this-folder, sub-folders,
files
```

Neste exemplo, o comando a seguir exibe informações sobre entradas SACL para descritor de segurança "D1":

```
vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
NTFS Security Descriptor Name: sd1

Account Name      Access      Access      Apply To
Type              Rights
-----
EXAMPLE\Domain Users
                  failure    read        this-folder, sub-folders,
files
EXAMPLE\engineering
                  success   full-control  this-folder, sub-folders,
files
```

6. Crie uma política de segurança usando o `vserver security file-directory policy create` comando.

O exemplo a seguir cria uma política chamada "policy1":

```
vserver security file-directory policy create -vserver vs1 -policy-name
policy1
```

7. Verifique se a política está corretamente configurada usando o `vserver security file-directory policy show` comando.

```
vserver security file-directory policy show
```

```
Vserver      Policy Name
-----
vs1          policy1
```

8. Adicione uma tarefa com um descritor de segurança associado à diretiva de segurança usando o `vserver security file-directory policy task add` comando com o `-access-control` parâmetro definido como `slag`.

Mesmo que uma política possa conter mais de uma tarefa Storage-Level Access Guard, você não pode configurar uma política para conter tarefas de diretório de arquivo e Guarda de acesso no nível de armazenamento. Uma diretiva deve conter todas as tarefas do Guarda de Acesso no nível de armazenamento ou todas as tarefas do diretório de arquivos.

Neste exemplo, uma tarefa é adicionada à política chamada "policy1", que é atribuída ao descritor de segurança "D1". Ele é atribuído ao `/datavol1` caminho com o tipo de controle de acesso definido como "lag".

```
vserver security file-directory policy task add -vserver vs1 -policy-name
policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode
propagate -ntfs-sd sd1
```

9. Verifique se a tarefa está configurada corretamente usando o `vserver security file-directory`

policy task show comando.

```
vserver security file-directory policy task show -vserver vs1 -policy-name policy1
```

```
Vserver: vs1
Policy: policy1
```

Index	File/Folder	Access	Security	NTFS	NTFS
Security	Path	Control	Type	Mode	Descriptor
Name					
-----	-----	-----	-----	-----	

1	/datavol1	slag	ntfs	propagate	sd1

10. Aplique a política de segurança Storage-Level Access Guard usando o `vserver security file-directory apply` comando.

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

O trabalho para aplicar a política de segurança está agendado.

11. Verifique se as configurações de segurança do Access Guard no nível de armazenamento aplicado estão corretas usando o `vserver security file-directory show` comando.

Neste exemplo, a saída do comando mostra que a segurança do Storage-Level Access Guard foi aplicada ao volume NTFS `/datavol1`. Mesmo que a DACL padrão que permite o controle total para todos permaneça, a segurança do Storage-Level Access Guard restringe (e audita) o acesso aos grupos definidos nas configurações do Storage-Level Access Guard.

```
vserver security file-directory show -vserver vs1 -path /datavol1
```

```

        Vserver: vs1
        File Path: /datavol1
File Inode Number: 77
        Security Style: ntfs
        Effective Style: ntfs
        DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
Control:0x8004
Owner: BUILTIN\Administrators
Group: BUILTIN\Administrators
DACL - ACEs
        ALLOW-Everyone-0x1f01ff
        ALLOW-Everyone-0x10000000-OI|CI|IO

Storage-Level Access Guard security
SACL (Applies to Directories):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Directories):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
SACL (Applies to Files):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Files):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

Informações relacionadas

[Gerenciamento da segurança de arquivos NTFS, políticas de auditoria NTFS e Guarda de acesso em nível de armazenamento em SVMs usando a CLI](#)

[Fluxo de trabalho para configurar o Storage-Level Access Guard](#)

[Exibindo informações sobre o Storage-Level Access Guard](#)

[Remoção do Storage-Level Access Guard](#)

Matriz DE ESCÓRIA eficaz

Você pode configurar O SLAG em um volume ou uma qtree ou ambos. A matriz DE ESCÓRIA define em que volume ou qtree é a configuração DE ESCÓRIA aplicável em vários cenários listados na tabela.

	ESCÓRIA de volume num AFS	ESCÓRIA de volume em uma cópia Snapshot	ESCÓRIA de Qtree em um AFS	ESCÓRIA de Qtree em uma cópia Snapshot
Acesso de volume num sistema de ficheiros de acesso (AFS)	SIM	NÃO	N/A.	N/A.
Acesso de volume em uma cópia Snapshot	SIM	NÃO	N/A.	N/A.
Acesso Qtree em um AFS (quando ESCÓRIA está presente na qtree)	NÃO	NÃO	SIM	NÃO
Acesso Qtree em um AFS (quando ESCÓRIA não está presente em qtree)	SIM	NÃO	NÃO	NÃO
Acesso Qtree na cópia Snapshot (quando A ESCÓRIA está presente no qtree AFS)	NÃO	NÃO	SIM	NÃO
Acesso Qtree na cópia Snapshot (quando A ESCÓRIA não está presente na qtree AFS)	SIM	NÃO	NÃO	NÃO

Exibir informações sobre o Storage-Level Access Guard

O Storage-Level Access Guard é uma terceira camada de segurança aplicada em um volume ou qtree. As configurações do Access Guard no nível de armazenamento não podem ser visualizadas usando a janela Propriedades do Windows. Você deve usar a CLI do ONTAP para exibir informações sobre a segurança do Guarda de acesso em nível de armazenamento, que pode ser usada para validar sua configuração ou para

solucionar problemas de acesso a arquivos.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para o volume ou qtree cujas informações de segurança do Storage-Level Access Guard você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

Passo

1. Exibir as configurações de segurança do Access Guard no nível de armazenamento com o nível de detalhe desejado:

Se você quiser exibir informações...	Digite o seguinte comando...
Em forma de resumo	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>
Com detalhes expandidos	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>

Exemplos

O exemplo a seguir exibe informações de segurança do Access Guard no nível de armazenamento para o volume de estilo de segurança NTFS com o caminho `/datavol1` no SVM VS1:


```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1
```

```

    Vserver: vs1
    File Path: /datavol1
File Inode Number: 77
    Security Style: ntfs
    Effective Style: ntfs
    DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
        Control:0x8004
        Owner: BUILTIN\Administrators
        Group: BUILTIN\Administrators
        DACL - ACEs
            ALLOW-Everyone-0x1f01ff
            ALLOW-Everyone-0x10000000-OI|CI|IO

Storage-Level Access Guard security
SACL (Applies to Directories):
    AUDIT-EXAMPLE\Domain Users-0x120089-FA
    AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Directories):
    ALLOW-EXAMPLE\Domain Users-0x120089
    ALLOW-EXAMPLE\engineering-0x1f01ff
    ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
SACL (Applies to Files):
    AUDIT-EXAMPLE\Domain Users-0x120089-FA
    AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Files):
    ALLOW-EXAMPLE\Domain Users-0x120089
    ALLOW-EXAMPLE\engineering-0x1f01ff
    ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

O exemplo a seguir exibe as informações do Access Guard no nível de storage sobre o volume de estilo de segurança misto no caminho /datavol15 do SVM VS1. O nível superior deste volume tem segurança eficaz UNIX. O volume tem segurança Storage-Level Access Guard.

```

cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5

        Vserver: vs1
        File Path: /datavol5
File Inode Number: 3374
        Security Style: mixed
        Effective Style: unix
        DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 755
Unix Mode Bits in Text: rwxr-xr-x
        ACLs: Storage-Level Access Guard security
        SACL (Applies to Directories):
            AUDIT-EXAMPLE\Domain Users-0x120089-FA
            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
        DACL (Applies to Directories):
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-EXAMPLE\engineering-0x1f01ff
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
        SACL (Applies to Files):
            AUDIT-EXAMPLE\Domain Users-0x120089-FA
            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
        DACL (Applies to Files):
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-EXAMPLE\engineering-0x1f01ff
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

Remove o Storage-Level Access Guard

Você pode remover o Storage-Level Access Guard em um volume ou qtree se não quiser mais definir a segurança de acesso no nível de armazenamento. A remoção do Storage-Level Access Guard não modifica ou remove a segurança regular do arquivo NTFS e do diretório.

Passos

1. Verifique se o volume ou a qtree tem o Storage-Level Access Guard configurado usando o `vserver security file-directory show` comando.

```
vserver security file-directory show -vserver vs1 -path /datavol2
```

```

Vserver: vs1
File Path: /datavol2
File Inode Number: 99
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0xbf14
Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
SACL - ACEs
AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
DACL - ACEs
ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

Storage-Level Access Guard security
DACL (Applies to Directories):
ALLOW-BUILTIN\Administrators-0x1f01ff
ALLOW-CREATOR OWNER-0x1f01ff
ALLOW-EXAMPLE\Domain Admins-0x1f01ff
ALLOW-EXAMPLE\Domain Users-0x120089
ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
DACL (Applies to Files):
ALLOW-BUILTIN\Administrators-0x1f01ff
ALLOW-CREATOR OWNER-0x1f01ff
ALLOW-EXAMPLE\Domain Admins-0x1f01ff
ALLOW-EXAMPLE\Domain Users-0x120089
ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

2. Remova o Storage-Level Access Guard usando o `vserver security file-directory remove-slag` comando.

```
vserver security file-directory remove-slag -vserver vs1 -path /datavol2
```

3. Verifique se o Storage-Level Access Guard foi removido do volume ou `qtree` usando o `vserver security file-directory show` comando.

```
vserver security file-directory show -vserver vs1 -path /datavol2
```

```
Vserver: vs1
File Path: /datavol2
File Inode Number: 99
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0xbf14
Owner: BUILTIN\Administrators
Group: BUILTIN\Administrators
SACL - ACEs
    AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
DACL - ACEs
    ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
    ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```

Gerencie o acesso a arquivos usando SMB

Use usuários e grupos locais para autenticação e autorização

Como o ONTAP usa usuários e grupos locais

Conceitos de usuários e grupos locais

Você deve saber o que são usuários e grupos locais e algumas informações básicas sobre eles, antes de determinar se deseja configurar e usar usuários e grupos locais em seu ambiente.

- **Usuário local**

Uma conta de usuário com um identificador de segurança exclusivo (SID) que tem visibilidade somente na máquina virtual de armazenamento (SVM) na qual é criada. As contas de usuário locais têm um conjunto de atributos, incluindo nome de usuário e SID. Uma conta de usuário local autentica localmente no servidor CIFS usando autenticação NTLM.

As contas de usuário têm vários usos:

- Usado para conceder *Gerenciamento de Direitos de Usuário Privileges* a um usuário.
- Usado para controlar o acesso em nível de compartilhamento e em nível de arquivo aos recursos de arquivo e pasta que o SVM possui.

- **Grupo local**

Um grupo com um SID exclusivo tem visibilidade somente na SVM em que ele é criado. Grupos contêm um conjunto de membros. Os membros podem ser usuários locais, usuários de domínio, grupos de domínio e contas de máquinas de domínio. Os grupos podem ser criados, modificados ou excluídos.

Os grupos têm vários usos:

- Usado para conceder *Gerenciamento de Direitos de Usuário Privileges* aos seus membros.
- Usado para controlar o acesso em nível de compartilhamento e em nível de arquivo aos recursos de arquivo e pasta que o SVM possui.

- **Domínio local**

Um domínio que tem escopo local, limitado pelo SVM. O nome do domínio local é o nome do servidor CIFS. Os usuários e grupos locais estão contidos no domínio local.

- **Identificador de segurança (SID)**

Um SID é um valor numérico de comprimento variável que identifica os princípios de segurança do estilo Windows. Por exemplo, um SID típico assume a seguinte forma: S-1-5-21-3139654847-1303905135-2517279418-123456.

- * Autenticação NTLM*

Um método de segurança do Microsoft Windows usado para autenticar usuários em um servidor CIFS.

- **Banco de dados replicado em cluster (RDB)**

Um banco de dados replicado com uma instância em cada nó em um cluster. Os objetos de usuário local e grupo são armazenados no RDB.

Razões para criar usuários locais e grupos locais

Há várias razões para criar usuários locais e grupos locais na sua máquina virtual de storage (SVM). Por exemplo, você pode acessar um servidor SMB usando uma conta de usuário local se os controladores de domínio (DCs) não estiverem disponíveis, talvez queira usar grupos locais para atribuir Privileges ou se o servidor SMB estiver em um grupo de trabalho.

Você pode criar uma ou mais contas de usuário locais pelos seguintes motivos:

- Seu servidor SMB está em um grupo de trabalho e os usuários de domínio não estão disponíveis.

Os utilizadores locais são necessários nas configurações do grupo de trabalho.

- Você deseja a capacidade de autenticar e fazer login no servidor SMB se os controladores de domínio não estiverem disponíveis.

Os usuários locais podem se autenticar com o servidor SMB usando a autenticação NTLM quando o controlador de domínio está inativo ou quando problemas de rede impedem que o servidor SMB entre em Contato com o controlador de domínio.

- Você deseja atribuir *User Rights Management Privileges* a um usuário local.

User Rights Management é a capacidade de um administrador de servidor SMB controlar quais direitos os usuários e grupos têm no SVM. Você pode atribuir Privileges a um usuário atribuindo o Privileges à conta do usuário ou tornando o usuário membro de um grupo local que tenha esses Privileges.

Você pode criar um ou mais grupos locais pelos seguintes motivos:

- O servidor SMB está em um grupo de trabalho e os grupos de domínio não estão disponíveis.

Os grupos locais não são necessários nas configurações do grupo de trabalho, mas podem ser úteis para gerenciar o Access Privileges para usuários locais do grupo de trabalho.

- Você deseja controlar o acesso aos recursos de arquivos e pastas usando grupos locais para controle de compartilhamento e acesso a arquivos.
- Você deseja criar grupos locais com *User Rights Management* Privileges personalizado.

Alguns grupos de utilizadores incorporados têm Privileges predefinidos. Para atribuir um conjunto personalizado de Privileges, você pode criar um grupo local e atribuir o Privileges necessário a esse grupo. Em seguida, você pode adicionar usuários locais, usuários de domínio e grupos de domínio ao grupo local.

Informações relacionadas

[Como funciona a autenticação de usuário local](#)

[Lista de Privileges suportados](#)

Como funciona a autenticação de usuário local

Antes que um usuário local possa acessar dados em um servidor CIFS, o usuário deve criar uma sessão autenticada.

Como o SMB é baseado em sessão, a identidade do usuário pode ser determinada apenas uma vez, quando a sessão é configurada pela primeira vez. O servidor CIFS usa autenticação baseada em NTLM ao autenticar usuários locais. Tanto o NTLMv1 como o NTLMv2 são suportados.

O ONTAP usa autenticação local em três casos de uso. Cada caso de uso depende se a parte do domínio do nome de usuário (com o formato DOMÍNIO/usuário) corresponde ao nome de domínio local do servidor CIFS (o nome do servidor CIFS):

- A parte do domínio corresponde

Os usuários que fornecem credenciais de usuário local ao solicitar acesso aos dados são autenticados localmente no servidor CIFS.

- A parte do domínio não corresponde

O ONTAP tenta usar a autenticação NTLM com um controlador de domínio no domínio ao qual o servidor CIFS pertence. Se a autenticação for bem-sucedida, o login será concluído. Se não for bem-sucedido, o que acontece a seguir depende do motivo pelo qual a autenticação não foi bem-sucedida.

Por exemplo, se o usuário existir no active Directory mas a senha for inválida ou expirada, o ONTAP não tentará usar a conta de usuário local correspondente no servidor CIFS. Em vez disso, a autenticação falha. Existem outros casos em que o ONTAP usa a conta local correspondente no servidor CIFS, se existir, para autenticação - mesmo que os nomes de domínio NetBIOS não correspondam. Por exemplo,

se existir uma conta de domínio correspondente mas estiver desativada, o ONTAP utiliza a conta local correspondente no servidor CIFS para autenticação.

- A parte do domínio não é especificada

O ONTAP tenta pela primeira vez a autenticação como um usuário local. Se a autenticação como um usuário local falhar, o ONTAP autenticará o usuário com um controlador de domínio no domínio ao qual o servidor CIFS pertence.

Depois que a autenticação de usuário local ou de domínio for concluída com sucesso, o ONTAP constrói um token de acesso completo de usuário, que leva em conta a associação de grupo local e o Privileges.

Para obter mais informações sobre autenticação NTLM para usuários locais, consulte a documentação do Microsoft Windows.

Informações relacionadas

[Ativar ou desativar a autenticação de utilizador local](#)

Como os tokens de acesso do usuário são construídos

Quando um usuário mapeia um compartilhamento, uma sessão SMB autenticada é estabelecida e um token de acesso de usuário é construído que contém informações sobre o usuário, a associação de grupo do usuário e Privileges cumulativos e o usuário UNIX mapeado.

A menos que a funcionalidade esteja desativada, as informações de usuário local e grupo também são adicionadas ao token de acesso do usuário. A forma como os tokens de acesso são construídos depende se o login é para um usuário local ou um usuário de domínio do Active Directory:

- Início de sessão do utilizador local

Embora os usuários locais possam ser membros de diferentes grupos locais, os grupos locais não podem ser membros de outros grupos locais. O token de acesso de usuário local é composto por uma união de todos os Privileges atribuídos a grupos aos quais um usuário local específico é membro.

- Login de usuário de domínio

Quando um usuário de domínio faz login, o ONTAP obtém um token de acesso de usuário que contém o SID do usuário e os SIDs para todos os grupos de domínio aos quais o usuário é membro. O ONTAP usa a união do token de acesso do usuário de domínio com o token de acesso fornecido por associações locais dos grupos de domínio do usuário (se houver), bem como qualquer Privileges direto atribuído ao usuário do domínio ou qualquer uma de suas associações de grupo de domínio.

Para login de usuário local e de domínio, o RID de grupo principal também é definido para o token de acesso do usuário. O RID predefinido é `Domain Users` (RID 513). Não é possível alterar a predefinição.

O processo de mapeamento de nomes do Windows para UNIX e UNIX para Windows segue as mesmas regras para contas locais e de domínio.



Não há mapeamento automático implícito de um usuário UNIX para uma conta local. Se isso for necessário, uma regra de mapeamento explícito deve ser especificada usando os comandos de mapeamento de nomes existentes.

Diretrizes para o uso do SnapMirror em SVMs que contêm grupos locais

Você deve estar ciente das diretrizes ao configurar o SnapMirror em volumes de propriedade de SVMs que contêm grupos locais.

Não é possível usar grupos locais em ACEs aplicados a arquivos, diretórios ou compartilhamentos replicados pelo SnapMirror para outro SVM. Se você usar o recurso SnapMirror para criar um espelhamento de DR para um volume em outro SVM e o volume tiver um ACE para um grupo local, o ACE não será válido no espelhamento. Se os dados forem replicados para uma SVM diferente, eles serão migrados para um domínio local diferente. As permissões concedidas a usuários e grupos locais são válidas somente dentro do escopo do SVM no qual foram criados originalmente.

O que acontece com usuários e grupos locais ao excluir servidores CIFS

O conjunto padrão de usuários e grupos locais é criado quando um servidor CIFS é criado e eles são associados à máquina virtual de armazenamento (SVM) que hospeda o servidor CIFS. Os administradores do SVM podem criar usuários e grupos locais a qualquer momento. Você precisa estar ciente do que acontece com usuários e grupos locais quando você exclui o servidor CIFS.

Usuários e grupos locais estão associados a SVMs; portanto, eles não são excluídos quando os servidores CIFS são excluídos devido a considerações de segurança. Embora os usuários e grupos locais não sejam excluídos quando o servidor CIFS é excluído, eles ficam ocultos. Não é possível exibir ou gerenciar usuários e grupos locais até que você crie novamente um servidor CIFS no SVM.



O status administrativo do servidor CIFS não afeta a visibilidade de usuários ou grupos locais.

Como você pode usar o Microsoft Management Console com usuários e grupos locais

Você pode exibir informações sobre usuários e grupos locais no Console de Gerenciamento da Microsoft. Com esta versão do ONTAP, não é possível executar outras tarefas de gerenciamento para usuários e grupos locais a partir do Console de Gerenciamento da Microsoft.

Diretrizes para reverter

Se você pretende reverter o cluster para uma versão do ONTAP que não ofereça suporte a usuários e grupos locais e usuários e grupos locais estejam sendo usados para gerenciar o acesso a arquivos ou direitos de usuário, você deve estar ciente de certas considerações.

- Devido a razões de segurança, as informações sobre usuários locais configurados, grupos e Privileges não são excluídas quando o ONTAP é revertido para uma versão que não suporta a funcionalidade de usuários locais e grupos.
- Após a reversão para uma versão principal anterior do ONTAP, o ONTAP não usa usuários e grupos locais durante a autenticação e criação de credenciais.
- Os utilizadores e grupos locais não são removidos das ACLs de ficheiros e pastas.
- Solicitações de acesso a arquivos que dependem do acesso concedido devido às permissões concedidas a usuários ou grupos locais são negadas.

Para permitir o acesso, você deve reconfigurar as permissões de arquivo para permitir o acesso com base em objetos de domínio em vez de objetos de usuário local e grupo.

O que são os Privileges locais

Lista de Privileges suportados

O ONTAP tem um conjunto predefinido de Privileges suportados. Alguns grupos locais predefinidos têm alguns desses Privileges adicionados a eles por padrão. Você também pode adicionar ou remover Privileges dos grupos predefinidos ou criar novos usuários ou grupos locais e adicionar Privileges aos grupos criados ou aos usuários e grupos de domínio existentes.

A tabela a seguir lista os Privileges suportados na máquina virtual de armazenamento (SVM) e fornece uma lista de grupos BUILTIN com Privileges atribuídos:

Nome do privilégio	Configuração de segurança padrão	Descrição
SeTcbPrivilege	Nenhum	Agir como parte do sistema operacional
SeBackupPrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators	Faça backup de arquivos e diretórios, substituindo quaisquer ACLs
SeRestorePrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators	Restaure arquivos e diretórios, substituindo qualquer ACLs defina qualquer SID válido de usuário ou grupo como proprietário do arquivo
SeTakeOwnershipPrivilege	BUILTIN\Administrators	Assuma a propriedade de arquivos ou outros objetos
SeSecurityPrivilege	BUILTIN\Administrators	Gerenciar a auditoria Isso inclui a visualização, o dumping e a limpeza do log de segurança.
SeChangeNotifyPrivilege	BUILTIN\Administrators BUILTIN\Backup Operators, BUILTIN\Power Users BUILTIN\Users , , , Everyone	Verificação da travessa de derivação Os usuários com esse privilégio não são obrigados a ter permissões de avanço (x) para percorrer pastas, links simbólicos ou junções.

Informações relacionadas

- [Atribuir Privileges local](#)
- [Configuração da verificação transversal de derivação](#)

Atribuir Privileges

Você pode atribuir Privileges diretamente a usuários locais ou usuários de domínio. Como alternativa, você pode atribuir usuários a grupos locais cujos Privileges atribuídos correspondem aos recursos que você deseja que esses usuários tenham.

- Você pode atribuir um conjunto de Privileges a um grupo que você criar.

Em seguida, adicione um utilizador ao grupo que tem o Privileges que pretende que esse utilizador tenha.

- Você também pode atribuir usuários locais e usuários de domínio a grupos predefinidos cujo Privileges padrão corresponde ao Privileges que você deseja conceder a esses usuários.

Informações relacionadas

- [Adicionando Privileges a usuários ou grupos locais ou de domínio](#)
- [Removendo Privileges de usuários ou grupos locais ou de domínio](#)
- [Redefinir o Privileges para usuários e grupos locais ou de domínio](#)
- [Configuração da verificação transversal de derivação](#)

Diretrizes para usar grupos BUILTIN e a conta de administrador local

Há certas diretrizes que você deve ter em mente quando você usa grupos BUILTIN e a conta de administrador local. Por exemplo, você pode renomear a conta de administrador local, mas não pode excluir essa conta.

- A conta de administrador pode ser renomeada, mas não pode ser excluída.
- A conta de administrador não pode ser removida do grupo BUILTIN/Administradores.
- Os grupos DE COMPILAÇÃO podem ser renomeados, mas não podem ser excluídos.

Depois que o grupo BUILTIN é renomeado, outro objeto local pode ser criado com o nome conhecido; no entanto, o objeto recebe um novo RID.

- Não existe uma conta de convidado local.

Informações relacionadas

[Grupos BUILTIN predefinidos e Privileges padrão](#)

Requisitos para senhas de usuários locais

Por padrão, as senhas de usuário local devem atender aos requisitos de complexidade. Os requisitos de complexidade de senha são semelhantes aos requisitos definidos na política de segurança local do Microsoft Windows *diretiva de segurança*.

A senha deve atender aos seguintes critérios:

- Deve ter pelo menos seis caracteres de comprimento

- Não deve conter o nome da conta de utilizador
- Deve conter caracteres de pelo menos três das quatro categorias seguintes:
 - Caracteres maiúsculos em inglês (A a Z)
 - Caracteres minúsculos em inglês (a a z)
 - Base 10 dígitos (0 a 9)
 - Caracteres especiais:
i. ! () [] : ; " ' > , . ? /

Informações relacionadas

[Ativar ou desativar a complexidade de senha necessária para usuários SMB locais](#)

[Exibindo informações sobre as configurações de segurança do servidor CIFS](#)

[Alterando senhas de contas de usuário locais](#)

Grupos BUILTIN predefinidos e Privileges padrão

Você pode atribuir a associação de um usuário local ou usuário de domínio a um conjunto predefinido de grupos BUILTIN fornecidos pelo ONTAP. Grupos predefinidos têm Privileges predefinidos atribuídos.

A tabela a seguir descreve os grupos predefinidos:

Grupo BUILTIN predefinido	Privileges padrão
BUILTIN\AdministratorsLIVRAR-SE 544 Quando criada pela primeira vez, a conta local Administrator, com um RID de 500, é automaticamente feita um membro deste grupo. Quando a máquina virtual de storage (SVM) é unida a um domínio, o domain\Domain Admins grupo é adicionado ao grupo. Se o SVM sair do domínio, o domain\Domain Admins grupo será removido do grupo.	<ul style="list-style-type: none"> • SeBackupPrivilege • SeRestorePrivilege • SeSecurityPrivilege • SeTakeOwnershipPrivilege • SeChangeNotifyPrivilege
BUILTIN\Power UsersLIVRAR-SE 547 Quando criado pela primeira vez, este grupo não tem nenhum membro. Os membros deste grupo têm as seguintes características: <ul style="list-style-type: none"> • Pode criar e gerenciar usuários e grupos locais. • Não é possível adicionar a si mesmos ou qualquer outro objeto ao BUILTIN\Administrators grupo. 	SeChangeNotifyPrivilege

Grupo BUILTIN predefinido	Privilegios padrão
BUILTIN\Backup OperatorsLIVRAR-SE 551 Quando criado pela primeira vez, este grupo não tem nenhum membro. Os membros deste grupo podem substituir as permissões de leitura e gravação em arquivos ou pastas se forem abertos com intenção de backup.	<ul style="list-style-type: none"> • SeBackupPrivilege • SeRestorePrivilege • SeChangeNotifyPrivilege
BUILTIN\UsersLIVRAR-SE 545 Quando criado pela primeira vez, este grupo não tem nenhum membro (além do grupo especial implícito <code>Authenticated Users</code>). Quando o SVM é associado a um domínio, o <code>domain\Domain Users</code> grupo é adicionado a esse grupo. Se o SVM sair do domínio, o <code>domain\Domain Users</code> grupo será removido desse grupo.	SeChangeNotifyPrivilege
EveryoneSID S-1-1-0 Este grupo inclui todos os utilizadores, incluindo convidados (mas não utilizadores anónimos). Este é um grupo implícito com uma associação implícita.	SeChangeNotifyPrivilege

Informações relacionadas

[Diretrizes para usar grupos BUILTIN e a conta de administrador local](#)

[Lista de Privilegios suportados](#)

[Configuração da verificação transversal de derivação](#)

Ativar ou desativar a funcionalidade de utilizadores e grupos locais

Ative ou desative a visão geral da funcionalidade de usuários e grupos locais

Antes de poder utilizar utilizadores e grupos locais para o controlo de acesso de dados de estilo de segurança NTFS, a funcionalidade de grupo e utilizador local tem de estar ativada. Além disso, se você quiser usar usuários locais para autenticação SMB, a funcionalidade de autenticação de usuário local deve estar ativada.

A funcionalidade de utilizadores e grupos locais e a autenticação de utilizadores locais são ativadas por predefinição. Se eles não estiverem ativados, você deverá ativá-los antes de configurar e usar usuários e grupos locais. Você pode desativar a funcionalidade de usuários e grupos locais a qualquer momento.

Além de desabilitar explicitamente a funcionalidade de usuário local e grupo, o ONTAP desabilita a funcionalidade de usuário local e grupo se qualquer nó no cluster for revertido para uma versão do ONTAP que não ofereça suporte à funcionalidade. A funcionalidade de usuário e grupo local não é ativada até que todos os nós do cluster estejam executando uma versão do ONTAP que o suporte.

Informações relacionadas

[Modificar contas de usuário locais](#)

[Modificar grupos locais](#)

[Adicione Privileges a usuários ou grupos locais ou de domínio](#)

Ative ou desative usuários e grupos locais

Você pode ativar ou desativar usuários locais e grupos para acesso SMB em máquinas virtuais de armazenamento (SVMs). A funcionalidade de utilizadores e grupos locais está ativada por predefinição.

Sobre esta tarefa

Você pode usar usuários e grupos locais ao configurar permissões de compartilhamento SMB e arquivos NTFS e pode, opcionalmente, usar usuários locais para autenticação ao criar uma conexão SMB. Para utilizar utilizadores locais para autenticação, também tem de ativar a opção de autenticação utilizadores locais e grupos.

Passos

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

Se você quiser que os usuários e grupos locais sejam...	Digite o comando...
Ativado	<code>vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled true</code>
Desativado	<code>vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled false</code>

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

Exemplo

O exemplo a seguir habilita a funcionalidade de usuários e grupos locais 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 -is-local-users-and
-groups-enabled true

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

Informações relacionadas

[Ativar ou desativar a autenticação de utilizador local](#)

[Ativar ou desativar contas de utilizador locais](#)

Ativar ou desativar a autenticação de utilizador local

Você pode ativar ou desativar a autenticação de usuário local para acesso SMB em máquinas virtuais de armazenamento (SVMs). O padrão é permitir a autenticação de usuário local, o que é útil quando o SVM não pode entrar em Contato com um controlador de domínio ou se você optar por não usar controles de acesso em nível de domínio.

Antes de começar

A funcionalidade de usuários e grupos locais deve estar ativada no servidor CIFS.

Sobre esta tarefa

Você pode ativar ou desativar a autenticação de usuário local a qualquer momento. Se você quiser usar usuários locais para autenticação ao criar uma conexão SMB, também deverá ativar a opção usuários e grupos locais do servidor CIFS.

Passos

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

Se você quiser que a autenticação local seja...	Digite o comando...
Ativado	<pre>vserver cifs options modify -vserver vserver_name -is-local-auth-enabled true</pre>
Desativado	<pre>vserver cifs options modify -vserver vserver_name -is-local-auth-enabled false</pre>

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

Exemplo

O exemplo a seguir habilita a autenticação de usuário local 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 -is-local-auth
-enabled true

cluster1::*> set -privilege admin

```

Informações relacionadas

[Como funciona a autenticação de usuário local](#)

[Ativar ou desativar utilizadores e grupos locais](#)

Gerenciar contas de usuários locais

Modificar contas de usuário locais

Você pode modificar uma conta de usuário local se quiser alterar o nome completo ou a descrição de um usuário existente e se quiser ativar ou desativar a conta de usuário. Você também pode renomear uma conta de usuário local se o nome do usuário estiver comprometido ou se uma alteração de nome for necessária para fins administrativos.

Se você quiser...	Digite o comando...
Modifique o nome completo do usuário local	<code>vserver cifs users-and-groups local-user modify -vserver vserver_name -user -name user_name -full-name text</code> Se o nome completo contiver um espaço, ele deve ser incluído entre aspas duplas.
Modifique a descrição do usuário local	<code>vserver cifs users-and-groups local-user modify -vserver vserver_name -user -name user_name -description text</code> Se a descrição contém um espaço, então ele deve ser fechado dentro de aspas duplas.
Ative ou desative a conta de utilizador local	<code>`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account-disabled {true</code>
<code>false}`</code>	Renomeie a conta de usuário local

Exemplo

O exemplo a seguir renomeia o usuário local "CIFS_SERVER" para "CIFS_Server' sue_new" na máquina virtual de armazenamento (SVM, anteriormente conhecida como SVM) VS1:

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name  
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

Ativar ou desativar contas de utilizador locais

Você ativa uma conta de usuário local se quiser que o usuário possa acessar os dados contidos na máquina virtual de armazenamento (SVM) em uma conexão SMB. Você também pode desativar uma conta de usuário local se não quiser que esse usuário acesse dados do SVM em SMB.

Sobre esta tarefa

Você ativa um usuário local modificando a conta de usuário.

Passo

1. Execute a ação apropriada:

Se você quiser...	Digite o comando...
Ative a conta de utilizador	<pre>vserver cifs users-and-groups local- user modify -vserver vserver_name -user-name user_name -is-account -disabled false</pre>
Desative a conta de usuário	<pre>vserver cifs users-and-groups local- user modify -vserver vserver_name -user-name user_name -is-account -disabled true</pre>

Altere as senhas da conta de usuário local

Pode alterar a palavra-passe da conta de um utilizador local. Isso pode ser útil se a senha do usuário for comprometida ou se o usuário tiver esquecido a senha.

Passo

1. Altere a senha executando a ação apropriada:

```
vserver cifs users-and-groups local-user  
set-password -vserver vserver_name -user-name user_name
```

Exemplo

O exemplo a seguir define a senha do usuário local "CIFS_Server" associada à máquina virtual de armazenamento (SVM, anteriormente conhecida como SVM) VS1:


```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1
```

Enter the new password:

Confirm the new password:

Informações relacionadas

[Ativar ou desativar a complexidade de senha necessária para usuários SMB locais](#)

[Exibindo informações sobre as configurações de segurança do servidor CIFS](#)

Exibir informações sobre usuários locais

Você pode exibir uma lista de todos os usuários locais em um formulário de resumo. Se você quiser determinar quais configurações de conta estão configuradas para um usuário específico, você pode exibir informações detalhadas de conta para esse usuário, bem como as informações de conta para vários usuários. Essas informações podem ajudá-lo a determinar se você precisa modificar as configurações de um usuário e também solucionar problemas de autenticação ou acesso a arquivos.

Sobre esta tarefa

As informações sobre a palavra-passe de um utilizador nunca são apresentadas.

Passo

1. Execute uma das seguintes ações:

Se você quiser...	Digite o comando...
Exibir informações sobre todos os usuários na máquina virtual de storage (SVM)	<pre>vserver cifs users-and-groups local- user show -vserver <i>vserver_name</i></pre>
Exibir informações detalhadas da conta para um usuário	<pre>vserver cifs users-and-groups local- user show -instance -vserver <i>vserver_name</i> -user-name <i>user_name</i></pre>

Há outros parâmetros opcionais que você pode escolher quando você executa o comando. Consulte a página de manual para obter mais informações.

Exemplo

O exemplo a seguir exibe informações sobre todos os usuários locais no SVM VS1:

```

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                Full Name      Description
-----  -
vs1      CIFS_SERVER\Administrator  James Smith   Built-in administrator
account
vs1      CIFS_SERVER\sue           Sue    Jones

```

Exibir informações sobre associações de grupos para usuários locais

Você pode exibir informações sobre os grupos locais aos quais um usuário local pertence. Você pode usar essas informações para determinar qual acesso o usuário deve ter aos arquivos e pastas. Essas informações podem ser úteis para determinar quais direitos de acesso o usuário deve ter a arquivos e pastas ou ao solucionar problemas de acesso ao arquivo.

Sobre esta tarefa

Você pode personalizar o comando para exibir apenas as informações que deseja ver.

Passo

1. Execute uma das seguintes ações:

Se você quiser...	Digite o comando...
Exibir informações de associação de usuário local para um usuário local especificado	<code>vserver cifs users-and-groups local-user show-membership -user-name <i>user_name</i></code>
Exibir informações de associação de usuários locais para o grupo local do qual esse usuário local é membro	<code>vserver cifs users-and-groups local-user show-membership -membership <i>group_name</i></code>
Exibir informações de associação de usuários para usuários locais associados a uma máquina virtual de armazenamento (SVM) especificada	<code>vserver cifs users-and-groups local-user show-membership -vserver <i>vserver_name</i></code>
Exibir informações detalhadas de todos os usuários locais em um SVM especificado	<code>vserver cifs users-and-groups local-user show-membership -instance -vserver <i>vserver_name</i></code>

Exemplo

O exemplo a seguir exibe as informações de associação para todos os usuários locais no SVM VS1; o usuário "CIFS_SERVER" é membro do grupo "BUILTIN" Administradores, e "CIFS_Server" é membro do grupo "CIFS_Server' G1":

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver      User Name                               Membership
-----
vs1          CIFS_SERVER\Administrator              BUILTIN\Administrators
            CIFS_SERVER\sue                       CIFS_SERVER\g1
```

Eliminar contas de utilizador locais

Você pode excluir contas de usuários locais da máquina virtual de storage (SVM) se elas não forem mais necessárias para a autenticação SMB local para o servidor CIFS ou para determinar os direitos de acesso aos dados contidos no SVM.

Sobre esta tarefa

Tenha em mente o seguinte ao excluir usuários locais:

- O sistema de ficheiros não foi alterado.

Os descritores de segurança do Windows em arquivos e diretórios que se referem a esse usuário não são ajustados.

- Todas as referências a usuários locais são removidas dos bancos de dados de associação e Privileges.
- Usuários padrão e bem conhecidos, como Administrador, não podem ser excluídos.

Passos

1. Determine o nome da conta de usuário local que você deseja excluir: `vserver cifs users-and-groups local-user show -vserver vserver_name`
2. Eliminar o utilizador local: `vserver cifs users-and-groups local-user delete -vserver vserver_name -user-name username_name`
3. Verifique se a conta de usuário foi excluída: `vserver cifs users-and-groups local-user show -vserver vserver_name`

Exemplo

O exemplo a seguir exclui o usuário local "CIFS_Server" associado ao SVM VS1:

```

cluster1::> vsserver cifs users-and-groups local-user show -vsserver vs1
Vserver  User Name                Full Name                Description
-----  -
vs1      CIFS_SERVER\Administrator  James Smith             Built-in administrator
account
vs1      CIFS_SERVER\sue           Sue Jones

```

```

cluster1::> vsserver cifs users-and-groups local-user delete -vsserver vs1
-user-name CIFS_SERVER\sue

```

```

cluster1::> vsserver cifs users-and-groups local-user show -vsserver vs1
Vserver  User Name                Full Name                Description
-----  -
vs1      CIFS_SERVER\Administrator  James Smith             Built-in administrator
account

```

Gerenciar grupos locais

Modificar grupos locais

Você pode modificar grupos locais existentes alterando a descrição de um grupo local existente ou renomeando o grupo.

Se você quiser...	Use o comando...
Modifique a descrição do grupo local	<code>vsserver cifs users-and-groups local-group modify -vsserver <i>vserver_name</i> -group-name <i>group_name</i> -description <i>text</i></code> Se a descrição contém um espaço, então ele deve ser fechado dentro de aspas duplas.
Renomeie o grupo local	<code>vsserver cifs users-and-groups local-group rename -vsserver <i>vserver_name</i> -group-name <i>group_name</i> -new-group-name <i>new_group_name</i></code>

Exemplos

O exemplo a seguir renomeia o grupo local "CIFS_SERVER' Engineering" para "CIFS_Server' Engineering_new":

```

cluster1::> vsserver cifs users-and-groups local-group rename -vsserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new

```

O exemplo a seguir modifica a descrição do grupo local "CIFS_SERVER' Engineering":

```
cluster1::> vsserver cifs users-and-groups local-group modify -vsserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

Exibir informações sobre grupos locais

É possível exibir uma lista de todos os grupos locais configurados no cluster ou em uma máquina virtual de armazenamento (SVM) especificada. Essas informações podem ser úteis ao solucionar problemas de acesso a arquivos para dados contidos no SVM ou problemas de direitos de usuário (privilégios) no SVM.

Passo

1. Execute uma das seguintes ações:

Se você quiser informações sobre...	Digite o comando...
Todos os grupos locais no cluster	<code>vsserver cifs users-and-groups local-group show</code>
Todos os grupos locais no SVM	<code>vsserver cifs users-and-groups local-group show -vsserver vsserver_name</code>

Há outros parâmetros opcionais que você pode escolher quando você executar este comando. Consulte a página de manual para obter mais informações.

Exemplo

O exemplo a seguir exibe informações sobre todos os grupos locais no SVM VS1:

```
cluster1::> vsserver cifs users-and-groups local-group show -vsserver vs1
Vserver  Group Name                Description
-----  -
vs1      BUILTIN\Administrators    Built-in Administrators group
vs1      BUILTIN\Backup Operators  Backup Operators group
vs1      BUILTIN\Power Users       Restricted administrative privileges
vs1      BUILTIN\Users             All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

Gerenciar a associação ao grupo local

Você pode gerenciar a associação de grupo local adicionando e removendo usuários locais ou de domínio ou adicionando e removendo grupos de domínio. Isso é útil se você quiser controlar o acesso a dados com base nos controles de acesso colocados no grupo ou se quiser que os usuários tenham o Privileges associado a esse grupo.

Sobre esta tarefa

Diretrizes para adicionar membros a um grupo local:

- Você não pode adicionar usuários ao grupo especial *todos*.
- O grupo local deve existir antes de poder adicionar um utilizador a ele.
- O utilizador tem de existir antes de poder adicionar o utilizador a um grupo local.
- Não é possível adicionar um grupo local a outro grupo local.
- Para adicionar um usuário ou grupo de domínio a um grupo local, o Data ONTAP deve ser capaz de resolver o nome para um SID.

Diretrizes para remover membros de um grupo local:

- Você não pode remover membros do grupo especial *todos*.
- O grupo do qual você deseja remover um membro deve existir.
- O ONTAP deve ser capaz de resolver os nomes dos membros que você deseja remover do grupo para um SID correspondente.

Passo

1. Adicione ou remova um membro em um grupo.

Se você quiser...	Em seguida, use o comando...
Adicione um membro a um grupo	<pre>vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]</pre> <p>Você pode especificar uma lista delimitada por vírgulas de usuários locais, usuários de domínio ou grupos de domínio para adicionar ao grupo local especificado.</p>
Remova um membro de um grupo	<pre>vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]</pre> <p>Você pode especificar uma lista delimitada por vírgulas de usuários locais, usuários de domínio ou grupos de domínio a serem removidos do grupo local especificado.</p>

O exemplo a seguir adiciona um usuário local "SMB_SERVER" e um grupo de domínio "AD_Dom_eng" ao grupo local "SMB_SERVER' Engineering" no SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-group add-members  
-vserver vs1 -group-name SMB_SERVER\engineering -member-names  
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

O exemplo a seguir remove os usuários locais "SMB_SERVER" e "SMB_SERVER' james" do grupo local

"SMB_Server' Engineering" no SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Informações relacionadas

[Exibindo informações sobre membros de grupos locais](#)

Exibir informações sobre membros de grupos locais

É possível exibir uma lista de todos os membros de grupos locais configurados no cluster ou em uma máquina virtual de armazenamento especificada (SVM). Essas informações podem ser úteis ao solucionar problemas de acesso a arquivos ou problemas de direitos de usuário (privilégios).

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre...	Digite o comando...
Membros de todos os grupos locais no cluster	<pre>vserver cifs users-and-groups local- group show-members</pre>
Membros de todos os grupos locais no SVM	<pre>vserver cifs users-and-groups local- group show-members -vserver vserver_name</pre>

Exemplo

O exemplo a seguir exibe informações sobre membros de todos os grupos locais no SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver      Group Name                Members
-----
vs1          BUILTIN\Administrators   CIFS_SERVER\Administrator
                                     AD_DOMAIN\Domain Admins
                                     AD_DOMAIN\dom_grpl
                                     BUILTIN\Users
                                     AD_DOMAIN\Domain Users
                                     AD_DOMAIN\dom_usr1
                                     CIFS_SERVER\engineering   CIFS_SERVER\james
```

Eliminar um grupo local

Você poderá excluir um grupo local da máquina virtual de storage (SVM) se não for mais

necessário para determinar direitos de acesso a dados associados a esse SVM ou se não for mais necessário atribuir direitos de usuário (Privileges) a membros do grupo.

Sobre esta tarefa

Tenha em mente o seguinte ao excluir grupos locais:

- O sistema de ficheiros não foi alterado.

Os descritores de segurança do Windows em arquivos e diretórios que se referem a esse grupo não são ajustados.

- Se o grupo não existir, um erro será retornado.
- O grupo especial *todos* não pode ser excluído.
- Grupos internos, como *BUILTIN__BUILTIN/Users*, não podem ser excluídos.

Passos

1. Determine o nome do grupo local que você deseja excluir exibindo a lista de grupos locais no SVM:
`vserver cifs users-and-groups local-group show -vserver vserver_name`
2. Eliminar o grupo local: `vserver cifs users-and-groups local-group delete -vserver vserver_name -group-name group_name`
3. Verifique se o grupo foi excluído: `vserver cifs users-and-groups local-user show -vserver vserver_name`

Exemplo

O exemplo a seguir exclui o grupo local "CIFS_SERVER" associado ao SVM VS1:


```

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver      Group Name                Description
-----
vs1          BUILTIN\Administrators    Built-in Administrators group
vs1          BUILTIN\Backup Operators  Backup Operators group
vs1          BUILTIN\Power Users       Restricted administrative
privileges
vs1          BUILTIN\Users             All users
vs1          CIFS_SERVER\engineering
vs1          CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver      Group Name                Description
-----
vs1          BUILTIN\Administrators    Built-in Administrators group
vs1          BUILTIN\Backup Operators  Backup Operators group
vs1          BUILTIN\Power Users       Restricted administrative
privileges
vs1          BUILTIN\Users             All users
vs1          CIFS_SERVER\engineering

```

Atualizar nomes de usuários e grupos de domínio em bancos de dados locais

Você pode adicionar usuários e grupos de domínio aos grupos locais de um servidor CIFS. Esses objetos de domínio são registrados em bancos de dados locais no cluster. Se um objeto de domínio for renomeado, os bancos de dados locais devem ser atualizados manualmente.

Sobre esta tarefa

Você deve especificar o nome da máquina virtual de armazenamento (SVM) na qual deseja atualizar nomes de domínio.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Execute a ação apropriada:

Se você quiser atualizar usuários e grupos de domínio e...	Use este comando...
Exibir usuários e grupos de domínio que foram atualizados com êxito e que falharam na atualização	<code>vserver cifs users-and-groups update-names -vserver vserver_name</code>

Se você quiser atualizar usuários e grupos de domínio e...	Use este comando...
Exibir usuários e grupos de domínio que foram atualizados com êxito	<pre>vserver cifs users-and-groups update- names -vserver vserver_name -display -failed-only false</pre>
Exiba apenas os usuários e grupos de domínio que não conseguem atualizar	<pre>vserver cifs users-and-groups update- names -vserver vserver_name -display -failed-only true</pre>
Suprimir todas as informações de status sobre atualizações	<pre>vserver cifs users-and-groups update- names -vserver vserver_name -suppress -all-output true</pre>

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

Exemplo

O exemplo a seguir atualiza os nomes de usuários e grupos de domínio associados à máquina virtual de armazenamento (SVM, anteriormente conhecido como SVM) VS1. Para a última atualização, há uma cadeia de nomes dependente que precisa ser atualizada:

```

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 users-and-groups update-names -vserver vs1

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654321-12345
Domain:           EXAMPLE1
Out-of-date Name: dom_user1
Updated Name:     dom_user2
Status:           Successfully updated

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654322-23456
Domain:           EXAMPLE2
Out-of-date Name: dom_user1
Updated Name:     dom_user2
Status:           Successfully updated

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654321-123456
Domain:           EXAMPLE1
Out-of-date Name: dom_user3
Updated Name:     dom_user4
Status:           Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                  to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                  to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                  to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                  to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin

```

Gerenciar Privileges local

Adicione Privileges a usuários ou grupos locais ou de domínio

Você pode gerenciar os direitos de usuário para usuários ou grupos locais ou de domínio adicionando o Privileges. O Privileges adicionado substitui o Privileges padrão atribuído a qualquer um desses objetos. Isso fornece segurança aprimorada, permitindo que você personalize o que o Privileges um usuário ou grupo tem.

Antes de começar

O usuário ou grupo local ou domínio ao qual o Privileges será adicionado já deve existir.

Sobre esta tarefa

Adicionar um privilégio a um objeto substitui o Privileges padrão para esse usuário ou grupo. Adicionar um privilégio não remove Privileges adicionados anteriormente.

Você deve ter em mente o seguinte ao adicionar o Privileges a usuários ou grupos locais ou de domínio:

- Você pode adicionar um ou mais Privileges.
- Ao adicionar Privileges a um usuário ou grupo de domínio, o ONTAP pode validar o usuário ou grupo de domínio contatando o controlador de domínio.

O comando pode falhar se o ONTAP não conseguir entrar em Contato com o controlador de domínio.

Passos

1. Adicione um ou mais Privileges a um usuário ou grupo local ou de domínio: `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. Verifique se os Privileges desejados são aplicados ao objeto: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Exemplo

O exemplo a seguir adiciona o "SeTcbPrivilege" e o "SeTakeOwnershipPrivilege" do Privileges ao usuário "SERVIDOR_Sue" na máquina virtual de armazenamento (SVM, anteriormente conhecida como CIFS) VS1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          CIFS_SERVER\sue        SeTcbPrivilege
                                     SeTakeOwnershipPrivilege
```

Remova o Privileges de usuários ou grupos locais ou de domínio

Você pode gerenciar os direitos de usuário para usuários ou grupos locais ou de domínio removendo o Privileges. Isso fornece segurança aprimorada, permitindo que você personalize o Privileges máximo que os usuários e grupos têm.

Antes de começar

O usuário ou grupo local ou domínio do qual o Privileges será removido já deve existir.

Sobre esta tarefa

Você deve ter em mente o seguinte ao remover o Privileges de usuários ou grupos locais ou de domínio:

- Você pode remover um ou mais Privileges.
- Ao remover o Privileges de um usuário ou grupo de domínio, o ONTAP pode validar o usuário ou grupo de domínio entrando em Contato com o controlador de domínio.

O comando pode falhar se o ONTAP não conseguir entrar em Contato com o controlador de domínio.

Passos

1. Remova um ou mais Privileges de um usuário ou grupo local ou de domínio: `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. Verifique se os Privileges desejados foram removidos do objeto: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Exemplo

O exemplo a seguir remove o Privileges "SeTcbPrivilege" e o "SeTakeOwnershipPrivilege" do usuário ""SERVIDOR_Sue"" na máquina virtual de armazenamento (SVM, anteriormente conhecida como CIFS) VS1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          CIFS_SERVER\sue        SeTcbPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          CIFS_SERVER\sue        -
```

Redefinir o Privileges para usuários e grupos locais ou de domínio

Você pode redefinir o Privileges para usuários e grupos locais ou de domínio. Isso pode ser útil quando você fez modificações no Privileges para um usuário ou grupo local ou de domínio e essas modificações não são mais desejadas ou necessárias.

Sobre esta tarefa

A redefinição do Privileges para um usuário ou grupo local ou de domínio remove quaisquer entradas de privilégio para esse objeto.

Passos

1. Redefina o Privileges em um usuário ou grupo local ou de domínio: `vserver cifs users-and-groups privilege reset-privilege -vserver vserver_name -user-or-group-name name`
2. Verifique se os Privileges são redefinidos no objeto: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Exemplos

O exemplo a seguir redefine o Privileges no usuário "CIFS_SERVER" na máquina virtual de armazenamento (SVM, anteriormente conhecida como SVM) VS1. Por padrão, os usuários normais não têm o Privileges associado às suas contas:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver    User or Group Name      Privileges
-----
vs1        CIFS_SERVER\sue        SeTcbPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

O exemplo a seguir redefine o Privileges para o grupo "Administradores", removendo efetivamente a entrada de privilégio:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver    User or Group Name      Privileges
-----
vs1        BUILTIN\Administrators  SeRestorePrivilege
                               SeSecurityPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Exibir informações sobre substituições de privilégios

Você pode exibir informações sobre Privileges personalizados atribuídos a grupos ou contas de usuário locais ou de domínio. Essas informações ajudam a determinar se os direitos de usuário desejados são aplicados.

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre...	Digite este comando...
Privilegios personalizado para todos os usuários e grupos de domínio e locais na máquina virtual de storage (SVM)	<code>vserver cifs users-and-groups privilege show -vserver <i>vserver_name</i></code>
Privilegios personalizado para um domínio específico ou usuário local e grupo no SVM	<code>vserver cifs users-and-groups privilege show -vserver <i>vserver_name</i> -user-or-group-name <i>name</i></code>

Há outros parâmetros opcionais que você pode escolher quando você executar este comando. Consulte a página de manual para obter mais informações.

Exemplo

O comando a seguir exibe todos os Privilegios explicitamente associados a usuários e grupos locais ou de domínio para o SVM VS1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                   SeRestorePrivilege
vs1          CIFS_SERVER\sue         SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

Configure a verificação de desvio transversal

Configure a visão geral da verificação da travessia de derivação

A verificação de desvio transversal é um direito de usuário (também conhecido como *privilégio*) que determina se um usuário pode percorrer todos os diretórios no caminho para um arquivo, mesmo que o usuário não tenha permissões no diretório atravessado. Você deve entender o que acontece ao permitir ou desativar a verificação de desvio transversal e como configurar a verificação de desvio transversal para usuários em máquinas virtuais de armazenamento (SVMs).

O que acontece ao permitir ou ao desativar a verificação transversal de desvio

- Se permitido, quando um usuário tenta acessar um arquivo, o ONTAP não verifica a permissão de avanço para os diretórios intermediários ao determinar se deve conceder ou negar acesso ao arquivo.
- Se não for permitido, o ONTAP verifica a permissão de avanço (execução) para todos os diretórios no caminho para o arquivo.

Se qualquer um dos diretórios intermediários não tiver o "X" (permissão de avanço), o ONTAP nega o

acesso ao arquivo.

Configure a verificação de desvio transversal

Você pode configurar a verificação de desvio transversal usando a CLI do ONTAP ou configurando políticas de grupo do active Directory com esse direito de usuário.

O `SeChangeNotifyPrivilege` privilégio controla se os usuários têm permissão para ignorar a verificação transversal.

- Adicioná-lo a usuários ou grupos SMB locais na SVM ou a usuários ou grupos de domínio permite a verificação de desvio transversal.
- Removê-lo de usuários ou grupos SMB locais no SVM ou de usuários ou grupos de domínio não permite a verificação de desvio transversal.

Por padrão, os seguintes grupos BUILTIN no SVM têm o direito de ignorar a verificação transversal:

- `BUILTIN\Administrators`
- `BUILTIN\Power Users`
- `BUILTIN\Backup Operators`
- `BUILTIN\Users`
- `Everyone`

Se você não quiser permitir que membros de um desses grupos ignorem a verificação transversal, você deve remover esse privilégio do grupo.

Você deve ter em mente o seguinte ao configurar a verificação de desvio transversal para usuários e grupos SMB locais no SVM usando a CLI:

- Se você quiser permitir que membros de um grupo de domínio ou local personalizado ignorem a verificação transversal, você deve adicionar o `SeChangeNotifyPrivilege` privilégio a esse grupo.
- Se você quiser permitir que um usuário local ou de domínio individual ignore a verificação transversal e que o usuário não seja membro de um grupo com esse privilégio, você pode adicionar o `SeChangeNotifyPrivilege` privilégio a essa conta de usuário.
- Você pode desativar a verificação de desvio transversal para usuários ou grupos locais ou de domínio removendo o `SeChangeNotifyPrivilege` privilégio a qualquer momento.



Para desativar a verificação de desvio de travers para usuários ou grupos locais ou de domínio especificados, você também deve remover o `SeChangeNotifyPrivilege` privilégio do `Everyone` grupo.

Informações relacionadas

[Permitir que usuários ou grupos ignorem a verificação da rotação do diretório](#)

[Não permitir que usuários ou grupos ignorem a verificação da rotação do diretório](#)

[Configure o mapeamento de caracteres para a tradução de nomes de arquivo SMB em volumes](#)

[Criar listas de controle de acesso de compartilhamento SMB](#)

[Proteja o acesso aos arquivos usando o Storage-Level Access Guard](#)

[Lista de Privileges suportados](#)

[Adicione Privileges a usuários ou grupos locais ou de domínio](#)

Permitir que usuários ou grupos ignorem a verificação da rotação do diretório

Se você quiser que um usuário possa percorrer todos os diretórios no caminho para um arquivo, mesmo que o usuário não tenha permissões em um diretório atravessado, você pode adicionar o `SeChangeNotifyPrivilege` privilégio a usuários ou grupos SMB locais em máquinas virtuais de armazenamento (SVMs). Por padrão, os usuários são capazes de ignorar a verificação de rotação do diretório.

Antes de começar

- Um servidor SMB deve estar presente na SVM.
- A opção local Users and Groups SMB Server (usuários locais e grupos) deve estar ativada.
- O usuário ou grupo local ou domínio ao qual o `SeChangeNotifyPrivilege` privilégio será adicionado já deve existir.

Sobre esta tarefa

Ao adicionar Privileges a um usuário ou grupo de domínio, o ONTAP pode validar o usuário ou grupo de domínio contatando o controlador de domínio. O comando pode falhar se o ONTAP não puder entrar em Contato com o controlador de domínio.

Passos

1. Ative a verificação de desvio transversal adicionando o `SeChangeNotifyPrivilege` privilégio a um usuário ou grupo local ou de domínio:

```
vserver cifs users-and-groups privilege add-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege
```

O valor para o `-user-or-group-name` parâmetro é um usuário ou grupo local, ou um usuário ou grupo de domínio.

2. Verifique se o usuário ou grupo especificado tem a verificação transversal de desvio ativada:

```
vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name
```

Exemplo

O comando a seguir permite que os usuários que pertencem ao grupo "EXAMPLE" ignorem a verificação da rotação do diretório adicionando o `SeChangeNotifyPrivilege` privilégio ao grupo:

```

cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          EXAMPLE\eng              SeChangeNotifyPrivilege

```

Informações relacionadas

[Não permitir que usuários ou grupos ignorem a verificação da rotação do diretório](#)

Não permitir que usuários ou grupos ignorem a verificação da rotação do diretório

Se você não quiser que um usuário percorra todos os diretórios no caminho para um arquivo porque o usuário não tem permissões no diretório atravessado, você pode remover o `SeChangeNotifyPrivilege` privilégio de usuários SMB locais ou grupos em máquinas virtuais de armazenamento (SVMs).

Antes de começar

O usuário ou grupo local ou domínio do qual o Privileges será removido já deve existir.

Sobre esta tarefa

Ao remover o Privileges de um usuário ou grupo de domínio, o ONTAP pode validar o usuário ou grupo de domínio entrando em Contato com o controlador de domínio. O comando pode falhar se o ONTAP não puder entrar em Contato com o controlador de domínio.

Passos

1. Não permitir a verificação da travessa de derivação: `vserver cifs users-and-groups privilege remove-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

O comando remove o `SeChangeNotifyPrivilege` privilégio do usuário ou grupo local ou domínio que você especificar com o valor do `-user-or-group-name name` parâmetro.

2. Verifique se o usuário ou grupo especificado tem verificação de desvio de rotação desativada: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Exemplo

O comando a seguir despermite que os usuários que pertencem ao grupo "EXAMPLE" ignorem a verificação da rotação do diretório:

```

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          EXAMPLE\eng              SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          EXAMPLE\eng              -

```

Informações relacionadas

[Permitir que usuários ou grupos ignorem a verificação de rotação do diretório](#)

Exibir informações sobre segurança de arquivos e diretivas de auditoria

Exibir informações sobre a visão geral das políticas de auditoria e segurança de arquivos

Você pode exibir informações sobre segurança de arquivos em arquivos e diretórios contidos em volumes em máquinas virtuais de armazenamento (SVMs). Você pode exibir informações sobre políticas de auditoria no FlexVol volumes. Se configurado, você pode exibir informações sobre as configurações de segurança do Guarda de Acesso em nível de armazenamento e Controle Dinâmico de Acesso no FlexVol volumes.

Exibindo informações sobre segurança de arquivos

Você pode exibir informações sobre a segurança de arquivos aplicada a dados contidos em volumes e qtrees (para volumes FlexVol) com os seguintes estilos de segurança:

- NTFS
- UNIX
- Misto

Exibindo informações sobre políticas de auditoria

Você pode exibir informações sobre políticas de auditoria para auditar eventos de acesso em volumes do FlexVol nos seguintes protocolos nas:

- SMB (todas as versões)
- NFSv4.x

Exibindo informações sobre a segurança do Storage-Level Access Guard (SLAG)

A segurança do Access Guard no nível de storage pode ser aplicada em volumes e objetos de qtree do FlexVol com os seguintes estilos de segurança:

- NTFS
- Misto
- UNIX (se um servidor CIFS estiver configurado na SVM que contém o volume)

Apresentar informações sobre a segurança do controle de acesso dinâmico (DAC)

A segurança do controle de acesso dinâmico pode ser aplicada em um objeto dentro de um FlexVol volume com os seguintes estilos de segurança:

- NTFS
- Misto (se o objeto tiver segurança efetiva NTFS)

Informações relacionadas

[Protegendo o acesso aos arquivos usando o Storage-Level Access Guard](#)

[Exibindo informações sobre o Storage-Level Access Guard](#)

Exibir informações sobre segurança de arquivos em volumes de estilo de segurança NTFS

Você pode exibir informações sobre a segurança de arquivos e diretórios em volumes de estilo de segurança NTFS, incluindo o estilo de segurança e estilos de segurança eficazes, quais permissões são aplicadas e informações sobre os atributos dos. Você pode usar os resultados para validar sua configuração de segurança ou para solucionar problemas de acesso a arquivos.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os dados cujas informações de segurança de arquivo ou pasta você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

- Como os volumes e qtrees de estilo de segurança NTFS usam apenas permissões de arquivo NTFS e usuários e grupos do Windows ao determinar direitos de acesso a arquivos, os campos de saída relacionados ao UNIX contêm informações de permissão de arquivo UNIX somente para exibição.
- A saída ACL é exibida para arquivos e pastas com segurança NTFS.
- Como a segurança do Storage-Level Access Guard pode ser configurada na raiz de volume ou qtree, a saída para um caminho de volume ou qtree em que o Storage-Level Access Guard está configurado pode exibir ACLs de arquivo regulares e ACLs de Storage-Level Access Guard.
- A saída também exibe informações sobre os ACEs do Controle de Acesso Dinâmico se o Controle de Acesso Dinâmico estiver configurado para o caminho do arquivo ou diretório específico.

Passo

1. Exiba as configurações de segurança de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações...	Digite o seguinte comando...
Em forma de resumo	<code>vserver security file-directory show -vserver vserver_name -path path</code>

Se você quiser exibir informações...	Digite o seguinte comando...
Com detalhes expandidos	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>

Exemplos

O exemplo a seguir exibe as informações de segurança sobre o caminho /vol4 no SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

          Vserver: vs1
          File Path: /vol4
    File Inode Number: 64
      Security Style: ntfs
    Effective Style: ntfs
      DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
          ACLs: NTFS Security Descriptor
                Control:0x8004
                Owner: BUILTIN\Administrators
                Group: BUILTIN\Administrators
                DACL - ACEs
                ALLOW-Everyone-0x1f01ff
                ALLOW-Everyone-0x10000000-

OI|CI|IO
```

O exemplo a seguir exibe as informações de segurança com máscaras expandidas sobre o caminho /data/engineering no SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true

          Vserver: vs1
          File Path: /data/engineering
    File Inode Number: 5544
      Security Style: ntfs
    Effective Style: ntfs
      DOS Attributes: 10
```

```

DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ...0 .... = Offline
    .... ..0. .... = Sparse
    .... .... 0... .... = Normal
    .... .... ..0. .... = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
    Control:0x8004

    1... .... = Self Relative
    .0.. .... = RM Control Valid
    ..0. .... = SACL Protected
    ...0 .... = DACL Protected
    .... 0... .... = SACL Inherited
    .... .0.. .... = DACL Inherited
    .... ..0. .... = SACL Inherit Required
    .... ...0 .... = DACL Inherit Required
    .... .... ..0. .... = SACL Defaulted
    .... .... ...0 .... = SACL Present
    .... .... .... 0... = DACL Defaulted
    .... .... .... .1.. = DACL Present
    .... .... .... ..0. = Group Defaulted
    .... .... .... ...0 = Owner Defaulted

Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs
    ALLOW-Everyone-0x1f01ff
    0... .... =
Generic Read
    .0.. .... =
Generic Write
    ..0. .... =
Generic Execute
    ...0 .... =
Generic All
    .... ..0 .... =
System Security

```

```

.....1..... =
Synchronize

.....1..... =
Write Owner

.....1..... =
Write DAC

.....1..... =
Read Control

.....1..... =
Delete

.....1..... =
Write Attributes

.....1..... =
Read Attributes

.....1..... =
Delete Child

.....1..... =
Execute

.....1..... =
Write EA

.....1..... =
Read EA

.....1..... =
Append

.....1..... =
Write

.....1..... =
Read

ALLOW-Everyone-0x10000000-OI|CI|IO
0..... =
Generic Read

.0..... =
Generic Write

..0..... =
Generic Execute

...1..... =
Generic All

.....0..... =
System Security

.....0..... =
Synchronize

.....0..... =
Write Owner

.....0..... =
Write DAC

```

```

Read Control      .....0..... =
Delete           .....0..... =
Write Attributes  .....0..... =
Read Attributes   .....0..... =
Delete Child     .....0..... =
Execute          .....0..... =
Write EA         .....0..... =
Read EA         .....0..... =
Append          .....0..... =
Write           .....0..... =
Read            .....0..... =

```

O exemplo a seguir exibe informações de segurança, incluindo informações de segurança do Storage-Level Access Guard, para o volume com o caminho /datavol1 no SVM VS1:


```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1
```

```

    Vserver: vs1
    File Path: /datavol1
File Inode Number: 77
    Security Style: ntfs
    Effective Style: ntfs
    DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
        Control:0x8004
        Owner: BUILTIN\Administrators
        Group: BUILTIN\Administrators
        DACL - ACEs
            ALLOW-Everyone-0x1f01ff
            ALLOW-Everyone-0x10000000-OI|CI|IO

Storage-Level Access Guard security
SACL (Applies to Directories):
    AUDIT-EXAMPLE\Domain Users-0x120089-FA
    AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Directories):
    ALLOW-EXAMPLE\Domain Users-0x120089
    ALLOW-EXAMPLE\engineering-0x1f01ff
    ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
SACL (Applies to Files):
    AUDIT-EXAMPLE\Domain Users-0x120089-FA
    AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Files):
    ALLOW-EXAMPLE\Domain Users-0x120089
    ALLOW-EXAMPLE\engineering-0x1f01ff
    ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Informações relacionadas

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

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

Exibir informações sobre segurança de arquivos em volumes mistos de estilo de segurança

Você pode exibir informações sobre segurança de arquivos e diretórios em volumes mistos de estilo de segurança, incluindo o estilo de segurança e estilos de segurança eficazes, quais permissões são aplicadas e informações sobre proprietários e grupos UNIX. Você pode usar os resultados para validar sua configuração de segurança ou para solucionar problemas de acesso a arquivos.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os dados cujas informações de segurança de arquivo ou pasta você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

- Volumes mistos de estilo de segurança e qtrees podem conter alguns arquivos e pastas que usam permissões de arquivo UNIX, bits de modo ou ACLs NFSv4 e alguns arquivos e diretórios que usam permissões de arquivo NTFS.
- O nível superior de um volume de estilo de segurança misto pode ter segurança eficaz UNIX ou NTFS.
- A saída ACL é exibida apenas para arquivos e pastas com segurança NTFS ou NFSv4.

Este campo está vazio para arquivos e diretórios que usam segurança UNIX que têm somente permissões de bit de modo aplicadas (sem ACLs NFSv4).

- Os campos de saída do proprietário e do grupo na saída da ACL aplicam-se apenas no caso de descritores de segurança NTFS.
- Como a segurança do Storage-Level Access Guard pode ser configurada em um volume ou qtree misto de estilo de segurança, mesmo que o estilo de segurança efetivo da raiz de volume ou qtree seja UNIX, a saída para um caminho de volume ou qtree em que o Storage-Level Access Guard esteja configurado pode exibir tanto as permissões de arquivo UNIX quanto as ACLs Storage-Level Access Guard.
- Se o caminho inserido no comando for para dados com segurança efetiva NTFS, a saída também exibirá informações sobre ACEs de Controle de Acesso Dinâmico se o Controle de Acesso Dinâmico estiver configurado para o caminho de arquivo ou diretório dado.

Passo

1. Exiba as configurações de segurança de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações...	Digite o seguinte comando...
Em forma de resumo	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>
Com detalhes expandidos	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>

Exemplos

O exemplo a seguir exibe as informações de segurança sobre o caminho `/projects` no SVM VS1 no formulário de máscara expandida. Este caminho de estilo de segurança misto tem segurança eficaz UNIX.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true
```

```
        Vserver: vs1
        File Path: /projects
File Inode Number: 78
        Security Style: mixed
        Effective Style: unix
        DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ...0 .... .... .... = Offline
    .... ..0. .... .... = Sparse
    .... .... 0... .... = Normal
    .... .... ..0. .... = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
        Unix User Id: 0
        Unix Group Id: 1
        Unix Mode Bits: 700
Unix Mode Bits in Text: rwx-----
        ACLs: -
```

O exemplo a seguir exibe as informações de segurança sobre o caminho /data no SVM VS1. Este caminho misto de estilo de segurança tem uma segurança eficaz NTFS.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data
```

```
          Vserver: vs1
          File Path: /data
    File Inode Number: 544
          Security Style: mixed
          Effective Style: ntfs
          DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
          Unix User Id: 0
          Unix Group Id: 0
          Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
          ACLs: NTFS Security Descriptor
                Control:0x8004
                Owner: BUILTIN\Administrators
                Group: BUILTIN\Administrators
                DACL - ACEs
                    ALLOW-Everyone-0x1f01ff
                    ALLOW-Everyone-0x10000000-
```

OI|CI|IO

O exemplo a seguir exibe as informações de segurança sobre o volume no caminho /datavol5 no SVM VS1. O nível superior deste volume misto de estilo de segurança tem segurança eficaz UNIX. O volume tem segurança Storage-Level Access Guard.

```

cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5

        Vserver: vs1
        File Path: /datavol5
File Inode Number: 3374
        Security Style: mixed
        Effective Style: unix
        DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 755
Unix Mode Bits in Text: rwxr-xr-x
        ACLs: Storage-Level Access Guard security
        SACL (Applies to Directories):
            AUDIT-EXAMPLE\Domain Users-0x120089-FA
            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
            AUDIT-EXAMPLE\market-0x1f01ff-SA
        DACL (Applies to Directories):
            ALLOW-BUILTIN\Administrators-0x1f01ff
            ALLOW-CREATOR OWNER-0x1f01ff
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-EXAMPLE\engineering-0x1f01ff
            ALLOW-EXAMPLE\market-0x1f01ff
        SACL (Applies to Files):
            AUDIT-EXAMPLE\Domain Users-0x120089-FA
            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
            AUDIT-EXAMPLE\market-0x1f01ff-SA
        DACL (Applies to Files):
            ALLOW-BUILTIN\Administrators-0x1f01ff
            ALLOW-CREATOR OWNER-0x1f01ff
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-EXAMPLE\engineering-0x1f01ff
            ALLOW-EXAMPLE\market-0x1f01ff

```

Informações relacionadas

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

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

Exibir informações sobre segurança de arquivos em volumes estilo de segurança UNIX

Você pode exibir informações sobre segurança de arquivos e diretórios em volumes estilo de segurança UNIX, incluindo quais são os estilos de segurança e estilos de segurança eficazes, quais permissões são aplicadas e informações sobre proprietários e

grupos UNIX. Você pode usar os resultados para validar sua configuração de segurança ou para solucionar problemas de acesso a arquivos.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os dados cujas informações de segurança de arquivo ou diretório você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

- Os volumes e qtrees de estilo de segurança UNIX usam apenas permissões de arquivo UNIX, bits de modo ou ACLs NFSv4 ao determinar direitos de acesso a arquivos.
- A saída ACL é exibida apenas para arquivos e pastas com segurança NFSv4.

Este campo está vazio para arquivos e diretórios que usam segurança UNIX que têm somente permissões de bit de modo aplicadas (sem ACLs NFSv4).

- Os campos de saída de proprietário e grupo na saída ACL não se aplicam no caso de descritores de segurança NFSv4.

Eles são apenas significativos para descritores de segurança NTFS.

- Como a segurança do Storage-Level Access Guard é suportada em um volume ou qtree UNIX se um servidor CIFS estiver configurado no SVM, a saída pode conter informações sobre a segurança do Storage-Level Access Guard aplicada ao volume ou qtree especificado no `-path` parâmetro.

Passo

1. Exiba as configurações de segurança de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações...	Digite o seguinte comando...
Em forma de resumo	<pre>vserver security file-directory show -vserver <i>vserver_name</i> -path <i>path</i></pre>
Com detalhes expandidos	<pre>vserver security file-directory show -vserver <i>vserver_name</i> -path <i>path</i> -expand-mask true</pre>

Exemplos

O exemplo a seguir exibe as informações de segurança sobre o caminho `/home` no SVM VS1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
```

```
          Vserver: vs1
          File Path: /home
    File Inode Number: 9590
          Security Style: unix
          Effective Style: unix
          DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
          Unix User Id: 0
          Unix Group Id: 1
          Unix Mode Bits: 700
    Unix Mode Bits in Text: rwx-----
          ACLs: -
```

O exemplo a seguir exibe as informações de segurança sobre o caminho /home no SVM VS1 no formulário de máscara expandida:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true
```

```
          Vserver: vs1
          File Path: /home
    File Inode Number: 9590
          Security Style: unix
          Effective Style: unix
          DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ...0 .... .... .... = Offline
    .... ..0. .... .... = Sparse
    .... .... 0... .... = Normal
    .... .... ..0. .... = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
          Unix User Id: 0
          Unix Group Id: 1
          Unix Mode Bits: 700
    Unix Mode Bits in Text: rwx-----
          ACLs: -
```

Informações relacionadas

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

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

Exibir informações sobre políticas de auditoria NTFS em volumes FlexVol usando a CLI

Você pode exibir informações sobre políticas de auditoria NTFS no FlexVol volumes, incluindo quais são os estilos de segurança e estilos de segurança eficazes, quais permissões são aplicadas e informações sobre listas de controle de acesso do sistema. Você pode usar os resultados para validar sua configuração de segurança ou para solucionar problemas de auditoria.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os arquivos ou pastas cujas informações de auditoria você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

- Os volumes e qtrees de estilo de segurança NTFS usam apenas as listas de controle de acesso do sistema NTFS (SACLs) para políticas de auditoria.
- Arquivos e pastas em um volume misto de estilo de segurança com segurança efetiva NTFS podem ter políticas de auditoria NTFS aplicadas a eles.

Volumes mistos de estilo de segurança e qtrees podem conter alguns arquivos e diretórios que usam permissões de arquivo UNIX, bits de modo ou ACLs NFSv4 e alguns arquivos e diretórios que usam permissões de arquivo NTFS.

- O nível superior de um volume de estilo de segurança misto pode ter segurança efetiva UNIX ou NTFS e pode ou não conter SACLs NTFS.
- Como a segurança do Storage-Level Access Guard pode ser configurada em um volume ou qtree misto de estilo de segurança, mesmo que o estilo de segurança efetivo da raiz de volume ou qtree seja UNIX, a saída para um caminho de volume ou qtree em que o Storage-Level Access Guard está configurado pode exibir tanto o arquivo normal quanto a pasta NFSv4 SACLs e o Storage-Level Access Guard NTFS SACLs.
- Se o caminho inserido no comando for para dados com segurança efetiva NTFS, a saída também exibirá informações sobre ACEs de Controle de Acesso Dinâmico se o Controle de Acesso Dinâmico estiver configurado para o caminho do arquivo ou diretório fornecido.
- Ao exibir informações de segurança sobre arquivos e pastas com segurança efetiva NTFS, os campos de saída relacionados ao UNIX contêm informações de permissão de arquivo UNIX somente para exibição.

Arquivos e pastas de estilo de segurança NTFS usam apenas permissões de arquivo NTFS e usuários e grupos do Windows ao determinar direitos de acesso a arquivos.

- A saída ACL é exibida apenas para arquivos e pastas com segurança NTFS ou NFSv4.

Este campo está vazio para arquivos e pastas que usam segurança UNIX que têm apenas permissões de bits de modo aplicadas (sem ACLs NFSv4).

- Os campos de saída do proprietário e do grupo na saída da ACL aplicam-se apenas no caso de descritores de segurança NTFS.

Passo

1. Exiba as configurações de diretiva de auditoria de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações...	Digite o seguinte comando...
Em forma de resumo	<code>vserver security file-directory show -vserver vserver_name -path path</code>
Como uma lista detalhada	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

Exemplos

O exemplo a seguir exibe as informações da política de auditoria do caminho `/corp` no SVM VS1. O caminho tem segurança eficaz NTFS. O descritor de segurança NTFS contém uma entrada SACL DE sucesso e uma entrada de sucesso/FALHA.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
      Vserver: vs1
      File Path: /corp
      File Inode Number: 357
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
      Control:0x8014
      Owner:DOMAIN\Administrator
      Group:BUILTIN\Administrators
      SACL - ACEs
        ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
        SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
      DACL - ACEs
        ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
        ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
        ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

O exemplo a seguir exibe as informações da política de auditoria do caminho `/datavol1` no SVM VS1. O caminho contém SACLs de arquivo e pasta regulares e SACLs de proteção de acesso em nível de armazenamento.

```

cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

        Vserver: vs1
        File Path: /datavol1
        File Inode Number: 77
        Security Style: ntfs
        Effective Style: ntfs
        DOS Attributes: 10
        DOS Attributes in Text: ----D---
        Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
        Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
              Control:0xaa14
              Owner: BUILTIN\Administrators
              Group: BUILTIN\Administrators
              SACL - ACEs
                AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
              DACL - ACEs
                ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

        Storage-Level Access Guard security
        SACL (Applies to Directories):
          AUDIT-EXAMPLE\Domain Users-0x120089-FA
          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
        DACL (Applies to Directories):
          ALLOW-EXAMPLE\Domain Users-0x120089
          ALLOW-EXAMPLE\engineering-0x1f01ff
          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
        SACL (Applies to Files):
          AUDIT-EXAMPLE\Domain Users-0x120089-FA
          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
        DACL (Applies to Files):
          ALLOW-EXAMPLE\Domain Users-0x120089
          ALLOW-EXAMPLE\engineering-0x1f01ff
          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

Exiba informações sobre as políticas de auditoria do NFSv4 em volumes do FlexVol usando a CLI

Você pode exibir informações sobre as políticas de auditoria do NFSv4 em volumes do FlexVol usando a CLI do ONTAP, incluindo quais são os estilos de segurança e estilos de

segurança eficazes, quais permissões são aplicadas e informações sobre as listas de controle de acesso do sistema (SACLs). Você pode usar os resultados para validar sua configuração de segurança ou para solucionar problemas de auditoria.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os arquivos ou diretórios cujas informações de auditoria você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

- Os volumes e qtrees de estilo de segurança UNIX usam apenas SACLs NFSv4 para políticas de auditoria.
- Arquivos e diretórios em um volume misto de estilo de segurança que são de estilo de segurança UNIX podem ter políticas de auditoria NFSv4 aplicadas a eles.

Volumes mistos de estilo de segurança e qtrees podem conter alguns arquivos e diretórios que usam permissões de arquivo UNIX, bits de modo ou ACLs NFSv4 e alguns arquivos e diretórios que usam permissões de arquivo NTFS.

- O nível superior de um volume de estilo de segurança misto pode ter segurança efetiva UNIX ou NTFS e pode ou não conter SACLs NFSv4.
- A saída ACL é exibida apenas para arquivos e pastas com segurança NTFS ou NFSv4.

Este campo está vazio para arquivos e pastas que usam segurança UNIX que têm apenas permissões de bits de modo aplicadas (sem ACLs NFSv4).

- Os campos de saída do proprietário e do grupo na saída da ACL aplicam-se apenas no caso de descritores de segurança NTFS.
- Como a segurança do Storage-Level Access Guard pode ser configurada em um volume ou qtree misto de estilo de segurança, mesmo que o estilo de segurança efetivo da raiz de volume ou qtree seja UNIX, a saída para um caminho de volume ou qtree em que o Storage-Level Access Guard esteja configurado pode exibir tanto SACLs de arquivo NFSv4 regulares como de diretório e SACLs de acesso no nível de armazenamento NTFS SACLs.
- Como a segurança do Storage-Level Access Guard é suportada em um volume ou qtree UNIX se um servidor CIFS estiver configurado no SVM, a saída pode conter informações sobre a segurança do Storage-Level Access Guard aplicada ao volume ou qtree especificado no `-path` parâmetro.

Passos

1. Exiba as configurações de segurança de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações...	Digite o seguinte comando...
Em forma de resumo	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>
Com detalhes expandidos	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>

Exemplos

O exemplo a seguir exibe as informações de segurança sobre o caminho `/lab` no SVM VS1. Este caminho de

estilo de segurança UNIX tem um SACL NFSv4.

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

      Vserver: vs1
      File Path: /lab
File Inode Number: 288
      Security Style: unix
      Effective Style: unix
      DOS Attributes: 11
DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 0
Unix Mode Bits in Text: -----
      ACLs: NFSV4 Security Descriptor
      Control:0x8014
      SACL - ACEs
              SUCCESSFUL-S-1-520-0-0xf01ff-SA
              FAILED-S-1-520-0-0xf01ff-FA
      DACL - ACEs
              ALLOW-S-1-520-1-0xf01ff
```

Maneiras de exibir informações sobre segurança de arquivos e diretivas de auditoria

Você pode usar o caractere curinga (*) para exibir informações sobre segurança de arquivos e políticas de auditoria de todos os arquivos e diretórios em um determinado caminho ou volume raiz.

O caractere curinga () **pode ser usado como o último subcomponente de um determinado caminho de diretório abaixo do qual você deseja exibir informações de todos os arquivos e diretórios. Se você quiser exibir informações de um arquivo ou diretório específico chamado ""**, então você precisa fornecer o caminho completo dentro de aspas duplas (""").

Exemplo

O comando a seguir com o caractere curinga exibe as informações sobre todos os arquivos e diretórios abaixo do caminho /1/ do SVM VS1:

```

cluster::> vserver security file-directory show -vserver vs1 -path /1/*

      Vserver: vs1
      File Path: /1/1
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8514
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

      Vserver: vs1
      File Path: /1/1/abc
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8404
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

```

O comando a seguir exibe as informações de um arquivo chamado "" no caminho /vol1/a do SVM VS1. O caminho está entre aspas duplas (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/voll/a/*"
```

```

    Vserver: vs1
    File Path: "/voll/a/*"
    Security Style: mixed
    Effective Style: unix
    DOS Attributes: 10
    DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
        Unix User Id: 1002
        Unix Group Id: 65533
        Unix Mode Bits: 755
    Unix Mode Bits in Text: rwxr-xr-x
        ACLs: NFSV4 Security Descriptor
            Control:0x8014
            SACL - ACEs
                AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
            DACL - ACEs
                ALLOW-EVERYONE@-0x1f00a9-FI|DI
                ALLOW-OWNER@-0x1f01ff-FI|DI
                ALLOW-GROUP@-0x1200a9-IG
```

Gerencie a segurança de arquivos NTFS, as políticas de auditoria NTFS e o Storage-Level Access Guard em SVMs usando a CLI

Gerencie a segurança de arquivos NTFS, as políticas de auditoria NTFS e o Storage-Level Access Guard em SVMs usando a visão geral da CLI

Você pode gerenciar a segurança de arquivos NTFS, políticas de auditoria NTFS e o Storage-Level Access Guard em máquinas virtuais de armazenamento (SVMs) usando a CLI.

Você pode gerenciar políticas de segurança e auditoria de arquivos NTFS de clientes SMB ou usando a CLI. No entanto, usar a CLI para configurar políticas de segurança e auditoria de arquivos remove a necessidade de usar um cliente remoto para gerenciar a segurança de arquivos. Usar a CLI pode reduzir significativamente o tempo necessário para aplicar a segurança em muitos arquivos e pastas usando um único comando.

Você pode configurar o Storage-Level Access Guard, que é outra camada de segurança aplicada pelo ONTAP aos volumes SVM. O Storage-Level Access Guard aplica-se a acessos de todos os protocolos nas ao objeto de armazenamento ao qual o Storage-Level Access Guard é aplicado.

O protetor de acesso no nível de storage pode ser configurado e gerenciado somente a partir da CLI do ONTAP. Não é possível gerenciar as configurações do protetor de acesso em nível de armazenamento de clientes SMB. Além disso, se você exibir as configurações de segurança em um arquivo ou diretório de um cliente NFS ou SMB, não verá a segurança Storage-Level Access Guard. A segurança do Access Guard no nível de armazenamento não pode ser revogada de um cliente, mesmo por um administrador do sistema (Windows ou UNIX). Portanto, o Storage-Level Access Guard fornece uma camada extra de segurança para o

acesso aos dados que é definido e gerenciado de forma independente pelo administrador do armazenamento.



Embora apenas as permissões de acesso NTFS sejam suportadas pelo Guarda de Acesso em nível de armazenamento, o ONTAP pode executar verificações de segurança para acesso através de NFS a dados em volumes em que o Guarda de Acesso em nível de armazenamento é aplicado se o utilizador do UNIX mapear para um utilizador do Windows na SVM que possui o volume.

Volumes de estilo de segurança NTFS

Todos os arquivos e pastas contidos em volumes e qtrees de estilo de segurança NTFS têm segurança efetiva NTFS. Você pode usar a `vserver security file-directory` família de comandos para implementar os seguintes tipos de segurança em volumes de estilo de segurança NTFS:

- Permissões de arquivo e políticas de auditoria para arquivos e pastas contidos no volume
- Segurança no nível de armazenamento de acesso Guarda em volumes

Volumes mistos de estilo de segurança

Volumes mistos de estilo de segurança e qtrees podem conter alguns arquivos e pastas que têm segurança efetiva UNIX e usam permissões de arquivos UNIX, bits de modo ou ACLs NFSv4.x e diretivas de auditoria NFSv4.x, e alguns arquivos e pastas que têm segurança efetiva NTFS e usam permissões de arquivos NTFS e políticas de auditoria. Você pode usar a `vserver security file-directory` família de comandos para aplicar os seguintes tipos de segurança a dados mistos de estilo de segurança:

- Permissões de arquivos e diretivas de auditoria para arquivos e pastas com o estilo de segurança eficaz NTFS no volume ou qtree misto
- Proteção de acesso no nível de armazenamento para volumes com o estilo de segurança eficaz NTFS e UNIX

Volumes de estilo de segurança UNIX

Os volumes e qtrees de estilo de segurança UNIX contêm arquivos e pastas que têm segurança efetiva UNIX (bits de modo ou ACLs NFSv4.x). Você deve ter em mente o seguinte se quiser usar a `vserver security file-directory` família de comandos para implementar a segurança em volumes estilo de segurança UNIX:

- A `vserver security file-directory` família de comandos não pode ser usada para gerenciar políticas de segurança e auditoria de arquivos UNIX em volumes e qtrees de estilo de segurança UNIX.
- Você pode usar a `vserver security file-directory` família de comandos para configurar o Storage-Level Access Guard em volumes de estilo de segurança UNIX, desde que o SVM com o volume de destino contenha um servidor CIFS.

Informações relacionadas

[Exibir informações sobre segurança de arquivos e diretivas de auditoria](#)

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

[Configure e aplique políticas de auditoria a arquivos e pastas NTFS usando a CLI](#)

[Proteja o acesso aos arquivos usando o Storage-Level Access Guard](#)

Use casos para usar a CLI para definir a segurança de arquivos e pastas

Como você pode aplicar e gerenciar a segurança de arquivos e pastas localmente sem envolvimento de um cliente remoto, você pode reduzir significativamente o tempo necessário para definir a segurança em massa em um grande número de arquivos ou pastas.

Você pode se beneficiar do uso da CLI para definir a segurança de arquivos e pastas nos seguintes casos de uso:

- Armazenamento de arquivos em grandes ambientes empresariais, como armazenamento de arquivos em diretórios base
- Migração de dados
- Mudança de domínio do Windows
- Padronização de políticas de segurança e auditoria de arquivos em sistemas de arquivos NTFS

Limites ao usar a CLI para definir a segurança de arquivos e pastas

Você precisa estar ciente de certos limites ao usar a CLI para definir a segurança de arquivos e pastas.

- A `vsserver security file-directory` família de comandos não suporta a configuração de ACLs NFSv4.

Você só pode aplicar descritores de segurança NTFS a arquivos e pastas NTFS.

Como os descritores de segurança são usados para aplicar a segurança de arquivos e pastas

Os descritores de segurança contêm as listas de controle de acesso que determinam quais ações um usuário pode executar em arquivos e pastas e o que é auditado quando um usuário acessa arquivos e pastas.

• Permissões

As permissões são permitidas ou negadas pelo proprietário de um objeto e determinam quais ações um objeto (usuários, grupos ou objetos de computador) pode executar em arquivos ou pastas especificados.

• Descritores de segurança

Descritores de segurança são estruturas de dados que contêm informações de segurança que definem permissões associadas a um arquivo ou pasta.

• Listas de controle de acesso (ACLs)

Listas de controle de acesso são as listas contidas em um descritor de segurança que contêm informações sobre quais ações os usuários, grupos ou objetos de computador podem executar no arquivo ou pasta à qual o descritor de segurança é aplicado. O descritor de segurança pode conter os dois tipos de ACLs a seguir:

- Listas de controle de acesso discricionárias (DACLS)
- Listas de controle de acesso do sistema (SACLs)

- **Listas de controle de acesso discricionárias (DACLS)**

As DACLS contêm a lista de SIDS para os usuários, grupos e objetos de computador que têm acesso permitido ou negado para executar ações em arquivos ou pastas. As DACLS contêm zero ou mais entradas de controle de acesso (ACEs).

- **Listas de controle de acesso do sistema (SACLs)**

Os SACLs contêm a lista de SIDS para os usuários, grupos e objetos de computador para os quais eventos de auditoria bem-sucedidos ou com falha são registrados. SACLs contêm zero ou mais entradas de controle de acesso (ACEs).

- **Entradas de Controle de Acesso (ACEs)**

Os ases são entradas individuais em DACLS ou SACLs:

- Uma entrada de controle de acesso DACL especifica os direitos de acesso que são permitidos ou negados para usuários, grupos ou objetos de computador específicos.
- Uma entrada de controle de acesso SACL especifica os eventos de sucesso ou falha a serem registrados ao auditar ações especificadas executadas por determinados usuários, grupos ou objetos de computador.

- * Herança de permissão*

A herança de permissões descreve como as permissões definidas em descritores de segurança são propagadas para um objeto de um objeto pai. Somente permissões herdáveis são herdadas por objetos filho. Ao definir permissões no objeto pai, você pode decidir se pastas, subpastas e arquivos podem herdá-los com ""aplicar a this-folder, sub-folders e 'arquivos'".

Informações relacionadas

["Auditoria de SMB e NFS e rastreamento de segurança"](#)

[Configurando e aplicando políticas de auditoria a arquivos e pastas NTFS usando a CLI](#)

Diretrizes para a aplicação de políticas de diretório de arquivos que usam usuários locais ou grupos no destino da recuperação de desastres do SVM

Há certas diretrizes que você deve ter em mente antes de aplicar políticas de diretório de arquivos no destino de recuperação de desastres de máquina virtual de armazenamento (SVM) em uma configuração de descarte de ID se a configuração de diretiva de diretório de arquivos usar usuários locais ou grupos no descritor de segurança ou nas entradas DACL ou SACL.

Você pode configurar uma configuração de recuperação de desastre para um SVM em que o SVM de origem no cluster de origem replique os dados e a configuração da SVM de origem a um SVM de destino em um cluster de destino.

É possível configurar um dos dois tipos de recuperação de desastres da SVM:

- Identidade preservada

Com essa configuração, a identidade do SVM e do servidor CIFS é preservada.

- Identidade descartada

Com essa configuração, a identidade do SVM e do servidor CIFS não é preservada. Nesse cenário, o nome do SVM e do servidor CIFS no SVM de destino são diferentes do SVM e do nome do servidor CIFS na SVM de origem.

Diretrizes para configurações de identidade descartadas

Em uma configuração de identidade descartada, para uma origem SVM que contenha configurações de usuário, grupo e privilégio locais, o nome do domínio local (nome do servidor CIFS local) deve ser alterado para corresponder ao nome do servidor CIFS no destino SVM. Por exemplo, se o nome do SVM de origem for "VS1" e o nome do servidor CIFS for "CIFS1 user1", e o nome do SVM de destino for "VS1 user1_dst" e o nome do servidor CIFS for "CIFS1_DST", então o nome de domínio local para um usuário local chamado "CIFS1" é alterado automaticamente para "CIFS1_DST" no destino:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst
```

Vserver	User Name	Full Name	Description
vs1	CIFS1\Administrator		Built-in
administrator	account		
vs1	CIFS1\user1	-	-

```
cluster1dst::> vserver cifs users-and-groups local-user show -vserver vs1_dst
```

Vserver	User Name	Full Name	Description
vs1_dst	CIFS1_DST\Administrator		Built-in
administrator	account		
vs1_dst	CIFS1_DST\user1	-	-

Mesmo que os nomes de usuários e grupos locais sejam alterados automaticamente nos bancos de dados de usuários e grupos locais, usuários locais ou nomes de grupos não são alterados automaticamente nas configurações de diretiva de diretório de arquivos (políticas configuradas na CLI usando a `vserver security file-directory` família de comandos).

Por exemplo, para "VS1", se você configurou uma entrada DACL onde o `-account` parâmetro é definido como "CIFS1 user1", a configuração não será alterada automaticamente no SVM de destino para refletir o nome do servidor CIFS de destino.

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1
```

```
Vserver: vs1
```

```
NTFS Security Descriptor Name: sdl
```

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
CIFS1\user1	allow	full-control	this-folder

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1_dst
```

```
Vserver: vs1_dst
```

```
NTFS Security Descriptor Name: sdl
```

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
CIFS1\user1		allow full-control	this-folder

Você deve usar os `vserver security file-directory modify` comandos para alterar manualmente o nome do servidor CIFS para o nome do servidor CIFS de destino.

Componentes de configuração de diretiva de diretório de arquivos que contêm parâmetros de conta

Há três componentes de configuração de diretiva de diretório de arquivos que podem usar configurações de parâmetros que podem conter usuários ou grupos locais:

- Descritor de segurança

Opcionalmente, você pode especificar o proprietário do descritor de segurança e o grupo principal do proprietário do descritor de segurança. Se o descritor de segurança usar um usuário ou grupo local para as entradas do proprietário e do grupo primário, você deverá modificar o descritor de segurança para usar o SVM de destino no nome da conta. Você pode usar o `vserver security file-directory ntfs modify` comando para fazer quaisquer alterações necessárias nos nomes de conta.

- Entradas DACL

Cada entrada DACL deve ser associada a uma conta. Você deve modificar quaisquer DACLs que usem contas de usuário ou grupo locais para usar o nome do SVM de destino. Como você não pode modificar o nome da conta para entradas DACL existentes, você deve remover quaisquer entradas DACL com usuários locais ou grupos dos descritores de segurança, criar novas entradas DACL com os nomes de conta de destino corrigidos e associar essas novas entradas DACL aos descritores de segurança apropriados.

- Entradas SACL

Cada entrada SACL deve ser associada a uma conta. Você deve modificar quaisquer SACLs que usem contas de usuário ou grupo locais para usar o nome do SVM de destino. Como você não pode modificar o

nome da conta para entradas SACL existentes, você deve remover quaisquer entradas SACL com usuários locais ou grupos dos descritores de segurança, criar novas entradas SACL com os nomes de conta de destino corrigidos e associar essas novas entradas SACL aos descritores de segurança apropriados.

Você deve fazer as alterações necessárias aos usuários locais ou grupos usados na configuração da diretiva de diretório de arquivos antes de aplicar a diretiva; caso contrário, a tarefa aplicar falha.

Configure e aplique segurança de arquivos em arquivos e pastas NTFS usando a CLI

Crie um descritor de segurança NTFS

Criar um descritor de segurança NTFS (política de segurança de arquivos) é a primeira etapa na configuração e aplicação de listas de controle de acesso (ACLs) NTFS a arquivos e pastas residentes em máquinas virtuais de armazenamento (SVMs). Você pode associar o descritor de segurança ao caminho do arquivo ou da pasta em uma tarefa de diretiva.

Sobre esta tarefa

Você pode criar descritores de segurança NTFS para arquivos e pastas que residem em volumes de estilo de segurança NTFS ou para arquivos e pastas que residem em volumes de estilo de segurança misto.

Por padrão, quando um descritor de segurança é criado, quatro entradas de controle de acesso (ACEs) da lista de controle de acesso discricionária (DACL) são adicionadas a esse descritor de segurança. Os quatro ACEs predefinidos são os seguintes:

Objeto	Tipo de acesso	Direitos de acesso	Onde aplicar as permissões
CRIAR/Administradores	Permitir	Controlo total	esta pasta, subpastas, ficheiros
CONSTRUIR/usuários	Permitir	Controlo total	esta pasta, subpastas, ficheiros
PROPRIETÁRIO DO CRIADOR	Permitir	Controlo total	esta pasta, subpastas, ficheiros
AUTORIDADE NT/SISTEMA	Permitir	Controlo total	esta pasta, subpastas, ficheiros

Você pode personalizar a configuração do descritor de segurança usando os seguintes parâmetros opcionais:

- Proprietário do descritor de segurança
- Grupo primário do proprietário
- Flags de controle bruto

O valor de qualquer parâmetro opcional é ignorado para o Storage-Level Access Guard. Consulte as páginas de manual para obter mais informações.

Adicione entradas de controle de acesso NTFS DACL ao descritor de segurança NTFS

Adicionar entradas de controle de acesso (ACEs) DACL (lista de controle de acesso discricionária) ao descritor de segurança NTFS é a segunda etapa na configuração e aplicação de ACLs NTFS a um arquivo ou pasta. Cada entrada identifica qual objeto é permitido ou negado acesso e define o que o objeto pode ou não pode fazer aos arquivos ou pastas definidos no ACE.

Sobre esta tarefa

Você pode adicionar um ou mais ACEs à DACL do descritor de segurança.

Se o descritor de segurança contiver uma DACL que tenha ACEs existentes, o comando adicionará o novo ACE à DACL. Se o descritor de segurança não contiver uma DACL, o comando criará a DACL e adicionará a nova ACE a ele.

Opcionalmente, você pode personalizar entradas DACL especificando quais direitos deseja permitir ou negar para a conta especificada no `-account` parâmetro. Existem três métodos mutuamente exclusivos para especificar direitos:

- Direitos
- Direitos avançados
- Direitos brutos (privilégio avançado)



Se você não especificar direitos para a entrada DACL, o padrão será definir os direitos como Full Control.

Opcionalmente, você pode personalizar entradas DACL especificando como aplicar herança.

O valor de qualquer parâmetro opcional é ignorado para o Storage-Level Access Guard. Consulte as páginas de manual para obter mais informações.

Passos

1. Adicione uma entrada DACL a um descritor de segurança: `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

```
vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
-account domain\joe -rights full-control -apply-to this-folder -vserver vs1
```

2. Verifique se a entrada DACL está correta: `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
-access-type deny -account domain\joe
```

```
Vserver: vs1
Security Descriptor Name: sd1
    Allow or Deny: deny
    Account Name or SID: DOMAIN\joe
    Access Rights: full-control
Advanced Access Rights: -
    Apply To: this-folder
    Access Rights: full-control
```

Crie políticas de segurança

Criar uma política de segurança de arquivos para SVMs é a terceira etapa na configuração e aplicação de ACLs a um arquivo ou pasta. Uma política atua como um contendor para várias tarefas, onde cada tarefa é uma única entrada que pode ser aplicada a arquivos ou pastas. Pode adicionar tarefas à política de segurança mais tarde.

Sobre esta tarefa

As tarefas que você adiciona a uma diretiva de segurança contêm associações entre o descritor de segurança NTFS e os caminhos de arquivo ou pasta. Portanto, você deve associar a política de segurança a cada SVM (contendo volumes de estilo de segurança NTFS ou volumes de estilo de segurança misto).

Passos

1. Criar uma política de segurança: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory policy create -policy-name policy1 -vserver vs1
```

2. Verifique a política de segurança: `vserver security file-directory policy show`

```
vserver security file-directory policy show
Vserver          Policy Name
-----          -
vs1              policy1
```

Adicione uma tarefa à política de segurança

Criar e adicionar uma tarefa de diretiva a uma diretiva de segurança é a quarta etapa na configuração e aplicação de ACLs a arquivos ou pastas em SVMs. Ao criar a tarefa de política, associe a tarefa a uma política de segurança. Você pode adicionar uma ou mais entradas de tarefa a uma diretiva de segurança.

Sobre esta tarefa

A política de segurança é um contendor para uma tarefa. Uma tarefa refere-se a uma única operação que pode ser feita por uma política de segurança para arquivos ou pastas com NTFS ou segurança mista (ou para

um objeto de volume se configurar o Storage-Level Access Guard).

Existem dois tipos de tarefas:

- Tarefas de arquivo e diretório

Usado para especificar tarefas que aplicam descritores de segurança a arquivos e pastas especificados. As ACLs aplicadas através de tarefas de arquivo e diretório podem ser gerenciadas com clientes SMB ou com a CLI do ONTAP.

- Tarefas do Access Guard no nível de storage

Usado para especificar tarefas que aplicam descritores de segurança do Storage-Level Access Guard a um volume especificado. As ACLs aplicadas por meio de tarefas de proteção de acesso no nível do storage podem ser gerenciadas somente por meio da CLI do ONTAP.

Uma tarefa contém definições para a configuração de segurança de um ficheiro (ou pasta) ou conjunto de ficheiros (ou pastas). Cada tarefa em uma política é identificada exclusivamente pelo caminho. Só pode haver uma tarefa por caminho dentro de uma única política. Uma política não pode ter entradas de tarefa duplicadas.

Diretrizes para adicionar uma tarefa a uma política:

- Pode haver um máximo de 10.000 entradas de tarefas por política.
- Uma política pode conter uma ou mais tarefas.

Mesmo que uma diretiva possa conter mais de uma tarefa, você não pode configurar uma diretiva para conter tarefas de diretório de arquivos e Guarda de Acesso em nível de armazenamento. Uma diretiva deve conter todas as tarefas do Guarda de Acesso no nível de armazenamento ou todas as tarefas do diretório de arquivos.

- O Access Guard no nível de storage é usado para restringir permissões.

Ele nunca dará permissões de acesso extra.

Ao adicionar tarefas a políticas de segurança, você deve especificar os quatro parâmetros necessários a seguir:

- Nome do SVM
- Nome da política
- Caminho
- Descritor de segurança para associar ao caminho

Você pode personalizar a configuração do descritor de segurança usando os seguintes parâmetros opcionais:

- Tipo de segurança
- Modo de propagação
- Posição do índice
- Tipo de controle de acesso

O valor de qualquer parâmetro opcional é ignorado para o Storage-Level Access Guard. Consulte as páginas

de manual para obter mais informações.

Passos

1. Adicione uma tarefa com um descritor de segurança associado à diretiva de segurança: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

`file-directory` é o valor padrão para o `-access-control` parâmetro. Especificar o tipo de controle de acesso ao configurar tarefas de acesso a arquivos e diretórios é opcional.

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
```

2. Verifique a configuração da tarefa de política: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

```
vserver security file-directory policy task show
```

```
Vserver: vs1
Policy: policy1

Index      File/Folder      Access          Security        NTFS           NTFS
Security
          Path            Control        Type            Mode
Descriptor Name
-----
1          /home/dir1      file-directory  ntfs            propagate      sd2
```

Aplicar políticas de segurança

Aplicar uma política de segurança de arquivos a SVMs é a última etapa na criação e aplicação de ACLs NTFS a arquivos ou pastas.

Sobre esta tarefa

Você pode aplicar as configurações de segurança definidas na diretiva de segurança a arquivos e pastas NTFS residentes em volumes FlexVol (NTFS ou estilo de segurança misto).



Quando uma política de auditoria e SACLs associados são aplicados, todas as DACLs existentes são substituídas. Quando uma diretiva de segurança e suas DACLs associadas são aplicadas, todas as DACLs existentes são substituídas. Você deve revisar as políticas de segurança existentes antes de criar e aplicar novas.

Passo

1. Aplicar uma política de segurança: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`


```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

O trabalho de aplicação de política está agendado e o Código trabalho é devolvido.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id 53322" command to view the status of the operation
```

Monitorize o trabalho de política de segurança

Ao aplicar a diretiva de segurança a máquinas virtuais de armazenamento (SVMs), você pode monitorar o progresso da tarefa monitorando a tarefa de diretiva de segurança. Isso é útil se você quiser verificar se a aplicação da diretiva de segurança foi bem-sucedida. Isso também é útil se você tiver um trabalho de longa duração onde você estiver aplicando segurança em massa a um grande número de arquivos e pastas.

Sobre esta tarefa

Para exibir informações detalhadas sobre um trabalho de política de segurança, use o `-instance` parâmetro.

Passo

1. Monitorar o trabalho de política de segurança: `vserver security file-directory job show -vserver vserver_name`

```
vserver security file-directory job show -vserver vs1
```

Job ID	Name	Vserver	Node	State
53322	Fsecurity Apply	vs1	node1	Success

Description: File Directory Security Apply Job

Verifique a segurança do arquivo aplicado

Você pode verificar as configurações de segurança do arquivo para confirmar se os arquivos ou pastas na máquina virtual de armazenamento (SVM) à qual você aplicou a diretiva de segurança têm as configurações desejadas.

Sobre esta tarefa

Você deve fornecer o nome do SVM que contém os dados e o caminho para o arquivo e pastas em que deseja verificar as configurações de segurança. Você pode usar o parâmetro opcional `-expand-mask` para exibir informações detalhadas sobre as configurações de segurança.

Passo

1. Exibir configurações de segurança de arquivos e pastas: `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

```
vserver security file-directory show -vserver vs1 -path /data/engineering -expand-mask true
```

```

Vserver: vs1
    File Path: /data/engineering
File Inode Number: 5544
    Security Style: ntfs
    Effective Style: ntfs
    DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ...0 .... = Offline
    .... ..0. .... = Sparse
    .... .... 0... .... = Normal
    .... .... ..0. .... = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
    Control:0x8004

    1... .... = Self Relative
    .0.. .... = RM Control Valid
    ..0. .... = SACL Protected
    ...0 .... = DACL Protected
    .... 0... .... = SACL Inherited
    .... .0.. .... = DACL Inherited
    .... ..0. .... = SACL Inherit Required
    .... ...0 .... = DACL Inherit Required
    .... .... ..0. .... = SACL Defaulted
    .... .... ...0 .... = SACL Present
    .... .... .... 0... = DACL Defaulted
    .... .... .... .1.. = DACL Present
    .... .... .... ..0. = Group Defaulted
    .... .... .... ...0 = Owner Defaulted

Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs
    ALLOW-Everyone-0x1f01ff
    0... .... =
Generic Read
    .0.. .... =

```

```

Generic Write          ..0. .... =
Generic Execute       ...0 .... =
Generic All           .....0 .... =
System Security       .....1 .... =
Synchronize          ..... 1... =
Write Owner           ..... 1.. =
Write DAC             ..... 1. =
Read Control         ..... 1 .... =
Delete               ..... 1 .... =
Write Attributes     ..... 1... =
Read Attributes      ..... 1.. =
Delete Child         ..... 1. .... =
Execute              ..... 1 .... =
Write EA             ..... 1... =
Read EA              ..... 1.. =
Append               ..... 1. =
Write                ..... 1 =
Read                 ..... 1 =

ALLOW-Everyone-0x10000000-OI|CI|IO
Generic Read         0... .... =
Generic Write       .0.. .... =
Generic Execute     ..0. .... =
Generic All         ...1 .... =
Generic All         .....0 .... =

```

```

System Security
.....0..... =
Synchronize
.....0..... =
Write Owner
.....0..... =
Write DAC
.....0..... =
Read Control
.....0..... =
Delete
.....0..... =
Write Attributes
.....0..... =
Read Attributes
.....0..... =
Delete Child
.....0..... =
Execute
.....0..... =
Write EA
.....0..... =
Read EA
.....0..... =
Append
.....0..... =
Write
.....0..... =
Read
.....0..... =

```

Configure e aplique políticas de auditoria a arquivos e pastas NTFS usando a CLI

Configure e aplique políticas de auditoria a arquivos e pastas NTFS usando a visão geral da CLI

Existem várias etapas que você deve executar para aplicar políticas de auditoria a arquivos e pastas NTFS ao usar a CLI do ONTAP. Primeiro, você cria um descritor de segurança NTFS e adiciona SACLs ao descritor de segurança. Em seguida, você cria uma política de segurança e adiciona tarefas de política. Em seguida, você aplica a política de segurança a uma máquina virtual de storage (SVM).

Sobre esta tarefa

Depois de aplicar a política de segurança, pode monitorizar o trabalho de política de segurança e, em seguida, verificar as definições da política de auditoria aplicada.



Quando uma política de auditoria e SACLs associados são aplicados, todas as DACLS existentes são substituídas. Você deve revisar as políticas de segurança existentes antes de criar e aplicar novas.

Informações relacionadas

[Protegendo o acesso aos arquivos usando o Storage-Level Access Guard](#)

[Limites ao usar a CLI para definir a segurança de arquivos e pastas](#)

[Como os descritores de segurança são usados para aplicar a segurança de arquivos e pastas](#)

["Auditoria de SMB e NFS e rastreamento de segurança"](#)

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

Crie um descritor de segurança NTFS

Criar uma política de auditoria do descritor de segurança NTFS é a primeira etapa na configuração e aplicação de listas de controle de acesso (ACLs) NTFS a arquivos e pastas residentes em SVMs. Você associará o descritor de segurança ao caminho do arquivo ou da pasta em uma tarefa de diretiva.

Sobre esta tarefa

Você pode criar descritores de segurança NTFS para arquivos e pastas que residem em volumes de estilo de segurança NTFS ou para arquivos e pastas que residem em volumes de estilo de segurança misto.

Por padrão, quando um descritor de segurança é criado, quatro entradas de controle de acesso (ACEs) da lista de controle de acesso discricionária (DACL) são adicionadas a esse descritor de segurança. Os quatro ACEs predefinidos são os seguintes:

Objeto	Tipo de acesso	Direitos de acesso	Onde aplicar as permissões
CRIAR/Administradores	Permitir	Controlo total	esta pasta, subpastas, ficheiros
CONSTRUIR/usuários	Permitir	Controlo total	esta pasta, subpastas, ficheiros
PROPRIETÁRIO DO CRIADOR	Permitir	Controlo total	esta pasta, subpastas, ficheiros
AUTORIDADE NT/SISTEMA	Permitir	Controlo total	esta pasta, subpastas, ficheiros

Você pode personalizar a configuração do descritor de segurança usando os seguintes parâmetros opcionais:

- Proprietário do descritor de segurança
- Grupo primário do proprietário
- Flags de controle bruto

O valor de qualquer parâmetro opcional é ignorado para o Storage-Level Access Guard. Consulte as páginas de manual para obter mais informações.

Passos

1. Se pretender utilizar os parâmetros avançados, defina o nível de privilégio para avançado: `set -privilege advanced`
2. Criar um descritor de segurança: `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

```
vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe
```

3. Verifique se a configuração do descritor de segurança está correta: `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

```
vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
Security Descriptor Name: sd1
Owner of the Security Descriptor: DOMAIN\joe
```

4. Se estiver no nível de privilégio avançado, regresse ao nível de privilégio admin: `set -privilege admin`

Adicione entradas de controle de acesso NTFS SACL ao descritor de segurança NTFS

Adicionar entradas de controle de acesso (ACEs) SACL (lista de controle de acesso do sistema) ao descritor de segurança NTFS é a segunda etapa na criação de políticas de auditoria NTFS para arquivos ou pastas em SVMs. Cada entrada identifica o usuário ou grupo que você deseja auditar. A entrada SACL define se você deseja auditar tentativas de acesso bem-sucedidas ou com falha.

Sobre esta tarefa

Você pode adicionar um ou mais ACEs ao SACL do descritor de segurança.

Se o descritor de segurança contiver um SACL que tenha ACEs existentes, o comando adicionará o novo ACE ao SACL. Se o descritor de segurança não contiver um SACL, o comando criará o SACL e adicionará o novo ACE a ele.

Você pode configurar entradas SACL especificando quais direitos deseja auditar para eventos de sucesso ou falha para a conta especificada no `-account` parâmetro. Existem três métodos mutuamente exclusivos para especificar direitos:

- Direitos
- Direitos avançados
- Direitos brutos (privilégio avançado)



Se não especificar direitos para a entrada SACL, a predefinição é Full Control.

Opcionalmente, você pode personalizar entradas SACL especificando como aplicar herança com o `apply to` parâmetro. Se você não especificar esse parâmetro, o padrão é aplicar essa entrada SACL a essa pasta, subpastas e arquivos.

Passos

1. Adicione uma entrada SACL a um descritor de segurança: `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

```
vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type failure -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
```

2. Verifique se a entrada SACL está correta: `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

```
vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1 -access-type deny -account domain\joe
```

```
Vserver: vs1
Security Descriptor Name: sd1
Access type for Specified Access Rights: failure
Account Name or SID: DOMAIN\joe
Access Rights: full-control
Advanced Access Rights: -
Apply To: this-folder
Access Rights: full-control
```

Crie políticas de segurança

Criar uma política de auditoria para máquinas virtuais de armazenamento (SVMs) é a terceira etapa na configuração e aplicação de ACLs a um arquivo ou pasta. Uma política atua como um contentor para várias tarefas, onde cada tarefa é uma única entrada que pode ser aplicada a arquivos ou pastas. Pode adicionar tarefas à política de segurança mais tarde.

Sobre esta tarefa

As tarefas que você adiciona a uma diretiva de segurança contêm associações entre o descritor de segurança NTFS e os caminhos de arquivo ou pasta. Portanto, você deve associar a política de segurança a cada máquina virtual de armazenamento (SVM) (contendo volumes de estilo de segurança NTFS ou volumes mistos de estilo de segurança).

Passos

1. Criar uma política de segurança: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory policy create -policy-name policy1 -vserver vs1
```

2. Verifique a política de segurança: `vserver security file-directory policy show`

```
vserver security file-directory policy show
Vserver          Policy Name
-----          -
vs1              policy1
```

Adicione uma tarefa à política de segurança

Criar e adicionar uma tarefa de diretiva a uma diretiva de segurança é a quarta etapa na configuração e aplicação de ACLs a arquivos ou pastas em SVMs. Ao criar a tarefa de política, associe a tarefa a uma política de segurança. Você pode adicionar uma ou mais entradas de tarefa a uma diretiva de segurança.

Sobre esta tarefa

A política de segurança é um contendor para uma tarefa. Uma tarefa refere-se a uma única operação que pode ser feita por uma política de segurança para arquivos ou pastas com NTFS ou segurança mista (ou para um objeto de volume se configurar o Storage-Level Access Guard).

Existem dois tipos de tarefas:

- Tarefas de arquivo e diretório

Usado para especificar tarefas que aplicam descritores de segurança a arquivos e pastas especificados. As ACLs aplicadas através de tarefas de arquivo e diretório podem ser gerenciadas com clientes SMB ou com a CLI do ONTAP.

- Tarefas do Access Guard no nível de storage

Usado para especificar tarefas que aplicam descritores de segurança do Storage-Level Access Guard a um volume especificado. As ACLs aplicadas por meio de tarefas de proteção de acesso no nível de storage podem ser gerenciadas somente por meio da CLI do ONTAP.

Uma tarefa contém definições para a configuração de segurança de um ficheiro (ou pasta) ou conjunto de ficheiros (ou pastas). Cada tarefa em uma política é identificada exclusivamente pelo caminho. Só pode haver uma tarefa por caminho dentro de uma única política. Uma política não pode ter entradas de tarefa duplicadas.

Diretrizes para adicionar uma tarefa a uma política:

- Pode haver um máximo de 10.000 entradas de tarefas por política.
- Uma política pode conter uma ou mais tarefas.

Mesmo que uma diretiva possa conter mais de uma tarefa, você não pode configurar uma diretiva para conter tarefas de diretório de arquivos e Guarda de Acesso em nível de armazenamento. Uma diretiva deve conter todas as tarefas do Guarda de Acesso no nível de armazenamento ou todas as tarefas do diretório de arquivos.

- O Access Guard no nível de storage é usado para restringir permissões.

Ele nunca dará permissões de acesso extra.

Você pode personalizar a configuração do descritor de segurança usando os seguintes parâmetros opcionais:

- Tipo de segurança
- Modo de propagação
- Posição do índice
- Tipo de controle de acesso

O valor de qualquer parâmetro opcional é ignorado para o Storage-Level Access Guard. Consulte as páginas de manual para obter mais informações.

Passos

1. Adicione uma tarefa com um descritor de segurança associado à diretiva de segurança: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

`file-directory` é o valor padrão para o `-access-control` parâmetro. Especificar o tipo de controle de acesso ao configurar tarefas de acesso a arquivos e diretórios é opcional.

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
```

2. Verifique a configuração da tarefa de política: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

```
vserver security file-directory policy task show
```

```
Vserver: vs1
Policy: policy1

Index      File/Folder      Access      Security      NTFS      NTFS
Security
          Path          Control      Type          Mode
Descriptor Name
-----
-----
1          /home/dir1      file-directory  ntfs          propagate  sd2
```

Aplicar políticas de segurança

Aplicar uma política de auditoria a SVMs é a última etapa na criação e aplicação de ACLs NTFS a arquivos ou pastas.

Sobre esta tarefa

Você pode aplicar as configurações de segurança definidas na diretiva de segurança a arquivos e pastas NTFS residentes em volumes FlexVol (NTFS ou estilo de segurança misto).



Quando uma política de auditoria e SACLs associados são aplicados, todas as DACLS existentes são substituídas. Quando uma diretiva de segurança e suas DACLS associadas são aplicadas, todas as DACLS existentes são substituídas. Você deve revisar as políticas de segurança existentes antes de criar e aplicar novas.

Passo

1. Aplicar uma política de segurança: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

O trabalho de aplicação de política está agendado e o Código trabalho é devolvido.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id 53322" command to view the status of the operation
```

Monitorize o trabalho de política de segurança

Ao aplicar a diretiva de segurança a máquinas virtuais de armazenamento (SVMs), você pode monitorar o progresso da tarefa monitorando a tarefa de diretiva de segurança. Isso é útil se você quiser verificar se a aplicação da diretiva de segurança foi bem-sucedida. Isso também é útil se você tiver um trabalho de longa duração onde você estiver aplicando segurança em massa a um grande número de arquivos e pastas.

Sobre esta tarefa

Para exibir informações detalhadas sobre um trabalho de política de segurança, use o `-instance` parâmetro.

Passo

1. Monitorar o trabalho de política de segurança: `vserver security file-directory job show -vserver vserver_name`

```
vserver security file-directory job show -vserver vs1
```

Job ID	Name	Vserver	Node	State
53322	Fsecurity Apply	vs1	node1	Success
Description: File Directory Security Apply Job				

Verifique a política de auditoria aplicada

Você pode verificar a política de auditoria para confirmar se os arquivos ou pastas na máquina virtual de armazenamento (SVM) à qual você aplicou a diretiva de segurança têm as configurações de segurança de auditoria desejadas.

Sobre esta tarefa

Você usa o `vserver security file-directory show` comando para exibir informações da política de auditoria. Você deve fornecer o nome do SVM que contém os dados e o caminho para os dados cujas informações de política de auditoria de arquivo ou pasta você deseja exibir.

Passo

1. Exibir configurações da política de auditoria: `vserver security file-directory show -vserver vserver_name -path path`

Exemplo

O comando a seguir exibe as informações da política de auditoria aplicadas ao caminho `"/corp"` no SVM `VS1`. O caminho tem um SUCESSO e uma entrada SACL DE SUCESSO/FALHA aplicada a ele:

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

      Vserver: vs1
      File Path: /corp
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8014
            Owner:DOMAIN\Administrator
            Group:BUILTIN\Administrators
      SACL - ACEs
            ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
            SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
      DACL - ACEs
            ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
            ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
            ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Considerações ao gerenciar trabalhos de diretiva de segurança

Se existir um trabalho de política de segurança, em determinadas circunstâncias, não é possível modificar essa política de segurança ou as tarefas atribuídas a essa diretiva. Você deve entender em que condições você pode ou não pode modificar políticas de segurança para que quaisquer tentativas que você fizer para modificar a diretiva sejam bem-sucedidas. As modificações à política incluem adicionar, remover ou modificar

tarefas atribuídas à política e excluir ou modificar a política.

Não é possível modificar uma política de segurança ou uma tarefa atribuída a essa política se existir um trabalho para essa política e essa tarefa estiver nos seguintes estados:

- O trabalho está em execução ou em curso.
- O trabalho está em pausa.
- O trabalho é retomado e está no estado em execução.
- Se a tarefa estiver aguardando o failover para outro nó.

Nas seguintes circunstâncias, se existir um trabalho para uma política de segurança, pode modificar com êxito essa política de segurança ou uma tarefa atribuída a essa política:

- O trabalho de política é interrompido.
- O trabalho de política foi concluído com êxito.

Comandos para gerenciar descritores de segurança NTFS

Existem comandos ONTAP específicos para gerenciar descritores de segurança. Você pode criar, modificar, excluir e exibir informações sobre descritores de segurança.

Se você quiser...	Use este comando...
Crie descritores de segurança NTFS	<code>vserver security file-directory ntfs create</code>
Modificar descritores de segurança NTFS existentes	<code>vserver security file-directory ntfs modify</code>
Exibir informações sobre descritores de segurança NTFS existentes	<code>vserver security file-directory ntfs show</code>
Excluir descritores de segurança NTFS	<code>vserver security file-directory ntfs delete</code>

Consulte as páginas de manual para `vserver security file-directory ntfs` obter mais informações.

Comandos para gerenciar entradas de controle de acesso NTFS DACL

Existem comandos ONTAP específicos para gerenciar entradas de controle de acesso DACL (ACEs). Você pode adicionar ACEs a DACLs NTFS a qualquer momento. Você também pode gerenciar DACLs NTFS existentes modificando, excluindo e exibindo informações sobre ACEs em DACLs.

Se você quiser...	Use este comando...
Crie ACEs e adicione-os a DACLs NTFS	<code>vserver security file-directory ntfs dacl add</code>
Modificar ACEs existentes em DACLs NTFS	<code>vserver security file-directory ntfs dacl modify</code>
Exibir informações sobre ACEs existentes em DACLs NTFS	<code>vserver security file-directory ntfs dacl show</code>
Remover ACEs existentes de DACLs NTFS	<code>vserver security file-directory ntfs dacl remove</code>

Consulte as páginas de manual para `vserver security file-directory ntfs dacl` obter mais informações.

Comandos para gerenciar entradas de controle de acesso NTFS SACL

Existem comandos ONTAP específicos para gerenciar entradas de controle de acesso SACL (ACEs). Você pode adicionar ACEs a SACLs NTFS a qualquer momento. Você também pode gerenciar SACLs NTFS existentes modificando, excluindo e exibindo informações sobre ACEs em SACLs.

Se você quiser...	Use este comando...
Crie ACEs e adicione-os a SACLs NTFS	<code>vserver security file-directory ntfs sacl add</code>
Modificar ACEs existentes em SACLs NTFS	<code>vserver security file-directory ntfs sacl modify</code>
Exibir informações sobre ACEs existentes em SACLs NTFS	<code>vserver security file-directory ntfs sacl show</code>
Remover ACEs existentes de SACLs NTFS	<code>vserver security file-directory ntfs sacl remove</code>

Consulte as páginas de manual para `vserver security file-directory ntfs sacl` obter mais informações.

Comandos para gerenciar políticas de segurança

Existem comandos ONTAP específicos para gerenciar políticas de segurança. Você pode exibir informações sobre políticas e excluir políticas. Não é possível modificar uma política de segurança.

Se você quiser...	Use este comando...
Crie políticas de segurança	<code>vserver security file-directory policy create</code>
Exibir informações sobre políticas de segurança	<code>vserver security file-directory policy show</code>
Eliminar políticas de segurança	<code>vserver security file-directory policy delete</code>

Consulte as páginas de manual para `vserver security file-directory policy` obter mais informações.

Comandos para gerenciar tarefas de diretiva de segurança

Existem comandos ONTAP para adicionar, modificar, remover e exibir informações sobre tarefas de diretiva de segurança.

Se você quiser...	Use este comando...
Adicione tarefas de política de segurança	<code>vserver security file-directory policy task add</code>
Modificar tarefas de política de segurança	<code>vserver security file-directory policy task modify</code>
Exibir informações sobre as tarefas da diretiva de segurança	<code>vserver security file-directory policy task show</code>
Remover tarefas de política de segurança	<code>vserver security file-directory policy task remove</code>

Consulte as páginas de manual para `vserver security file-directory policy task` obter mais informações.

Comandos para gerenciar trabalhos de diretiva de segurança

Existem comandos ONTAP para pausar, retomar, parar e exibir informações sobre tarefas de diretiva de segurança.

Se você quiser...	Use este comando...
Pausar trabalhos de diretiva de segurança	<code>vserver security file-directory job pause -vserver vserver_name -id integer</code>

Se você quiser...	Use este comando...
Retomar os trabalhos de política de segurança	<code>vserver security file-directory job resume -vserver vserver_name -id integer</code>
Exibir informações sobre os trabalhos de diretiva de segurança	<code>vserver security file-directory job show -vserver vserver_name</code> Pode determinar a ID da tarefa de uma tarefa utilizando este comando.
Interromper trabalhos de política de segurança	<code>vserver security file-directory job stop -vserver vserver_name -id integer</code>

Consulte as páginas de manual para `vserver security file-directory job` obter mais informações.

Configure o cache de metadados para compartilhamentos SMB

Como o armazenamento em cache de metadados SMB funciona

O armazenamento em cache de metadados permite o armazenamento em cache de atributos de arquivo em clientes SMB 1,0 para fornecer acesso mais rápido aos atributos de arquivo e pasta. Você pode ativar ou desativar o cache de atributos por compartilhamento. Você também pode configurar o tempo de permanência para entradas em cache se o armazenamento em cache de metadados estiver habilitado. A configuração do cache de metadados não é necessária se os clientes estiverem se conectando a compartilhamentos por SMB 2.x ou SMB 3,0.

Quando ativado, o cache de metadados SMB armazena dados de caminho e atributo de arquivo por um período limitado de tempo. Isso pode melhorar a performance do SMB para clientes SMB 1,0 com workloads comuns.

Para certas tarefas, o SMB cria uma quantidade significativa de tráfego que pode incluir várias consultas idênticas para metadados de caminho e arquivo. Você pode reduzir o número de consultas redundantes e melhorar o desempenho para clientes SMB 1,0 usando o cache de metadados SMB para buscar informações do cache.



Embora improvável, é possível que o cache de metadados possa servir informações obsoletas para clientes SMB 1,0. Se o seu ambiente não puder suportar esse risco, você não deve habilitar esse recurso.

Ative o cache de metadados SMB

Você pode melhorar o desempenho do SMB para clientes SMB 1,0 ativando o cache de metadados SMB. Por padrão, o armazenamento em cache de metadados SMB está desativado.

Passo

1. Execute a ação desejada:

Se você quiser...	Digite o comando...
Ative o armazenamento em cache de metadados SMB ao criar um compartilhamento	<code>vserver cifs share create -vserver <i>vserver_name</i> -share-name <i>share_name</i> -path <i>path</i> -share-properties attributecache</code>
Habilite o armazenamento em cache de metadados SMB em um compartilhamento existente	<code>vserver cifs share properties add -vserver <i>vserver_name</i> -share-name <i>share_name</i> -share-properties attributecache</code>

Informações relacionadas

[Configurando o tempo de vida das entradas de cache de metadados SMB](#)

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

Configure o tempo de vida das entradas de cache de metadados SMB

Você pode configurar o tempo de vida das entradas de cache de metadados SMB para otimizar o desempenho do cache de metadados SMB em seu ambiente. O padrão é 10 segundos.

Antes de começar

Você deve ter habilitado o recurso de cache de metadados SMB. Se o armazenamento em cache de metadados SMB não estiver ativado, a configuração TTL de cache SMB não será usada.

Passo

1. Execute a ação desejada:

Se você quiser configurar o tempo de vida das entradas de cache de metadados SMB quando...	Digite o comando...
Crie um compartilhamento	<code>vserver cifs share -create -vserver <i>vserver_name</i> -share-name <i>share_name</i> -path <i>path</i> -attribute-cache-ttl [<i>integerh</i>][<i>integerm</i>][<i>integers</i>]</code>
Modificar um compartilhamento existente	<code>vserver cifs share -modify -vserver <i>vserver_name</i> -share-name <i>share_name</i> -attribute-cache-ttl [<i>integerh</i>][<i>integerm</i>][<i>integers</i>]</code>

Você pode especificar opções e propriedades de configuração de compartilhamento adicionais ao criar ou modificar compartilhamentos. Consulte as páginas de manual para obter mais informações.

Gerenciar bloqueios de arquivos

Acerca do bloqueio de ficheiros entre protocolos

Bloqueio de arquivos é um método usado por aplicativos cliente para impedir que um usuário acesse um arquivo aberto anteriormente por outro usuário. A forma como o ONTAP bloqueia ficheiros depende do protocolo do cliente.

Se o cliente for um cliente NFS, os bloqueios são consultivos; se o cliente for um cliente SMB, os bloqueios são obrigatórios.

Devido às diferenças entre os bloqueios de arquivos NFS e SMB, um cliente NFS pode não conseguir acessar um arquivo aberto anteriormente por um aplicativo SMB.

O seguinte ocorre quando um cliente NFS tenta aceder a um ficheiro bloqueado por uma aplicação SMB:

- Em volumes mistos ou NTFS, operações de manipulação de arquivos como `rm`, `rmdir` e `mv` podem causar falha no aplicativo NFS.
- As operações de leitura e gravação NFS são negadas pelos modos abertos SMB `deny-read` e `deny-write`, respetivamente.
- As operações de gravação NFS falham quando o intervalo escrito do arquivo é bloqueado com um `bytelock` SMB exclusivo.

- Desvincular

- Para sistemas de arquivos NTFS, as operações de exclusão SMB e CIFS são suportadas.

O arquivo será removido após o último fechamento.

- As operações de desvinculação NFS não são suportadas.

Ele não é suportado porque as semânticas NTFS e SMB são necessárias e a última operação `Excluir-em-close` não é suportada para NFS.

- Para sistemas de arquivos UNIX, a operação de desvinculação é suportada.

Ele é compatível porque a semântica NFS e UNIX são necessárias.

- Mudar o nome

- Para sistemas de arquivos NTFS, se o arquivo de destino for aberto a partir de SMB ou CIFS, o arquivo de destino pode ser renomeado.
- O nome de NFS não é suportado.

Não é suportado porque as semânticas NTFS e SMB são necessárias.

Em volumes de estilo de segurança UNIX, as operações NFS desvincular e renomear ignoram o estado de bloqueio SMB e permitem o acesso ao arquivo. Todas as outras operações NFS em volumes estilo segurança UNIX honram o estado de bloqueio SMB.

Como o ONTAP trata bits somente de leitura

O bit somente leitura é definido em uma base arquivo por arquivo para refletir se um arquivo é gravável (desativado) ou somente leitura (habilitado).

Os clientes SMB que usam o Windows podem definir um bit somente leitura por arquivo. Os clientes NFS não definem um bit somente leitura por arquivo porque os clientes NFS não têm operações de protocolo que usam um bit somente leitura por arquivo.

O ONTAP pode definir um bit somente leitura em um arquivo quando um cliente SMB que usa o Windows cria esse arquivo. O ONTAP também pode definir um bit somente leitura quando um arquivo é compartilhado entre clientes NFS e clientes SMB. Alguns softwares, quando usados por clientes NFS e clientes SMB, exigem que o bit somente leitura seja ativado.

Para que o ONTAP mantenha as permissões de leitura e gravação apropriadas em um arquivo compartilhado entre clientes NFS e clientes SMB, ele trata o bit somente leitura de acordo com as seguintes regras:

- O NFS trata qualquer arquivo com o bit somente leitura ativado como se ele não tivesse bits de permissão de gravação ativados.
- Se um cliente NFS desativar todos os bits de permissão de gravação e pelo menos um desses bits tiver sido ativado anteriormente, o ONTAP ativa o bit somente leitura para esse arquivo.
- Se um cliente NFS ativar qualquer bit de permissão de gravação, o ONTAP desativa o bit somente leitura para esse arquivo.
- Se o bit somente leitura de um arquivo estiver ativado e um cliente NFS tentar descobrir permissões para o arquivo, os bits de permissão para o arquivo não serão enviados para o cliente NFS; em vez disso, o ONTAP enviará os bits de permissão para o cliente NFS com os bits de permissão de gravação mascarados.
- Se o bit somente leitura de um arquivo estiver ativado e um cliente SMB desabilitar o bit somente leitura, o ONTAP ativa o bit de permissão de gravação do proprietário para o arquivo.
- Os arquivos com o bit somente leitura habilitado são graváveis somente pelo root.



As alterações às permissões de arquivo entram em vigor imediatamente em clientes SMB, mas podem não ter efeito imediatamente em clientes NFS se o cliente NFS ativar o armazenamento em cache de atributos.

Como o ONTAP difere do Windows ao lidar com bloqueios em componentes de caminho de compartilhamento

Ao contrário do Windows, o ONTAP não bloqueia cada componente do caminho para um arquivo aberto enquanto o arquivo está aberto. Esse comportamento também afeta os caminhos de compartilhamento SMB.

Como o ONTAP não bloqueia cada componente do caminho, é possível renomear um componente do caminho acima do arquivo aberto ou do compartilhamento, o que pode causar problemas para determinados aplicativos ou fazer com que o caminho de compartilhamento na configuração do SMB seja inválido. Isso pode fazer com que o compartilhamento seja inacessível.

Para evitar problemas causados pela renomeação de componentes de caminho, você pode aplicar configurações de segurança que impedem que usuários ou aplicativos renomeem diretórios críticos.

Apresentar informações sobre bloqueios

Você pode exibir informações sobre os bloqueios de arquivo atuais, incluindo quais tipos de bloqueios são mantidos e qual é o estado de bloqueio, detalhes sobre bloqueios de intervalo de bytes, modos de sharelock, bloqueios de delegação e bloqueios

oportunistas, e se os bloqueios são abertos com alças duráveis ou persistentes.

Sobre esta tarefa

O endereço IP do cliente não pode ser exibido para bloqueios estabelecidos através de NFSv4 ou NFSv4.1.

Por padrão, o comando exibe informações sobre todos os bloqueios. Você pode usar parâmetros de comando para exibir informações sobre bloqueios de uma máquina virtual de armazenamento específica (SVM) ou para filtrar a saída do comando por outros critérios.

O `vserver locks show` comando exibe informações sobre quatro tipos de bloqueios:

- Bloqueios de intervalo de bytes, que bloqueiam apenas uma parte de um arquivo.
- Bloqueios de compartilhamento, que bloqueiam arquivos abertos.
- Bloqueios oportunistas, que controlam o cache do lado do cliente sobre SMB.
- Delegações, que controlam o cache do lado do cliente sobre NFSv4.x.

Ao especificar parâmetros opcionais, você pode determinar informações importantes sobre cada tipo de bloqueio. Consulte a página de manual para obter mais informações.

Passo

1. Exiba informações sobre bloqueios usando o `vserver locks show` comando.

Exemplos

O exemplo a seguir exibe informações de resumo de um bloqueio NFSv4 em um arquivo com o `/vol1/file1` caminho. O modo de acesso sharelock é `write-deny_none`, e o bloqueio foi concedido com delegação de gravação:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path                LIF          Protocol  Lock Type  Client
-----
-----
vol1    /vol1/file1                    lif1         nfsv4     share-level -
                Sharelock Mode: write-deny_none
                delegation -
                Delegation Type: write
```

O exemplo a seguir exibe informações detalhadas de oplock e sharelock sobre o bloqueio SMB em um arquivo com o `/data2/data2_2/intro.pptx` caminho. Um manipulador durável é concedido no arquivo com um modo de acesso de bloqueio de compartilhamento de `write-deny_none` para um cliente com um endereço IP de 10,3.1,3. Uma locação de oplock é concedida com um nível de lote de oplock:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

Vserver: vs1
Volume: data2_2
```

```
Logical Interface: lif2
    Object Path: /data2/data2_2/intro.pptx
    Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
    Lock Protocol: cifs
    Lock Type: share-level
Node Holding Lock State: node3
    Lock State: granted
Bytelock Starting Offset: -
    Number of Bytes Locked: -
    Bytelock is Mandatory: -
    Bytelock is Exclusive: -
    Bytelock is Superlock: -
    Bytelock is Soft: -
    Oplock Level: -
Shared Lock Access Mode: write-deny_none
    Shared Lock is Soft: false
    Delegation Type: -
    Client Address: 10.3.1.3
    SMB Open Type: durable
    SMB Connect State: connected
SMB Expiration Time (Secs): -
    SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

    Vserver: vs1
    Volume: data2_2
Logical Interface: lif2
    Object Path: /data2/data2_2/test.pptx
    Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
    Lock Protocol: cifs
    Lock Type: op-lock
Node Holding Lock State: node3
    Lock State: granted
Bytelock Starting Offset: -
    Number of Bytes Locked: -
    Bytelock is Mandatory: -
    Bytelock is Exclusive: -
    Bytelock is Superlock: -
    Bytelock is Soft: -
    Oplock Level: batch
Shared Lock Access Mode: -
    Shared Lock is Soft: -
    Delegation Type: -
    Client Address: 10.3.1.3
    SMB Open Type: -
    SMB Connect State: connected
```

```
SMB Expiration Time (Secs): -
      SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Bloqueios de rutura

Quando os bloqueios de arquivos estão impedindo o acesso do cliente aos arquivos, você pode exibir informações sobre os bloqueios atualmente mantidos e, em seguida, quebrar bloqueios específicos. Exemplos de cenários em que você pode precisar quebrar bloqueios incluem depuração de aplicativos.

Sobre esta tarefa

O `vserver locks break` comando está disponível apenas no nível de privilégio avançado e superior. A página de manual do comando contém informações detalhadas.

Passos

1. Para encontrar as informações que você precisa para quebrar um bloqueio, use o `vserver locks show` comando.

A página de manual do comando contém informações detalhadas.

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

Se você quiser quebrar um bloqueio especificando...	Digite o comando...
O nome do SVM, o nome do volume, o nome LIF e o caminho do arquivo	<code>vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif</code>
A ID de bloqueio	<code>vserver locks break -lockid UUID</code>

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

Monitorar a atividade de SMB

Exibir informações de sessão SMB

Você pode exibir informações sobre sessões SMB estabelecidas, incluindo a conexão SMB e Session ID e o endereço IP da estação de trabalho usando a sessão. Você pode exibir informações sobre a versão do protocolo SMB da sessão e o nível de proteção continuamente disponível, o que ajuda a identificar se a sessão é compatível com operações ininterruptas.

Sobre esta tarefa

É possível exibir informações de todas as sessões no SVM no formulário de resumo. No entanto, em muitos casos, a quantidade de saída que é retornada é grande. Você pode personalizar quais informações são

exibidas na saída especificando parâmetros opcionais:

- Você pode usar o parâmetro opcional `-fields` para exibir a saída sobre os campos que você escolher.

Você pode inserir `-fields ?` para determinar quais campos você pode usar.

- Você pode usar o `-instance` parâmetro para exibir informações detalhadas sobre sessões SMB estabelecidas.
- Você pode usar o `-fields` parâmetro ou o `-instance` parâmetro sozinho ou em combinação com outros parâmetros opcionais.

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir informações de sessão SMB...	Digite o seguinte comando...
Para todas as sessões no SVM de forma resumida	<code>vserver cifs session show -vserver vserver_name</code>
Em um ID de conexão especificado	<code>vserver cifs session show -vserver vserver_name -connection-id integer</code>
A partir de um endereço IP de estação de trabalho especificado	<code>vserver cifs session show -vserver vserver_name -address workstation_IP_address</code>
Em um endereço IP de LIF especificado	<code>vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address</code>
Em um nó especificado	<code>`vserver cifs session show -vserver vserver_name -node {node_name</code>
local}`	De um usuário do Windows especificado
<code>vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name</code>	Com um mecanismo de autenticação especificado
<code>`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1</code>	NTLMv2
Kerberos	Anonymous}`
Com uma versão de protocolo especificada	<code>`vserver cifs session show -vserver vserver_name -protocol-version {SMB1</code>
SMB2	SMB2_1

Se você quiser exibir informações de sessão SMB...	Digite o seguinte comando...
SMB3	<p>SMB3_1}`</p> <p>[NOTE] ==== A proteção continuamente disponível e o SMB multicanal estão disponíveis apenas nas sessões SMB 3,0 e posteriores. Para ver o seu estado em todas as sessões de qualificação, deve especificar este parâmetro com o valor definido para SMB3 ou posterior.</p> <p>====</p>
Com um nível especificado de proteção continuamente disponível	`vserver cifs session show -vserver vserver_name -continuously-available {No
Yes	<p>Partial}`</p> <p>[NOTE] ==== Se o status continuamente disponível for Partial, isso significa que a sessão contém pelo menos um arquivo aberto continuamente disponível, mas a sessão tem alguns arquivos que não estão abertos com proteção continuamente disponível. Você pode usar o <code>vserver cifs sessions file show</code> comando para determinar quais arquivos na sessão estabelecida não estão abertos com proteção continuamente disponível.</p> <p>====</p>
Com um status de sessão de assinatura SMB especificado	`vserver cifs session show -vserver vserver_name -is-session-signed {true

Exemplos

O comando a seguir exibe informações de sessão para as sessões no SVM VS1 estabelecidas a partir de uma estação de trabalho com endereço IP 10,1,1,1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session
ID       ID       Workstation      Windows User      Open      Idle
-----  -----  -----
3151272279,
3151272280,
3151272281  1       10.1.1.1        DOMAIN\joe        2         23s
```

O comando a seguir exibe informações detalhadas da sessão para sessões com proteção continuamente disponível no SVM VS1. A conexão foi feita usando a conta de domínio.

```
cluster1::> vserver cifs session show -instance -continuously-available  
Yes
```

```
        Node: nodel  
        Vserver: vs1  
        Session ID: 1  
        Connection ID: 3151274158  
Incoming Data LIF IP Address: 10.2.1.1  
        Workstation IP address: 10.1.1.2  
        Authentication Mechanism: Kerberos  
        Windows User: DOMAIN\SERVER1$\br/>        UNIX User: pcuser  
        Open Shares: 1  
        Open Files: 1  
        Open Other: 0  
        Connected Time: 10m 43s  
        Idle Time: 1m 19s  
        Protocol Version: SMB3  
        Continuously Available: Yes  
        Is Session Signed: false  
        User Authenticated as: domain-user  
        NetBIOS Name: -  
        SMB Encryption Status: Unencrypted
```

O comando a seguir exibe informações de sessão em uma sessão usando SMB 3,0 e SMB Multichannel no SVM VS1. No exemplo, o usuário conectado a esse compartilhamento a partir de um cliente compatível com SMB 3,0 usando o endereço IP LIF; portanto, o mecanismo de autenticação padrão é NTLMv2. A conexão deve ser feita usando a autenticação Kerberos para se conectar com a proteção continuamente disponível.


```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

Node: nodel
Vserver: vs1
Session ID: 1
**Connection IDs: 3151272607,31512726078,3151272609
Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
Workstation IP address: 10.1.1.3
Authentication Mechanism: NTLMv2
Windows User: DOMAIN\administrator
UNIX User: pcuser
Open Shares: 1
Open Files: 0
Open Other: 0
Connected Time: 6m 22s
Idle Time: 5m 42s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

Informações relacionadas

[Exibindo informações sobre arquivos SMB abertos](#)

Exibir informações sobre arquivos SMB abertos

Você pode exibir informações sobre arquivos SMB abertos, incluindo a conexão SMB e Session ID, o volume de hospedagem, o nome do compartilhamento e o caminho do compartilhamento. Você pode exibir informações sobre o nível de proteção continuamente disponível de um arquivo, o que é útil para determinar se um arquivo aberto está em um estado compatível com operações ininterruptas.

Sobre esta tarefa

Você pode exibir informações sobre arquivos abertos em uma sessão SMB estabelecida. As informações exibidas são úteis quando você precisa determinar informações de sessão SMB para arquivos específicos em uma sessão SMB.

Por exemplo, se você tiver uma sessão SMB em que alguns dos arquivos abertos estão abertos com proteção continuamente disponível e alguns não estão abertos com proteção continuamente disponível (o valor para o `-continuously-available` campo na `vserver cifs session show` saída de comando é `Partial`), você pode determinar quais arquivos não estão disponíveis continuamente usando este comando.

Você pode exibir informações de todos os arquivos abertos em sessões SMB estabelecidas em máquinas virtuais de armazenamento (SVMs) em forma de resumo usando o `vserver cifs session file show`

comando sem quaisquer parâmetros opcionais.

No entanto, em muitos casos, a quantidade de saída retornada é grande. Você pode personalizar quais informações são exibidas na saída especificando parâmetros opcionais. Isso pode ser útil quando você deseja exibir informações para apenas um pequeno subconjunto de arquivos abertos.

- Você pode usar o parâmetro opcional `-fields` para exibir a saída nos campos que você escolher.

Você pode usar este parâmetro sozinho ou em combinação com outros parâmetros opcionais.

- Você pode usar o `-instance` parâmetro para exibir informações detalhadas sobre arquivos SMB abertos.

Você pode usar este parâmetro sozinho ou em combinação com outros parâmetros opcionais.

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir arquivos SMB abertos...	Digite o seguinte comando...
No SVM no formulário de resumo	<pre>vserver cifs session file show -vserver vserver_name</pre>
Em um nó especificado	<pre>`vserver cifs session file show -vserver vserver_name -node {node_name</pre>
local}`	Em um ID de arquivo especificado
<pre>vserver cifs session file show -vserver vserver_name -file-id integer</pre>	Em uma ID de conexão SMB especificada
<pre>vserver cifs session file show -vserver vserver_name -connection-id integer</pre>	Em um SMB Session ID especificado
<pre>vserver cifs session file show -vserver vserver_name -session-id integer</pre>	No agregado de hospedagem especificado
<pre>vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name</pre>	No volume especificado
<pre>vserver cifs session file show -vserver vserver_name -hosting-volume volume_name</pre>	No compartilhamento SMB especificado

Se você quiser exibir arquivos SMB abertos...	Digite o seguinte comando...
<code>vserver cifs session file show -vserver vserver_name -share share_name</code>	No caminho SMB especificado
<code>vserver cifs session file show -vserver vserver_name -path path</code>	Com o nível especificado de proteção continuamente disponível
<code>`vserver cifs session file show -vserver vserver_name -continuously-available {No</code>	Yes}` [NOTE] ==== Se o status continuamente disponível for No, isso significa que esses arquivos abertos não serão capazes de se recuperar sem interrupções da aquisição e da giveback. Eles também não podem se recuperar da realocação geral agregada entre parceiros em um relacionamento de alta disponibilidade. ====
Com o estado de reconexão especificado	<code>`vserver cifs session file show -vserver vserver_name -reconnected {No</code>

Existem parâmetros opcionais adicionais que você pode usar para refinar os resultados de saída. Consulte a página de manual para obter mais informações.

Exemplos

O exemplo a seguir exibe informações sobre arquivos abertos no SVM VS1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:      node1
Vserver:   vs1
Connection: 3151274158
Session:   1
File      File      Open Hosting      Continuously
ID        Type        Mode Volume      Share      Available
-----
41        Regular    r      data      data      Yes
Path:     \mytest.rtf
```

O exemplo a seguir exibe informações detalhadas sobre arquivos SMB abertos com ID de arquivo 82 no SVM VS1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance
```

```
        Node: node1
        Vserver: vs1
        File ID: 82
    Connection ID: 104617
        Session ID: 1
        File Type: Regular
        Open Mode: rw
Aggregate Hosting File: aggr1
    Volume Hosting File: data1
        CIFS Share: data1
    Path from CIFS Share: windows\win8\test\test.txt
        Share Mode: rw
        Range Locks: 1
Continuously Available: Yes
        Reconnected: No
```

Informações relacionadas

[Exibindo informações de sessão SMB](#)

Determine quais objetos e contadores de estatísticas estão disponíveis

Antes de obter informações sobre as estatísticas de hash CIFS, SMB, auditoria e BranchCache e monitorar o desempenho, você deve saber quais objetos e contadores estão disponíveis a partir dos quais você pode obter dados.

Passos

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

Se você quiser determinar...	Digite...
Quais objetos estão disponíveis	<code>statistics catalog object show</code>
Objetos específicos que estão disponíveis	<code>statistics catalog object show object object_name</code>
Quais contadores estão disponíveis	<code>statistics catalog counter show object object_name</code>

Consulte as páginas man para obter mais informações sobre quais objetos e contadores estão disponíveis.

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

Exemplos

O comando a seguir exibe descrições de objetos estatísticos selecionados relacionados ao acesso CIFS e SMB no cluster, como visto no nível avançado de privilégio:

```
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

cluster1::*> statistics catalog object show -object audit
    audit_ng                CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                    The CIFS object reports activity of the
                           Common Internet File System protocol
                           ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs            The Common Internet File System (CIFS)
                           protocol is an implementation of the
Server
                           ...

cluster1::*> statistics catalog object show -object smb1
    smb1                   These counters report activity from the
SMB
                           revision of the protocol. For information
                           ...

cluster1::*> statistics catalog object show -object smb2
    smb2                   These counters report activity from the
                           SMB2/SMB3 revision of the protocol. For
                           ...

cluster1::*> statistics catalog object show -object hashd
    hashd                  The hashd object provides counters to
measure
                           the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

O comando a seguir exibe informações sobre alguns dos contadores para o `cifs` objeto, como visto no nível

de privilégio avançado:



Este exemplo não exibe todos os contadores disponíveis para o `cifs` objeto; a saída é truncada.

```
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
```

```
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
...	...

```
cluster2::> statistics start -object client -sample-id
```

```
Object: client
```

Counter	Value
cifs_ops	0
cifs_read_ops	0
cifs_read_recv_ops	0
cifs_read_recv_size	0B
cifs_read_size	0B
cifs_write_ops	0
cifs_write_recv_ops	0
cifs_write_recv_size	0B
cifs_write_size	0B
instance_name	vserver_1:10.72.205.179
instance_uuid	2:10.72.205.179
local_ops	0
mount_ops	0

```
[...]
```

Informações relacionadas

[Exibindo estatísticas](#)

Apresentar estatísticas

É possível exibir várias estatísticas, incluindo estatísticas sobre CIFS e SMB, auditoria e hashes BranchCache, para monitorar a performance e diagnosticar problemas.

Antes de começar

Você deve ter coletado amostras de dados usando os `statistics start` comandos e `statistics stop` antes de exibir informações sobre objetos.

Passos

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

Se você quiser exibir estatísticas para...	Digite...
Todas as versões do SMB	<code>statistics show -object cifs</code>
SMB 1,0	<code>statistics show -object smb1</code>
SMB 2.x e SMB 3,0	<code>statistics show -object smb2</code>
Subsistema CIFS do nó	<code>statistics show -object nblade_cifs</code>
Auditoria multiprotocolo	<code>statistics show -object audit_ng</code>
Serviço de hash BranchCache	<code>statistics show -object hashd</code>
DNS dinâmico	<code>statistics show -object ddns_update</code>

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

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

Informações relacionadas

[Determinando quais objetos e contadores de estatísticas estão disponíveis](#)

[Monitoramento de estatísticas de sessão assinadas pelo SMB](#)

[Exibindo estatísticas do BranchCache](#)

[Uso de estatísticas para monitorar a atividade automática de referência de nós](#)

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

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

Implantar serviços baseados em cliente SMB

Use arquivos off-line para permitir o armazenamento em cache de arquivos para uso off-line

Use arquivos off-line para permitir o armazenamento em cache de arquivos para visão geral de uso off-line

O ONTAP suporta o recurso arquivos off-line da Microsoft, ou *cache do lado do cliente*, que permite que os arquivos sejam armazenados em cache no host local para uso off-line. Os usuários podem usar a funcionalidade de arquivos off-line para continuar trabalhando em arquivos, mesmo quando eles são desconetados da rede.

Você pode especificar se os documentos e programas do usuário do Windows são automaticamente armazenados em cache em um compartilhamento ou se os arquivos devem ser selecionados manualmente para armazenamento em cache. O armazenamento em cache manual é ativado por padrão para novos compartilhamentos. Os arquivos disponibilizados offline são sincronizados com o disco local do cliente Windows. A sincronização ocorre quando a conectividade de rede a um compartilhamento de sistema de armazenamento específico é restaurada.

Como os arquivos e pastas offline mantêm as mesmas permissões de acesso que a versão dos arquivos e pastas salvos no servidor CIFS, o usuário deve ter permissões suficientes nos arquivos e pastas salvos no servidor CIFS para executar ações nos arquivos e pastas offline.

Quando o usuário e outra pessoa na rede fazem alterações no mesmo arquivo, o usuário pode salvar a versão local do arquivo na rede, manter a outra versão ou salvar ambas. Se o usuário mantiver ambas as versões, um novo arquivo com as alterações do usuário local será salvo localmente e o arquivo em cache será substituído por alterações da versão do arquivo salvo no servidor CIFS.

Você pode configurar arquivos off-line em uma base de compartilhamento por compartilhamento usando as configurações de compartilhamento. Você pode escolher uma das quatro configurações de pastas offline ao criar ou modificar compartilhamentos:

- Sem armazenamento em cache

Desativa o cache do lado do cliente para o compartilhamento. Arquivos e pastas não são automaticamente armazenados em cache localmente em clientes e os usuários não podem optar por armazenar em cache arquivos ou pastas localmente.

- Armazenamento manual em cache

Permite a seleção manual de arquivos a serem armazenados em cache no compartilhamento. Esta é a configuração padrão. Por padrão, nenhum arquivo ou pasta é armazenado em cache no cliente local. Os usuários podem escolher quais arquivos e pastas desejam armazenar em cache localmente para uso off-line.

- Armazenamento automático de documentos

Permite que os documentos do usuário sejam automaticamente armazenados em cache no compartilhamento. Somente arquivos e pastas acessados são armazenados em cache localmente.

- Armazenamento em cache automático do programa

Permite que programas e documentos do usuário sejam automaticamente armazenados em cache no

compartilhamento. Somente arquivos, pastas e programas acessados são armazenados em cache localmente. Além disso, essa configuração permite que o cliente execute executáveis armazenados localmente em cache, mesmo quando conectado à rede.

Para obter mais informações sobre a configuração de arquivos off-line em servidores e clientes do Windows, consulte a Biblioteca Microsoft TechNet.

Informações relacionadas

[Usando perfis de roaming para armazenar perfis de usuário centralmente em um servidor CIFS associado ao SVM](#)

[Usando redirecionamento de pasta para armazenar dados em um servidor CIFS](#)

[Usando o BranchCache para armazenar em cache conteúdo de compartilhamento SMB em uma filial](#)

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

Requisitos para usar arquivos off-line

Antes de poder utilizar a funcionalidade arquivos offline da Microsoft com o servidor CIFS, tem de saber quais as versões do ONTAP e SMB e quais os clientes do Windows que suportam a funcionalidade.

Requisitos de versão do ONTAP

As versões do ONTAP suportam arquivos off-line.

Requisitos de versão do protocolo SMB

Para máquina virtual de storage (SVM), o ONTAP oferece suporte a arquivos off-line em todas as versões do SMB.

Requisitos do cliente Windows

O cliente Windows deve suportar os arquivos off-line.

Para obter as informações mais recentes sobre quais clientes do Windows oferecem suporte ao recurso arquivos off-line, consulte Matriz de interoperabilidade.

"mysupport.NetApp.com/matrix"

Diretrizes para a implantação de arquivos offline

Existem algumas diretrizes importantes que você precisa entender quando você implantar arquivos off-line em compartilhamentos de diretório home que têm a `showsnapshot` propriedade de compartilhamento definida em diretórios home.

Se a `showsnapshot` propriedade compartilhar estiver definida em um compartilhamento de diretório inicial que tenha arquivos off-line configurados, os clientes do Windows armazenam em cache todas as cópias `Snapshot ~snapshot` na pasta no diretório inicial do usuário.

Os clientes Windows armazenam em cache todas as cópias Snapshot no diretório inicial se uma das seguintes opções for verdadeira:

- O usuário torna o diretório home disponível offline a partir do cliente.

O conteúdo da `~snapshot` pasta no diretório inicial é incluído e disponibilizado offline.

- O usuário configura o redirecionamento de pasta para redirecionar uma pasta, como `My Documents` a raiz de um diretório home que reside no compartilhamento do servidor CIFS.

Alguns clientes do Windows podem tornar a pasta redirecionada automaticamente disponível offline. Se a pasta for redirecionada para a raiz do diretório inicial, a `~snapshot` pasta será incluída no conteúdo offline em cache.



Implantações de arquivos offline onde a `~snapshot` pasta está incluída em arquivos offline devem ser evitadas. As cópias Snapshot na `~snapshot` pasta contêm todos os dados no volume no ponto em que o ONTAP criou a cópia Snapshot. Portanto, criar uma cópia off-line da `~snapshot` pasta consome armazenamento local significativo no cliente, consome largura de banda da rede durante a sincronização de arquivos off-line e aumenta o tempo necessário para sincronizar arquivos off-line.

Configure o suporte a arquivos off-line em compartilhamentos SMB usando a CLI

Você pode configurar o suporte a arquivos off-line usando a CLI do ONTAP especificando uma das quatro configurações de arquivos off-line ao criar compartilhamentos SMB ou a qualquer momento modificando compartilhamentos SMB existentes. O suporte manual de arquivos offline é a configuração padrão.

Sobre esta tarefa

Ao configurar o suporte a arquivos off-line, você pode escolher uma das quatro configurações de arquivos off-line a seguir:

Definição	Descrição
<code>none</code>	Não permite que os clientes Windows armazenem quaisquer arquivos neste compartilhamento.
<code>manual</code>	Permite que os usuários em clientes Windows selecionem manualmente os arquivos a serem armazenados em cache.
<code>documents</code>	Permite que os clientes Windows armazenem documentos de usuário que são usados pelo usuário para acesso off-line.
<code>programs</code>	Permite que os clientes do Windows armazenem programas que são usados pelo usuário para acesso off-line. Os clientes podem usar os arquivos de programa armazenados em cache no modo offline, mesmo que o compartilhamento esteja disponível.

Você pode escolher apenas uma configuração de arquivo off-line. Se você modificar uma configuração de arquivos off-line em um compartilhamento SMB existente, a nova configuração arquivos off-line substituirá a

configuração original. Outras configurações de compartilhamento SMB existentes e propriedades de compartilhamento não são removidas ou substituídas. Eles permanecem em vigor até que sejam explicitamente removidos ou alterados.

Passos

1. Execute a ação apropriada:

Se você quiser configurar arquivos off-line em...	Digite o comando...
Um novo compartilhamento SMB	<code>`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none</code>
manual	documents
programs}`	Um compartilhamento SMB existente
<code>`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none</code>	manual
documents	programs}`

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 arquivos off-line definidos como `documents`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

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: Offline files
                Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: documents
Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
                UNIX Group for File Create: -
```

O comando a seguir modifica um compartilhamento SMB existente chamado "d.ATA1" alterando a configuração de arquivos off-line manual e adicionando valores para a máscara de criação de modo de arquivo e diretório:

```

cluster1::> vserver cifs share modify -vserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777

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: 644
Directory Mode Creation Mask: 777
                Share Comment: Offline files
                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

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

Configure o suporte a arquivos off-line em compartilhamentos SMB usando o MMC Gerenciamento do computador

Se você quiser permitir que os usuários armazenem arquivos localmente para uso off-line, você pode configurar o suporte a arquivos off-line usando o MMC de Gerenciamento do computador (Microsoft Management Console).

Passos

1. Para abrir o MMC no servidor Windows, no Windows Explorer, clique com o botão direito do Mouse no ícone do computador local e selecione **Gerenciar**.
2. No painel esquerdo, selecione **Gerenciamento de computador**.
3. Selecione **Ação > ligar a outro computador**.

A caixa de diálogo Selecionar computador é exibida.

4. Digite o nome do servidor CIFS ou clique em **Procurar** para localizar o servidor CIFS.

Se o nome do servidor CIFS for o mesmo nome do host da máquina virtual de storage (SVM), digite o nome do SVM. Se o nome do servidor CIFS for diferente do nome do host SVM, digite o nome do servidor

CIFS.

5. Clique em **OK**.
6. Na árvore da consola, clique em **Ferramentas do sistema > pastas partilhadas**.
7. Clique em **compartilhamentos**.
8. No painel de resultados, clique com o botão direito do rato no partilhar.
9. Clique em **Propriedades**.

As propriedades para a partilha seleccionada são apresentadas.

10. Na guia **Geral**, clique em **Configurações off-line**.

A caixa de diálogo Configurações off-line é exibida.

11. Configure as opções de disponibilidade off-line conforme apropriado.
12. Clique em **OK**.

Use perfis de roaming para armazenar perfis de usuário centralmente em um servidor SMB associado ao SVM

Use perfis de roaming para armazenar perfis de usuário centralmente em um servidor SMB associado à visão geral da SVM

O ONTAP suporta o armazenamento de perfis de roaming do Windows em um servidor CIFS associado à máquina virtual de armazenamento (SVM). A configuração de perfis de roaming de usuários oferece vantagens para o usuário, como disponibilidade automática de recursos, independentemente de onde o usuário faz login. Os perfis de roaming também simplificam a administração e o gerenciamento de perfis de usuário.

Os perfis de usuário de roaming têm as seguintes vantagens:

- Disponibilidade automática de recursos

O perfil exclusivo de um usuário fica automaticamente disponível quando esse usuário faz login em qualquer computador na rede que esteja executando o Windows 8, Windows 7, Windows 2000 ou Windows XP. Os usuários não precisam criar um perfil em cada computador que usam em uma rede.

- Substituição simplificada do computador

Como todas as informações de perfil do usuário são mantidas separadamente na rede, o perfil de um usuário pode ser facilmente baixado em um novo computador de substituição. Quando o usuário faz login no novo computador pela primeira vez, a cópia do perfil do usuário é copiada para o novo computador.

Informações relacionadas

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

[Usando redirecionamento de pasta para armazenar dados em um servidor CIFS](#)

Requisitos para usar perfis de roaming

Antes de poder utilizar os perfis de roaming da Microsoft com o seu servidor CIFS, tem de saber quais versões do ONTAP e SMB e quais clientes do Windows suportam a funcionalidade.

Requisitos de versão do ONTAP

ONTAP suporta perfis de roaming.

Requisitos de versão do protocolo SMB

Para máquina virtual de armazenamento (SVM), o ONTAP oferece suporte a perfis de roaming em todas as versões do SMB.

Requisitos do cliente Windows

Antes que um usuário possa usar os perfis de roaming, o cliente Windows deve suportar o recurso.

Para obter as informações mais recentes sobre quais clientes Windows suportam perfis de roaming, consulte a Matriz de interoperabilidade.

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

Configurar perfis de roaming

Se você quiser disponibilizar automaticamente o perfil de um usuário quando ele fizer logon em qualquer computador da rede, poderá configurar perfis de roaming através do snap-in MMC usuários e computadores do active Directory. Se estiver configurando perfis de roaming no Windows Server, você poderá usar o Centro de Administração do active Directory.

Passos

1. No servidor Windows, abra o MMC usuários e computadores do active Directory (ou o Centro de Administração do active Directory em servidores Windows).
2. Localize o usuário para o qual você deseja configurar um perfil de roaming.
3. Clique com o botão direito do rato no utilizador e clique em **Propriedades**.
4. Na guia **Perfil**, insira o caminho do perfil para o compartilhamento onde deseja armazenar o perfil de roaming do usuário, seguido de %username%.

Por exemplo, um caminho de perfil pode ser o seguinte `\\vs1.example.com\profiles\%username%`. A primeira vez que um utilizador inicia sessão %username% é substituído pelo nome do utilizador.



No caminho `\\vs1.example.com\profiles\%username%` `profiles`, é o nome de compartilhamento de um compartilhamento na máquina virtual de armazenamento (SVM) VS1 que tem direitos de controle total para todos.

5. Clique em **OK**.

Use o redirecionamento de pastas para armazenar dados em um servidor SMB

Use o redirecionamento de pastas para armazenar dados em uma visão geral do servidor SMB

O ONTAP oferece suporte ao redirecionamento de pastas da Microsoft, o que permite que usuários ou administradores redirecionem o caminho de uma pasta local para um local no servidor CIFS. Aparece como se as pastas redirecionadas fossem armazenadas no cliente Windows local, mesmo que os dados estejam armazenados em um compartilhamento SMB.

O redirecionamento de pastas destina-se principalmente a organizações que já implantaram diretórios base e que desejam manter a compatibilidade com seu ambiente de diretório base existente.

- `Documents`, `Desktop` e `Start Menu` são exemplos de pastas que podem ser redirecionadas.
- Os usuários podem redirecionar pastas de seu cliente Windows.
- Os administradores podem configurar e gerenciar centralmente o redirecionamento de pastas configurando GPOs no `Active Directory`.
- Se os administradores tiverem configurado perfis de roaming, o redirecionamento de pastas permite que os administradores dividam os dados do usuário dos dados do perfil.
- Os administradores podem usar o redirecionamento de pastas e arquivos offline juntos para redirecionar o armazenamento de dados para pastas locais para o servidor CIFS, permitindo que os usuários armazenem o conteúdo localmente.

Informações relacionadas

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

[Usando perfis de roaming para armazenar perfis de usuário centralmente em um servidor CIFS associado ao SVM](#)

Requisitos para usar o redirecionamento de pastas

Antes de poder usar o redirecionamento de pastas da Microsoft com o servidor CIFS, você precisa saber quais versões do ONTAP e SMB e quais clientes do Windows suportam o recurso.

Requisitos de versão do ONTAP

O ONTAP suporta redirecionamento de pastas da Microsoft.

Requisitos de versão do protocolo SMB

Para máquina virtual de storage (SVM), o ONTAP oferece suporte ao redirecionamento de pastas da Microsoft em todas as versões do SMB.

Requisitos do cliente Windows

Antes que um usuário possa usar o redirecionamento de pastas da Microsoft, o cliente do Windows deve suportar o recurso.

Para obter as informações mais recentes sobre quais clientes do Windows suportam redirecionamento de pastas, consulte [Matriz de interoperabilidade](#).

Configurar redirecionamento de pastas

Você pode configurar o redirecionamento de pastas usando a janela Propriedades do Windows. A vantagem de usar esse método é que o usuário do Windows pode configurar o redirecionamento de pastas sem a ajuda do administrador SVM.

Passos

1. No Explorador do Windows, clique com o botão direito do rato na pasta que pretende redirecionar para uma partilha de rede.
2. Clique em **Propriedades**.

As propriedades para a partilha selecionada são apresentadas.

3. Na guia **atalho**, clique em **destino** e especifique o caminho para o local da rede onde deseja redirecionar a pasta selecionada.

Por exemplo, se você quiser redirecionar uma pasta para a data pasta em um diretório inicial mapeado para Q:\, especifique Q:\data como destino.

4. Clique em **OK**.

Para obter mais informações sobre como configurar pastas offline, consulte a Biblioteca Microsoft TechNet.

Informações relacionadas

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

Acesse o diretório de snapshot de clientes Windows usando SMB 2.x

O método usado para acessar o `~snapshot` diretório de clientes do Windows usando SMB 2.x difere do método usado para SMB 1,0. Você precisa entender como acessar o `~snapshot` diretório ao usar conexões SMB 2.x para acessar com êxito os dados armazenados em cópias Snapshot.

O administrador do SVM controla se os usuários em clientes Windows podem exibir e acessar o `~snapshot` diretório em um compartilhamento ativando ou desativando a `showsnapshot` propriedade de compartilhamento usando comandos das famílias de propriedades de compartilhamento cifs do vserver.

Quando a `showsnapshot` propriedade compartilhar está desativada, um usuário em um cliente Windows que usa SMB 2.x não pode exibir o `~snapshot` diretório e não pode acessar cópias Snapshot dentro `~snapshot` do diretório, mesmo quando manualmente inserir o caminho para `~snapshot` o diretório ou para cópias Snapshot específicas dentro do diretório.

Quando a `showsnapshot` propriedade compartilhar está ativada, um usuário em um cliente Windows que usa SMB 2.x ainda não pode exibir o `~snapshot` diretório na raiz do compartilhamento ou em qualquer junção ou diretório abaixo da raiz do compartilhamento. No entanto, depois de se conectar a um compartilhamento, o usuário pode acessar o diretório oculto `~snapshot` anexando manualmente `\~snapshot` ao final do caminho de compartilhamento. O diretório oculto `~snapshot` é acessível a partir de dois pontos de entrada:

- Na raiz da partilha
- Em cada ponto de junção no espaço de partilha

O diretório oculto `~snapshot` não é acessível a partir de subdiretórios que não sejam de junção dentro do compartilhamento.

Exemplo

Com a configuração mostrada no exemplo a seguir, um usuário em um cliente Windows com uma conexão SMB 2.x ao compartilhamento "eng" pode acessar o `~snapshot` diretório anexando manualmente `\~snapshot` o caminho de compartilhamento na raiz do compartilhamento e em cada ponto de junção no caminho. O diretório oculto `~snapshot` é acessível a partir dos seguintes três caminhos:

- `\\vs1\eng\~snapshot`
- `\\vs1\eng\projects1\~snapshot`
- `\\vs1\eng\projects2\~snapshot`

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume          junction-path
-----
vs1      vs1_root              /
vs1      vs1_vol1              /eng
vs1      vs1_vol2              /eng/projects1
vs1      vs1_vol3              /eng/projects2

cluster1::> vsserver cifs share show
Vserver  Share  Path      Properties      Comment  ACL
-----
vs1      eng    /eng      oplocks         -        Everyone / Full Control
          chngenotify
          browsable
          showsnapshot
```

Recupere arquivos e pastas usando versões anteriores

Recupere arquivos e pastas usando a visão geral das versões anteriores

A capacidade de usar as versões anteriores da Microsoft é aplicável a sistemas de arquivos que suportam cópias Snapshot de alguma forma e as habilitam. A tecnologia Snapshot faz parte integrante do ONTAP. Os usuários podem recuperar arquivos e pastas de cópias Snapshot de seu cliente Windows usando o recurso versões anteriores da Microsoft.

A funcionalidade de versões anteriores fornece um método para os usuários navegarem pelas cópias Snapshot ou restaurarem dados de uma cópia Snapshot sem a intervenção do administrador de storage. As versões anteriores não são configuráveis. Está sempre ativado. Se o administrador de storage disponibilizar cópias Snapshot em um compartilhamento, o usuário poderá usar versões anteriores para executar as

seguintes tarefas:

- Recuperar arquivos que foram excluídos acidentalmente.
- Recuperar de acidentalmente sobrescrever um arquivo.
- Compare versões do arquivo enquanto trabalha.

Os dados armazenados nas cópias Snapshot são somente leitura. Os usuários devem salvar uma cópia de um arquivo em outro local para fazer quaisquer alterações no arquivo. As cópias snapshot são excluídas periodicamente; portanto, os usuários precisam criar cópias de arquivos contidos em versões anteriores se quiserem manter indefinidamente uma versão anterior de um arquivo.

Requisitos para usar versões anteriores da Microsoft

Antes de poder utilizar versões anteriores com o seu servidor CIFS, precisa de saber quais as versões do ONTAP e SMB e quais os clientes do Windows que o suportam. Você também precisa saber sobre o requisito de configuração de cópia Snapshot.

Requisitos de versão do ONTAP

Suporta versões anteriores.

Requisitos de versão do protocolo SMB

Para máquina virtual de storage (SVM), o ONTAP é compatível com versões anteriores em todas as versões do SMB.

Requisitos do cliente Windows

Antes que um usuário possa usar versões anteriores para acessar dados em cópias Snapshot, o cliente do Windows deve oferecer suporte ao recurso.

Para obter as informações mais recentes sobre quais clientes Windows suportam versões anteriores, consulte a Matriz de interoperabilidade.

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

Requisitos para configurações de cópia Snapshot

Para usar versões anteriores para acessar dados em cópias Snapshot, uma política de Snapshot habilitada deve estar associada ao volume que contém os dados, os clientes precisam ter acesso aos dados do Snapshot e as cópias Snapshot devem existir.

Use a guia versões anteriores para exibir e gerenciar dados de cópia Snapshot

Os usuários em máquinas clientes Windows podem usar a guia versões anteriores na janela Propriedades do Windows para restaurar dados armazenados em cópias Snapshot sem precisar envolver o administrador da máquina virtual de armazenamento (SVM).

Sobre esta tarefa

Você só poderá usar a guia versões anteriores para exibir e gerenciar dados em cópias Snapshot de dados armazenados no SVM se o administrador tiver habilitado cópias Snapshot no volume que contém o

compartilhamento e se o administrador configurar o compartilhamento para mostrar cópias Snapshot.

Passos

1. No Windows Explorer, exiba o conteúdo da unidade mapeada dos dados armazenados no servidor CIFS.
2. Clique com o botão direito do rato no ficheiro ou pasta na unidade de rede mapeada cujas cópias Snapshot pretende visualizar ou gerir.
3. Clique em **Propriedades**.

As propriedades para o arquivo ou pasta selecionado são exibidas.

4. Clique no separador **versões anteriores**.

Uma lista de cópias Snapshot disponíveis do arquivo ou pasta selecionado é exibida na caixa versões da pasta. As cópias Snapshot listadas são identificadas pelo prefixo do nome da cópia Snapshot e pelo carimbo de data/hora da criação.

5. Na caixa **versões da pasta**, clique com o botão direito do Mouse na cópia do arquivo ou pasta que você deseja gerenciar.
6. Execute a ação apropriada:

Se você quiser...	Faça o seguinte...
Exibir dados dessa cópia Snapshot	Clique em abrir .
Crie uma cópia dos dados dessa cópia Snapshot	Clique em Copiar .

Os dados nas cópias Snapshot são somente leitura. Se você quiser fazer modificações nos arquivos e pastas listados na guia versões anteriores, salve uma cópia dos arquivos e pastas que deseja modificar para um local gravável e faça modificações nas cópias.

7. Depois de concluir o gerenciamento dos dados do Snapshot, feche a caixa de diálogo **Propriedades** clicando em **OK**.

Para obter mais informações sobre como usar a guia versões anteriores para exibir e gerenciar dados do Snapshot, consulte a Biblioteca Microsoft TechNet.

Informações relacionadas

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

Determine se as cópias Snapshot estão disponíveis para uso em versões anteriores

Você pode exibir cópias Snapshot da guia versões anteriores somente se uma política de snapshot habilitada for aplicada ao volume que contém o compartilhamento e se a configuração de volume permitir acesso a cópias snapshot. Determinar a disponibilidade da cópia Snapshot é útil ao ajudar um usuário com acesso a versões anteriores.

Passos

1. Determine se o volume no qual residem os dados de compartilhamento tem cópias automáticas do Snapshot ativadas e se os clientes têm acesso aos diretórios do Snapshot: `volume show -vserver vserver-name -volume volume-name -fields vserver,volume,snapsdir-`

`access, snapshot-policy, snapshot-count`

A saída exibe a política Snapshot associada ao volume, se o acesso ao diretório Snapshot do cliente está habilitado e o número de cópias Snapshot disponíveis.

2. Determine se a política de snapshot associada está ativada: `volume snapshot policy show -policy policy-name`
3. Listar as cópias Snapshot disponíveis: `volume snapshot show -volume volume_name`

Para obter mais informações sobre como configurar e gerenciar políticas de Snapshot e programações de snapshot, "[Proteção de dados](#)" consulte .

Exemplo

O exemplo a seguir exibe informações sobre políticas de Snapshot associadas ao volume chamado "ATA1" que contém os dados compartilhados e as cópias Snapshot disponíveis no "ATA1".

```

cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume  snapdir-access  snapshot-policy  snapshot-count
-----  -----  -----
vs1      data1  true            default          10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1

          Number of Is
Policy Name  Schedules Enabled Comment
-----
default          3 true  Default policy with hourly, daily &
weekly schedules.
  Schedule      Count      Prefix      SnapMirror Label
  -----
  hourly         6      hourly      -
  daily          2      daily       daily
  weekly         2      weekly      weekly

cluster1::> volume snapshot show -volume data1

          ---Blocks---
Vserver  Volume  Snapshot          State      Size  Total%  Used%
-----  -----  -----
vs1      data1
          weekly.2012-12-16_0015  valid      408KB    0%     1%
          daily.2012-12-22_0010  valid      420KB    0%     1%
          daily.2012-12-23_0010  valid      192KB    0%     0%
          weekly.2012-12-23_0015  valid      360KB    0%     1%
          hourly.2012-12-23_1405  valid      196KB    0%     0%
          hourly.2012-12-23_1505  valid      196KB    0%     0%
          hourly.2012-12-23_1605  valid      212KB    0%     0%
          hourly.2012-12-23_1705  valid      136KB    0%     0%
          hourly.2012-12-23_1805  valid      200KB    0%     0%
          hourly.2012-12-23_1905  valid      184KB    0%     0%

```

Informações relacionadas

[Criando uma configuração Snapshot para habilitar o acesso a versões anteriores](#)

["Proteção de dados"](#)

Crie uma configuração Snapshot para habilitar o acesso a versões anteriores

A funcionalidade de versões anteriores está sempre disponível, desde que o acesso do cliente às cópias Snapshot esteja habilitado e desde que existam cópias Snapshot. Se a configuração da cópia Snapshot não atender a esses requisitos, você poderá criar uma configuração de cópia Snapshot correspondente.

Passos

1. Se o volume que contém o compartilhamento ao qual você deseja permitir o acesso a versões anteriores não tiver uma política Snapshot associada, associe uma política Snapshot ao volume e ative-a usando o `volume modify` comando.

Para obter mais informações sobre como usar o `volume modify` comando, consulte as páginas de manual.

2. Habilite o acesso às cópias Snapshot usando o `volume modify` comando para definir a `-snap-dir` opção como `true`.

Para obter mais informações sobre como usar o `volume modify` comando, consulte as páginas de manual.

3. Verifique se as políticas Snapshot estão ativadas e se o acesso aos diretórios Snapshot está ativado usando os `volume show` comandos e `volume snapshot policy show`

Para obter mais informações sobre como usar os `volume show` comandos e `volume snapshot policy show`, consulte as páginas de manual.

Para obter mais informações sobre como configurar e gerenciar políticas de Snapshot e programações de snapshot, "[Proteção de dados](#)" consulte .

Informações relacionadas

["Proteção de dados"](#)

Diretrizes para restaurar diretórios que contêm junções

Existem certas diretrizes que você deve ter em mente ao usar versões anteriores para restaurar pastas que contêm pontos de junção.

Ao usar versões anteriores para restaurar pastas com pastas filhas que são pontos de junção, a restauração pode falhar com um `Access Denied` erro.

Você pode determinar se a pasta que você está tentando restaurar contém uma junção usando o `vol show` comando com a `-parent` opção. Você também pode usar os `vserver security trace` comandos para criar logs detalhados sobre problemas de acesso a arquivos e pastas.

Informações relacionadas

[Criação e gerenciamento de volumes de dados em namespaces nas](#)

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

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

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

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

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

```
cluster::> vserver cifs home-directory search-path show -vserver vs1
```

```
Vserver      Position Path
-----
vs1          1          /home1
```

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

```
cluster::> vserver 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 /voll/user contém diretórios base...	Compartilhar comando...
Para criar um caminho de compartilhamento \\vs1\~win_username que direcione o usuário /voll/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 /voll/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 /voll/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 /voll/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
enable (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 <code>widelinks</code> . O acesso à <code>Widelink</code> 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 <code>widelinks</code> para acesso de leitura e gravação. Os anúncios DFS são gerados para links simbólicos locais e <code>widelinks</code> , 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 <code>widelinks</code> 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 `v_s1` 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/"

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.
<i>Path to hash store</i>	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. 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. O caminho hash pode conter espaços em branco e quaisquer caracteres de nome de arquivo válidos.

Opcionalmente, você pode especificar os seguintes parâmetros:

Parâmetros opcionais	Descrição
<i>Versões suportadas</i>	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.
<i>Tamanho máximo do armazenamento de hash</i>	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.
<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:

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

- b. 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`
- c. 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.

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

- e. 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

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

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

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. Saiba mais sobre " Gerenciamento de volumes do FlexVol "	Modifique o caminho do diretório de armazenamento de hash

Se você quiser...	Digite o seguinte...
<pre>`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true</pre>	<p>false}` 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>
Altere o modo de funcionamento	<pre>`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share</pre>
all-shares	<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>
Altere o suporte à versão do BranchCache	<pre>`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable</pre>
v2-enable	<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

[Excluindo a configuração BranchCache em SVMs](#)

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.



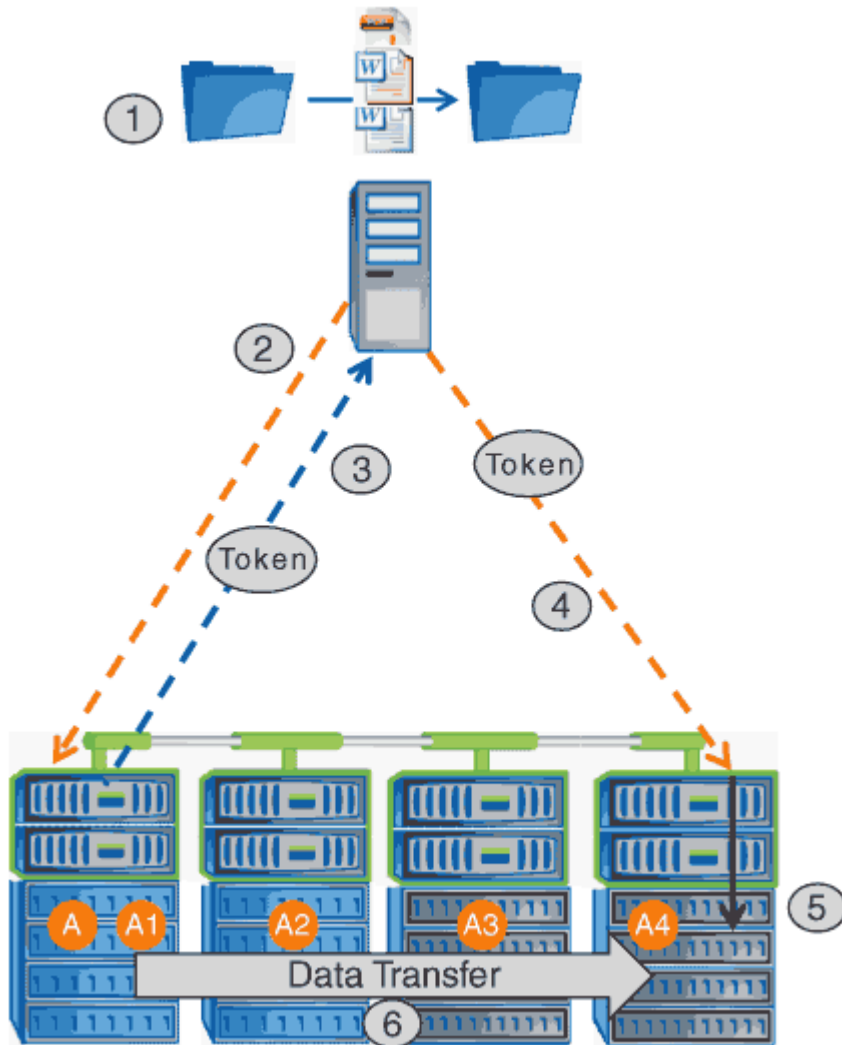
A origem e o destino podem estar na mesma máquina virtual de storage (SVM) ou em SVMs diferentes, dependendo do escopo da operação de cópia.

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

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

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.

Dependências de nomes de arquivos e diretórios NFS e SMB

Visão geral das dependências de nomes de arquivos e diretórios NFS e SMB

As convenções de nomenclatura de arquivos e diretórios dependem tanto dos sistemas operacionais dos clientes de rede quanto dos protocolos de compartilhamento de arquivos, além das configurações de idioma do cluster e dos clientes do ONTAP.

O sistema operacional e os protocolos de compartilhamento de arquivos determinam o seguinte:

- Carateres que um nome de arquivo pode usar
- Sensibilidade em caso de um nome de ficheiro

O ONTAP suporta caracteres multibyte em nomes de arquivo, diretório e `qtree`, dependendo da versão do ONTAP.

Carateres que um nome de arquivo ou diretório pode usar

Se você estiver acessando um arquivo ou diretório de clientes com sistemas operacionais diferentes, use carateres válidos em ambos os sistemas operacionais.

Por exemplo, se você usar UNIX para criar um arquivo ou diretório, não use dois pontos (`:`) no nome porque os dois pontos não são permitidos em nomes de arquivo ou diretório MS-dos. Como as restrições em carateres válidos variam de um sistema operacional para outro, consulte a documentação do sistema operacional cliente para obter mais informações sobre carateres proibidos.

Sensibilidade de casos de nomes de arquivos e diretórios em um ambiente multiprotocolo

Os nomes de arquivos e diretórios são sensíveis a maiúsculas e minúsculas para clientes NFS, mas que preservam casos para clientes SMB. Você deve entender quais são as implicações em um ambiente multiprotocolo e as ações que pode precisar tomar ao especificar o caminho ao criar compartilhamentos SMB e ao acessar dados nos compartilhamentos.

Se um cliente SMB criar um diretório `testdir` chamado , os clientes SMB e NFS exibirão o nome do arquivo como `testdir`. No entanto, se um usuário SMB tentar criar um nome de diretório mais tarde `TESTDIR` , o

nome não será permitido porque, para o cliente SMB, esse nome existe atualmente. Se um usuário NFS criar posteriormente um diretório `TESTDIR` chamado , clientes NFS e SMB exibirão o nome do diretório de maneira diferente, da seguinte forma:

- Em clientes NFS, você verá ambos os nomes de diretório à medida que foram criados, por `testdir` exemplo e `TESTDIR`, porque os nomes de diretório são sensíveis a maiúsculas e minúsculas.
- Os clientes SMB usam os nomes 8,3 para distinguir entre os dois diretórios. Um diretório tem o nome do arquivo base. Os diretórios adicionais recebem um nome de arquivo 8,3.
 - Em clientes SMB, você verá `testdir` e `TESTDI~1`.
 - O ONTAP cria o `TESTDI~1` nome do diretório para diferenciar os dois diretórios.

Nesse caso, você deve usar o nome 8,3 ao especificar um caminho de compartilhamento ao criar ou modificar um compartilhamento em uma máquina virtual de storage (SVM).

Da mesma forma para arquivos, se um cliente SMB criar `test.txt`, os clientes SMB e NFS exibirão o nome do arquivo como `text.txt`. No entanto, se um usuário SMB tentar criar mais tarde `Test.txt`, o nome não será permitido porque, para o cliente SMB, esse nome existe atualmente. Se um usuário NFS criar mais tarde um arquivo `Test.txt` chamado , clientes NFS e SMB exibirão o nome do arquivo de forma diferente, da seguinte forma:

- Em clientes NFS, você verá ambos os nomes de arquivos à medida que foram criados e `test.txt` `Test.txt`, porque os nomes de arquivos são sensíveis a maiúsculas e minúsculas.
- Os clientes SMB usam os nomes 8,3 para distinguir entre os dois arquivos. Um arquivo tem o nome do arquivo base. Os ficheiros adicionais recebem um nome de ficheiro 8,3.
 - Em clientes SMB, você verá `test.txt` e `TEST~1.TXT`.
 - O ONTAP cria o `TEST~1.TXT` nome do arquivo para diferenciar os dois arquivos.



Se você tiver ativado ou modificado o mapeamento de caracteres usando os comandos SVM CIFS de mapeamento de caracteres, uma pesquisa Windows normalmente insensível a maiúsculas e minúsculas torna-se sensível a maiúsculas e minúsculas.

Como o ONTAP cria nomes de arquivo e diretório

O ONTAP cria e mantém dois nomes para arquivos ou diretórios em qualquer diretório que tenha acesso de um cliente SMB: O nome longo original e um nome no formato 8,3.

Para nomes de arquivo ou diretório que excedam o nome de oito caracteres ou o limite de extensão de três caracteres (para arquivos), o ONTAP gera um nome de formato 8,3 da seguinte forma:

- Ele trunca o nome do arquivo ou diretório original para seis caracteres, se o nome exceder seis caracteres.
- Ele adiciona um til (...) e um número, um a cinco, aos nomes de arquivo ou diretório que não são mais exclusivos depois de serem truncados.

Se ele ficar sem números porque há mais de cinco nomes semelhantes, ele cria um nome exclusivo que não tem relação com o nome original.

- No caso dos arquivos, ele trunca a extensão do nome do arquivo para três caracteres.

Por exemplo, se um cliente NFS criar um arquivo chamado `specifications.html`, o nome do arquivo de

formato 8,3 criado pelo ONTAP será `specif~1.htm`. Se esse nome já existir, o ONTAP usará um número diferente no final do nome do arquivo. Por exemplo, se um cliente NFS criar outro arquivo chamado `specifications_new.html`, o formato 8,3 do `specifications_new.html` é `specif~2.htm`.

Como o ONTAP lida com nomes de arquivos, diretórios e qtree de vários bytes

Começando com ONTAP 9.5, o suporte para nomes codificados UTF-8 de 4 bytes permite a criação e exibição de nomes de arquivos, diretórios e árvores que incluem caracteres suplementares Unicode fora do plano multilíngue básico (BMP). Em versões anteriores, esses caracteres suplementares não foram exibidos corretamente em ambientes multiprotocolo.

Para ativar o suporte para nomes codificados UTF-8 de 4 bytes, um novo código de linguagem `utf8mb4` está disponível para as `vserver` famílias de comandos e `volume`.

Você deve criar um novo volume de uma das seguintes maneiras:

- Definir a opção de volume `-language` explicitamente: `volume create -language utf8mb4 {...}`
- Herdando a opção de volume `-language` de uma SVM que foi criada ou modificada para a opção: `vserver [create|modify] -language utf8mb4 {...}`volume create {...}`
- No ONTAP 9.6 e anteriores, não é possível modificar volumes existentes para suporte a `utf8mb4`; é necessário criar um novo volume pronto para `utf8mb4` e migrar os dados usando ferramentas de cópia baseadas em cliente.

Você pode atualizar SVMs para suporte a `utf8mb4`, mas os volumes existentes mantêm seus códigos de idioma originais.

Se você estiver usando o ONTAP 9.7P1 ou posterior, poderá modificar volumes existentes para o `utf8mb4` com uma solicitação de suporte. Para obter mais informações, "[O idioma do volume pode ser alterado após a criação no ONTAP?](#)" consulte .

- Começando com ONTAP 9.8, você pode usar o `[-language <Language code>]` parâmetro para alterar o idioma do volume de `*.UTF-8` para `utf8mb4`. Para alterar o idioma de um volume, "[Suporte à NetApp](#)" contacte .



Nomes LUN com caracteres UTF-8 de 4 bytes não são suportados atualmente.

- Os dados de caracteres Unicode são normalmente representados em aplicações de sistemas de ficheiros Windows utilizando o formato de transformação Unicode de 16 bits (UTF-16) e em sistemas de ficheiros NFS utilizando o formato de transformação Unicode de 8 bits (UTF-8).

Em versões anteriores ao ONTAP 9.5, nomes incluindo caracteres suplementares UTF-16 que foram criados por clientes Windows foram exibidos corretamente para outros clientes Windows, mas não foram traduzidos corretamente para UTF-8 para clientes NFS. Da mesma forma, nomes com caracteres suplementares UTF-8 por clientes NFS criados não foram traduzidos corretamente para UTF-16 para clientes Windows.

- Quando você cria nomes de arquivo em sistemas que executam o ONTAP 9.4 ou anteriores que contêm caracteres suplementares válidos ou inválidos, o ONTAP rejeita o nome do arquivo e retorna um erro de nome de arquivo inválido.

Para evitar esse problema, use apenas caracteres BMP em nomes de arquivo e evite usar caracteres

suplementares ou atualize para o ONTAP 9.5 ou posterior.

Começando com ONTAP 9, caracteres Unicode são permitidos em nomes de qtree.

- Você pode usar a `volume qtree` família de comandos ou o System Manager para definir ou modificar nomes de qtree.
- Os nomes de qtree podem incluir caracteres de vários bytes no formato Unicode, como caracteres japoneses e chineses.
- Em versões anteriores ao ONTAP 9.5, apenas os caracteres BMP (ou seja, aqueles que poderiam ser representados em 3 bytes) foram suportados.



Em versões anteriores ao ONTAP 9.5, o caminho de junção do volume pai da qtree pode conter nomes de qtree e diretório com caracteres Unicode. O `volume show` comando exibe esses nomes corretamente quando o volume pai tem uma configuração de idioma UTF-8. No entanto, se o idioma do volume pai não for uma das configurações de idioma UTF-8, algumas partes do caminho de junção serão exibidas usando um nome alternativo NFS numérico.

- Em versões 9,5 e posteriores, os caracteres de 4 bytes são suportados em nomes de qtree, desde que a qtree esteja em um volume habilitado para `utf8mb4`.

Configure o mapeamento de caracteres para a tradução de nomes de arquivo SMB em volumes

Os clientes NFS podem criar nomes de arquivos que contêm caracteres que não são válidos para clientes SMB e determinados aplicativos do Windows. Você pode configurar o mapeamento de caracteres para a tradução de nome de arquivo em volumes para permitir que clientes SMB acessem arquivos com nomes NFS que, de outra forma, não seriam válidos.

Sobre esta tarefa

Quando os arquivos criados por clientes NFS são acessados por clientes SMB, o ONTAP examina o nome do arquivo. Se o nome não for um nome de arquivo SMB válido (por exemplo, se ele tiver um caractere de dois pontos ":" incorporado), o ONTAP retornará o nome de arquivo 8,3 que é mantido para cada arquivo. No entanto, isso causa problemas para aplicativos que codificam informações importantes em nomes de arquivos longos.

Portanto, se você estiver compartilhando um arquivo entre clientes em sistemas operacionais diferentes, você deve usar caracteres nos nomes de arquivo que são válidos em ambos os sistemas operacionais.

No entanto, se você tiver clientes NFS que criam nomes de arquivo contendo caracteres que não são nomes de arquivo válidos para clientes SMB, você poderá definir um mapa que converte os caracteres NFS inválidos em caracteres Unicode que tanto SMB quanto determinados aplicativos do Windows aceitam. Por exemplo, essa funcionalidade suporta os aplicativos CATIA MCAD e Mathematica, bem como outros aplicativos que têm esse requisito.

Você pode configurar o mapeamento de caracteres em uma base volume por volume.

Você deve ter em mente o seguinte ao configurar o mapeamento de caracteres em um volume:

- O mapeamento de caracteres não é aplicado em pontos de junção.

Você deve configurar explicitamente o mapeamento de caracteres para cada volume de junção.

- Você deve certificar-se de que os caracteres Unicode que são usados para representar caracteres inválidos ou ilegais são caracteres que normalmente não aparecem em nomes de arquivos; caso contrário, mapeamentos indesejados ocorrem.

Por exemplo, se você tentar mapear dois pontos (:) para um hífen (-), mas o hífen (-) foi usado no nome do arquivo corretamente, um cliente Windows tentando acessar um arquivo chamado "a-b" teria sua solicitação mapeada para o nome NFS de "a:b" (não o resultado desejado).

- Depois de aplicar o mapeamento de caracteres, se o mapeamento ainda contiver um caractere Windows inválido, o ONTAP volta para os nomes de arquivos do Windows 8,3.
- Em notificações FPolicy, logs de auditoria nas e mensagens de rastreamento de segurança, os nomes de arquivo mapeados são exibidos.
- Quando uma relação SnapMirror do tipo DP é criada, o mapeamento de caracteres do volume de origem não é replicado no volume DP de destino.
- Sensibilidade do caso: Como os nomes mapeados do Windows se transformam em nomes NFS, a pesquisa dos nomes segue semântica de NFS. Isso inclui o fato de que pesquisas NFS são sensíveis a maiúsculas e minúsculas. Isso significa que os aplicativos que acessam compartilhamentos mapeados não devem depender de comportamento insensível a maiúsculas e minúsculas do Windows. No entanto, o nome 8,3 está disponível, e isso é insensível a maiúsculas e minúsculas.
- Mapeamentos parciais ou inválidos: Depois de mapear um nome para retornar aos clientes fazendo enumeração de diretórios ("dir"), o nome Unicode resultante é verificado para a validade do Windows. Se esse nome ainda tiver caracteres inválidos nele, ou se for inválido para o Windows (por exemplo, termina em "." ou em branco), o nome 8,3 será retornado em vez do nome inválido.

Passo

1. Configurar mapeamento de caracteres

```
vserver cifs character-mapping create -vserver vserver_name -volume volume_name
-mapping mapping_text, ...E
```

O mapeamento consiste em uma lista de pares de caracteres fonte-alvo separados por ":". Os caracteres são caracteres Unicode inseridos usando dígitos hexadecimais. Por exemplo: 3c:E03C. E

O primeiro valor de cada *mapping_text* par que é separado por dois pontos é o valor hexadecimal do caractere NFS que você deseja traduzir, e o segundo valor é o valor Unicode que SMB usa. Os pares de mapeamento devem ser únicos (deve existir um mapeamento um-para-um).

- Mapeamento de origem

A tabela a seguir mostra o conjunto de caracteres Unicode permissível para mapeamento de fontes:

E

Caractere Unicode	Caráter impresso	Descrição
0x01-0x19	Não aplicável	Caracteres de controle não-impressão
0x5C		Barra invertida

Caractere Unicode	Caráter impresso	Descrição
0x3A	:	Cólon
0x2A	*	Asterisco
0x3F	?	Ponto de interrogação
0x22	"	Marca de cotação
0x3C	<	Menos de
0x3E	>	Superior a.
0x7C		
Linha vertical	0xB1	±

- Mapeamento de alvos

Você pode especificar caracteres de destino na ""Área de uso privado"" do Unicode no seguinte intervalo: U-E0000...U-F8FF.

Exemplo

O comando a seguir cria um mapeamento de caracteres para um volume chamado "data" na máquina virtual de armazenamento (SVM) VS1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show
```

Vserver	Volume Name	Character Mapping
vs1	data	3c:e17c, 3e:f17d, 2a:f745

Informações relacionadas

[Criação e gerenciamento de volumes de dados em namespaces nas](#)

Comandos para gerenciar mapeamentos de caracteres para a tradução de nome de arquivo SMB

É possível gerenciar o mapeamento de caracteres criando, modificando, exibindo informações ou excluindo mapeamentos de caracteres de arquivo usados para a tradução de nomes de arquivo SMB em volumes FlexVol.

Se você quiser...	Use este comando...
Criar novos mapeamentos de caracteres de arquivo	<code>vserver cifs character-mapping create</code>
Exibir informações sobre mapeamentos de caracteres de arquivo	<code>vserver cifs character-mapping show</code>
Modificar mapeamentos de caracteres de arquivo existentes	<code>vserver cifs character-mapping modify</code>
Excluir mapeamentos de caracteres de arquivo	<code>vserver cifs character-mapping delete</code>

Para obter mais informações, consulte a página man para cada comando.

Informações relacionadas

[Configurando o mapeamento de caracteres para a tradução de nome de arquivo SMB em volumes](#)

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.