Configure o acesso a arquivos usando SMB

ONTAP 9

NetApp
January 17, 2025

Índice

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	Clientes que podem modificar permissões	Permissões que os clientes podem usar	Estilo de segurança eficaz resultante	Clientes 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 volumesconsulte .

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	• 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	• 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	`volume create` e inclua o `-security-style` parâmetro para especificar o estilo de segurança.
Já existe	`volume modify` e inclua o `-security-style` 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	`volume qtree create` e inclua o `-security -style` parâmetro para especificar o estilo de segurança.
Já existe	`volume qtree modify` e inclua o `-security -style` 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 carateres não podem ser usados no caminho de junção: * *
>
> Além disso, o comprimento do caminho de junção não pode ter mais de 255 carateres.

Passos

1. Crie o volume com um ponto de junção: `volume create -vserver` *`vserver_name`* `-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` *`vserver_name`* `-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
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   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	`volume mount -vserver svm_name -volume volume_name -junction-path junction_path`

Desmontar um volume	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

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	`volume show -vserver vserver_name -junction`
Informações detalhadas sobre volumes montados e não montados no SVM	`volume show -vserver vserver_name -volume volume_name -instance`

Se você quiser exibir…	Digite o comando…
Informações específicas sobre volumes montados e não montados no SVM	a. Se necessário, você pode exibir campos válidos para o `-fields` parâmetro usando o seguinte comando: `volume show -fields ?` b. Exiba as informações desejadas usando o `-fields` parâmetro: Volume show -vserver vserver_name -fieldname,…

Exemplos

O exemplo a seguir exibe um resumo dos volumes montados e não montados no SVM VS1:

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
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 conetando 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 ative 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	• 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
*	• *	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. O padrão* é válido apenas para mapeamento de nomes do UNIX para o Windows, e não para o contrário.

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 carateres 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	`vserver cifs options modify -default -unix-user` *`user_name`*
Configure o usuário padrão do Windows	`vserver nfs modify -default-win-user` *`user_name`*

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	`vserver name-mapping create`
Insira um mapeamento de nomes em uma posição específica	`vserver name-mapping insert`
Exibir mapeamentos de nomes	`vserver name-mapping show`

Se você quiser…	Use este comando…
Troque a posição de dois mapeamentos de nomes Uma troca não é permitida quando o mapeamento de nomes é configurado com uma entrada de qualificador ip.	`vserver name-mapping swap`
Modificar um mapeamento de nomes	`vserver name-mapping modify`
Eliminar um mapeamento de nomes	`vserver name-mapping delete`
Valide o mapeamento de nomes correto	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

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	`vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled true`
Desativado	`vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled false`

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	`vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...`
Remova domínios confiáveis da lista	`vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]`
Modifique a lista existente	`vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...`

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)	`vserver cifs domain name-mapping-search show`
Todos os domínios confiáveis preferenciais para um SVM especificado	`vserver cifs domain name-mapping-search show -vserver` *`vserver_name`*

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 carateres 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 caraterísticas da participação:

- O caminho para esse compartilhamento é sempre o caminho para o volume raiz da SVM e não pode ser modificado.
- A 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 carateres.
- 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 carateres especiais são suportados quando você nomeia compartilhamentos SMB:

  ! A % e ' _ - . Clique em "OK"

- Os seguintes carateres 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 conete 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.
`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 *Access Based Enumeração* (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 aceder a dados SMB não poderão aceder 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 removem, permanecem em vigor.

Passos

1. Introduza o comando adequado:

Se você quiser…	Digite o comando…
Adicione propriedades de compartilhamento	`vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`
Remover propriedades de compartilhamento	`vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`

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 carateres (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 carateres.

   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 conetar 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 conetar 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 coneta 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 conetar 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	`vserver cifs share create`
Exibir compartilhamentos SMB	`vserver cifs share show`
Modificar um compartilhamento SMB	`vserver cifs share modify`
Excluir um compartilhamento SMB	`vserver cifs share delete`
Adicione propriedades de compartilhamento a um compartilhamento existente	`vserver cifs share properties add`
Remover propriedades de compartilhamento de um compartilhamento existente	`vserver cifs share properties remove`
Exibir informações sobre as propriedades de compartilhamento	`vserver cifs share properties show`

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	`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>`

Se você quiser configurar ACLs usando um…	Digite o comando…
Grupo Windows	`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>`
Utilizador UNIX	`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>`
Grupo UNIX	`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>`

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
                Share       User/Group              User/Group  Access
Vserver         Name        Name                    Type
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::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com
                Share       User/Group               User/Group  Access
Vserver         Name        Name                     Type
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::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

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

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
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	`vserver cifs share access-control create`
Exibir ACLs	`vserver cifs share access-control show`
Modificar uma ACL	`vserver cifs share access-control modify`
Eliminar uma ACL	`vserver cifs share access-control delete`

Proteja o acesso aos arquivos usando permissões de arquivo

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

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

Antes de começar

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

Sobre esta tarefa

A configuração de permissões de arquivos NTFS é feita em um host do Windows adicionando entradas a listas de controle de acesso discricionárias (DACLs) NTFS associadas a um descritor de segurança NTFS. O descritor de segurança é então aplicado a arquivos e diretórios NTFS. Essas tarefas são tratadas automaticamente pela GUI do Windows.

Passos

1. No menu **Ferramentas** no Windows Explorer, selecione **Mapear unidade de rede**.
2. Preencha a caixa de diálogo **Map Network Drive**:

   a. Selecione uma letra **Drive**.

   b. Na caixa **pasta**, digite o nome do servidor CIFS que contém o compartilhamento que contém os dados aos quais você deseja aplicar permissões e o nome do compartilhamento.

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

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

   c. Clique em **Finish**.

A unidade selecionada está montada e pronta com a janela do Windows Explorer exibindo arquivos e pastas contidos no compartilhamento.

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

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

6. Clique em **Avançado**.

   A janela Propriedades do Windows exibe informações sobre permissões de arquivo existentes atribuídas a usuários e grupos.

7. Clique em **alterar permissões**.

   A janela permissões é aberta.

8. Execute as ações desejadas:

Se você quiser…	Faça o seguinte…
Configurar permissões NTFS avançadas para um novo utilizador ou grupo	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	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	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 conetar aos dados usando um compartilhamento SMB em um cliente Windows.

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

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

Passos

1. Crie um descritor de segurança NTFS.

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

2. Adicione DACLs ao descritor de segurança NTFS.

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

```
{this-folder|sub-folders|files}
```

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

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

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

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

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

- Permissões de exportação

  Configurar permissões de exportação para o acesso SMB é opcional.

- Permissões de compartilhamento
- Permissões de arquivo

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

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

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

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

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 analógico 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 impactos 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 impactos de uma alteração de política de acesso antes de realmente colocar a política em jogo. Depois de avaliar o impactos 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

Exibindo informações sobre a segurança do controle de acesso dinâmico

"Auditoria de SMB e NFS e rastreamento de segurança"

Funcionalidade de controlo 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 ative Directory.

Suportado para controlo de acesso dinâmico

O ONTAP suporta a seguinte funcionalidade quando o controlo 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 ative 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.

Funcionalidade	Comentários
Suporte para exibir informações sobre a segurança da diretiva de acesso central usando a CLI do ONTAP	Estende o `vserver security file-directory show` comando para exibir informações sobre políticas de acesso centrais aplicadas.
Rastreamento de segurança que inclui políticas de acesso central	Estende a `vserver security trace` família de comandos para exibir resultados que incluem informações sobre políticas de acesso central aplicadas.

Não suportado para o controlo de acesso dinâmico

O ONTAP não suporta a seguinte funcionalidade quando o controlo 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 controlo de Acesso Dinâmico

A opção que permite utilizar o controlo 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 controlo 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 controlo de Acesso Dinâmico estiver desativado, as entradas atuais do controlo 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	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled true`
Desativado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled false`

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 controlo de acesso dinâmico ser desativado, não é possível remover os ACEs de controlo de

acesso não dinâmico existentes nem adicionar novos ACEs de controlo de acesso não dinâmico até ter removido os ACEs de controlo 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 ative Directory, aplicar as políticas de acesso central a contentores do ative Directory com GPOs e habilitar GPOs no servidor CIFS.

Antes de começar

- O ative Directory deve ser configurado para usar políticas de acesso central.
- Você precisa ter acesso suficiente nos controladores de domínio do ative 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 ative Directory.
4. Crie um objeto de diretiva de grupo (GPO) para implantar as políticas de acesso central no ative 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:
             /vol1/home
             /vol1/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:
        /vol1/home
        /vol1/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 controlo de acesso dinâmico

Apresentar informações sobre a segurança do controlo de acesso dinâmico

Pode apresentar informações sobre a segurança do controlo 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	`vserver security file-directory show -vserver vserver_name -path path`
Com detalhes expandidos	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
Onde a saída é exibida com SIDs de grupo e usuário	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
Sobre segurança de arquivos e diretórios para arquivos e diretórios onde a máscara de bits hexadecimal é traduzida para o formato textual	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

Exemplos

O exemplo a seguir exibe informações de segurança do Dynamic Access Control sobre o caminho `/vol1` 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 controlo de Acesso Dinâmico são ignorados após a reversão, o acesso aos ficheiros será alterado nos ficheiros com ACEs do controlo 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 controlo de Acesso Dinâmico são ignorados após a reversão, não é necessário removê-los ao aplicar ACEs do controlo de Acesso não Dinâmico aos ficheiros 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 carateres.

- 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: cifsnfs1
- 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
cifsnfs1 -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 excecional 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

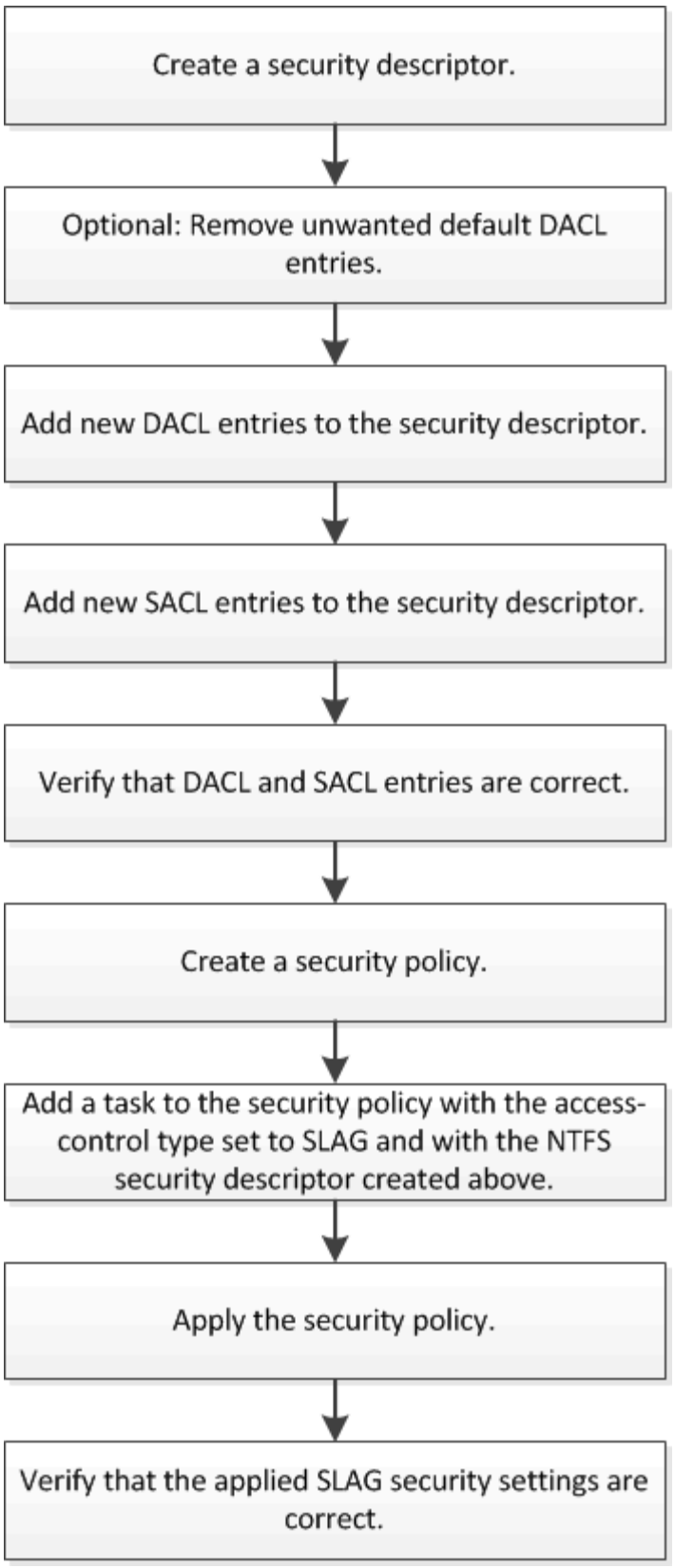
O Storage-Level Access Guard fornece segurança adicional no nível de armazenamento, que não é visível do lado do cliente; portanto, ele não pode ser revogado por nenhum dos usuários ou administradores de seus desktops. Há certos casos de uso em que a capacidade de controlar o acesso no nível de storage é benéfica.

Os casos de uso típicos para esse recurso incluem os seguintes cenários:

- Proteção da propriedade intelectual através da auditoria e controlo 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    Owner Name
      Descriptor 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   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       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 DACA ACE 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`, respetivamente.

   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	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Com detalhes expandidos	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

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 `/datavol5` 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
```

Remova 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
```

Informações sobre direitos autorais

Informações sobre marcas comerciais