Configure o SMB com a CLI

ONTAP 9

NetApp
January 17, 2025

Índice

Configure o SMB com a CLI

Visão geral da configuração SMB com a CLI

Você pode usar os comandos de CLI do ONTAP 9 para configurar o acesso de cliente SMB a arquivos contidos em um novo volume ou qtree em um SVM novo ou existente.

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

Use estes procedimentos se quiser configurar o acesso SMB a um volume ou qtree da seguinte maneira:

- Você deseja usar SMB versão 2 ou posterior.
- Você deseja atender apenas clientes SMB, não clientes NFS (não uma configuração multiprotocolo).
- As permissões de arquivo NTFS serão usadas para proteger o novo volume.
- Você tem o administrador de clusters Privileges, e não o Privileges do administrador da SVM.

  Os Privileges do administrador de cluster são necessários para criar SVMs e LIFs. Os Privileges de administrador do SVM são suficientes para outras tarefas de configuração de SMB.

- Você deseja usar a CLI, não o System Manager ou uma ferramenta de script automatizado.

  Para usar o System Manager para configurar o acesso multiprotocolo nas, "Provisionar storage nas para Windows e Linux usando NFS e SMB"consulte .

- Você quer usar as práticas recomendadas, não explorar todas as opções disponíveis.

  Detalhes sobre a sintaxe de comando estão disponíveis nas páginas de ajuda CLI e man do ONTAP.

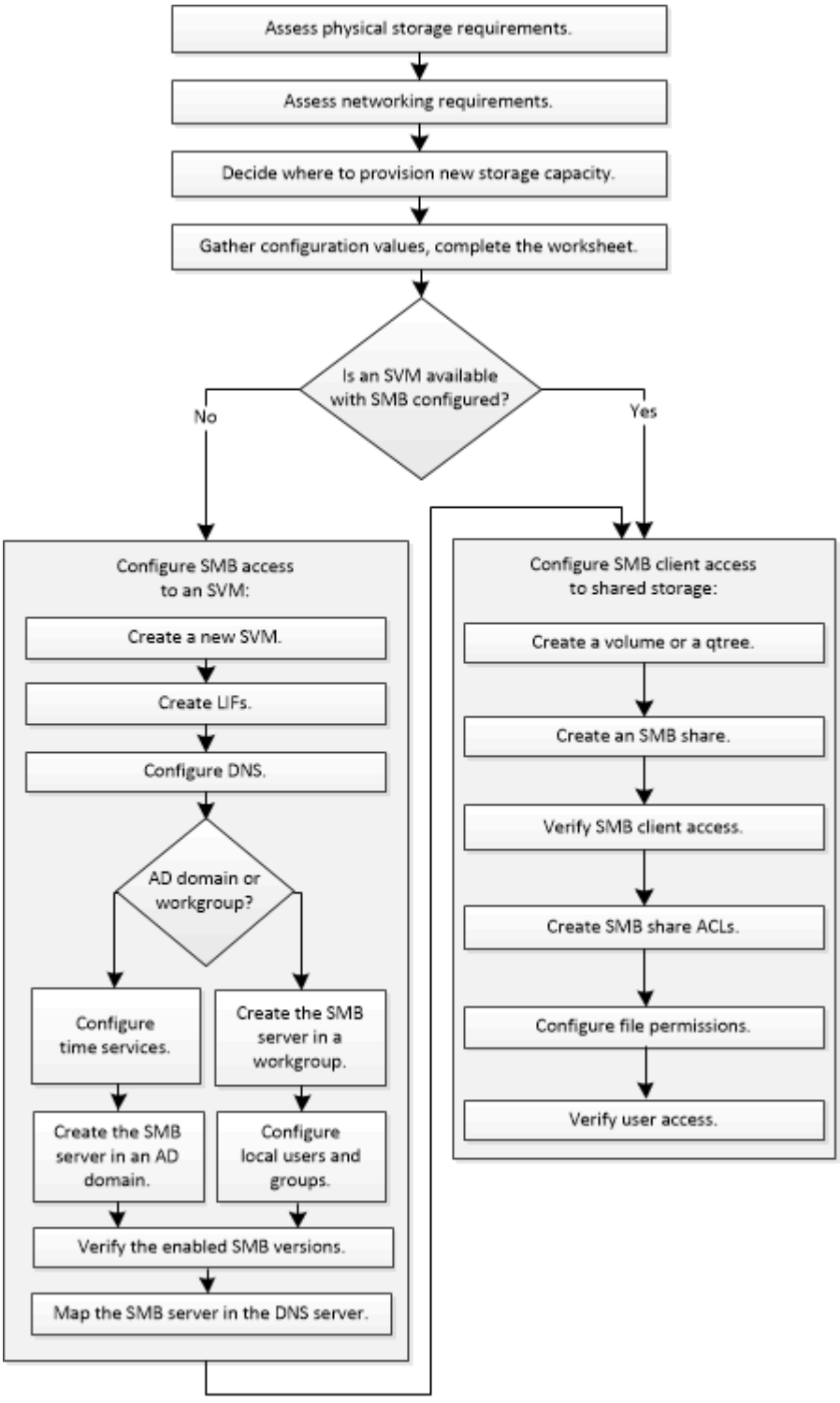
Se pretender obter detalhes sobre a gama de capacidades do protocolo SMB do ONTAP, consulte o "Visão geral de referência SMB".

Outras maneiras de fazer isso em ONTAP

Para executar estas tarefas com…	Consulte…
O Gerenciador de sistema redesenhado (disponível com o ONTAP 9.7 e posterior)	"Provisione storage nas para servidores Windows usando SMB"
System Manager Classic (disponível com o ONTAP 9.7 e versões anteriores)	"Visão geral da configuração SMB"

Fluxo de trabalho de configuração SMB

A configuração do SMB envolve a avaliação dos requisitos de storage físico e rede e, depois, a escolha de um fluxo de trabalho específico para sua meta; a configuração do acesso SMB a uma SVM nova ou existente ou a adição de um volume ou qtree a uma SVM existente que já esteja totalmente configurada para acesso SMB.



Preparação

Avaliar os requisitos de armazenamento físico

Antes de provisionar o storage SMB para clientes, você deve garantir que haja espaço suficiente em um agregado existente para o novo volume. Se não houver, você poderá adicionar discos a um agregado existente ou criar um novo agregado do tipo desejado.

Passos

1. Exibir espaço disponível em agregados existentes: `storage aggregate show`

   Se houver um agregado com espaço suficiente, Registre seu nome na Planilha.

```
cluster::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                        normal
aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                        normal
6 entries were displayed.
```

2. Se não houver agregados com espaço suficiente, adicione discos a um agregado existente usando o `storage aggregate add-disks` comando ou crie um novo agregado usando o `storage aggregate create` comando.

Avaliar os requisitos de rede

Antes de fornecer armazenamento SMB aos clientes, você deve verificar se a rede está configurada corretamente para atender aos requisitos de provisionamento SMB.

Antes de começar

Os seguintes objetos de rede de cluster devem ser configurados:

- Portas físicas e lógicas
- Domínios de broadcast
- Sub-redes (se necessário)
- IPspaces (conforme necessário, além do IPspace padrão)
- Grupos de failover (conforme necessário, além do grupo de failover padrão para cada domínio de broadcast)
- Firewalls externos

Passos

1. Exiba as portas físicas e virtuais disponíveis: `network port show`
   - Quando possível, você deve usar a porta com a velocidade mais alta para a rede de dados.

- Todos os componentes da rede de dados devem ter a mesma configuração de MTU para obter o melhor desempenho.

2. Se você estiver planejando usar um nome de sub-rede para alocar o endereço IP e o valor de máscara de rede para um LIF, verifique se a sub-rede existe e tem endereços suficientes disponíveis: `network subnet show`

   As sub-redes contêm um conjunto de endereços IP que pertencem à mesma sub-rede da camada 3. As sub-redes são criadas usando o `network subnet create` comando.

3. Exibir IPspaces disponíveis: `network ipspace show`

   Você pode usar o IPspace padrão ou um IPspace personalizado.

4. Se você quiser usar endereços IPv6, verifique se IPv6 está ativado no cluster: `network options ipv6 show`

   Se necessário, você pode ativar o IPv6 usando o `network options ipv6 modify` comando.

Decida onde provisionar nova capacidade de storage SMB

Antes de criar um novo volume ou qtree SMB, você precisa decidir se deve colocá-lo em uma SVM nova ou existente e quanto de configuração o SVM precisa. Esta decisão determina o seu fluxo de trabalho.

Opções

- Se você quiser provisionar um volume ou qtree em um novo SVM ou em um SVM existente que tenha o SMB habilitado, mas não configurado, execute as etapas em ""Configurando o acesso SMB a um SVM"" e "adicionando capacidade de storage a um SVM habilitado para SMB".

  Configurando o acesso SMB a uma SVM

  Configurando o acesso de cliente SMB ao armazenamento compartilhado

  Você pode optar por criar um novo SVM se uma das seguintes opções for verdadeira:

  - Você está habilitando o SMB em um cluster pela primeira vez.
  - Você tem SVMs existentes em um cluster no qual não deseja ativar o suporte a SMB.
  - Você tem um ou mais SVMs habilitados para SMB em um cluster e deseja uma das seguintes conexões:
    - Para uma floresta ou grupo de trabalho diferente do ative Directory.
    - Para um servidor SMB em um namespace isolado (cenário de alocação a vários clientes). Você também deve escolher essa opção para provisionar storage em uma SVM existente que tenha SMB habilitado, mas não configurado. Esse pode ser o caso se você criou o SVM para acesso à SAN ou se nenhum protocolo foi habilitado quando o SVM foi criado.

  Depois de ativar o SMB no SVM, proceda ao provisionamento de um volume ou qtree.

- Se você quiser provisionar um volume ou qtree em um SVM existente totalmente configurado para acesso SMB, execute as etapas em ""adicionando capacidade de storage a um SVM habilitado para SMB"".

  Configurando o acesso de cliente SMB ao armazenamento compartilhado

Folha de cálculo para recolher informações de configuração SMB

A folha de cálculo de configuração SMB permite-lhe recolher as informações necessárias para configurar o acesso SMB para clientes.

Você deve completar uma ou ambas as seções da Planilha, dependendo da decisão tomada sobre onde provisionar o armazenamento:

- Se você estiver configurando o acesso SMB a um SVM, deve concluir ambas as seções.

  Configurando o acesso SMB a uma SVM

  Configurando o acesso de cliente SMB ao armazenamento compartilhado

- Se você estiver adicionando capacidade de storage a uma SVM habilitada para SMB, deverá concluir apenas a segunda seção.

  Configurando o acesso de cliente SMB ao armazenamento compartilhado

As páginas de manual do comando contêm detalhes sobre os parâmetros.

Configurando o acesso SMB a uma SVM

Parâmetros para criar um SVM

Você fornece esses valores com o `vserver create` comando se estiver criando um novo SVM.

Campo	Descrição	O seu valor
`-vserver`	Nome fornecido para o novo SVM que é um nome de domínio totalmente qualificado (FQDN) ou que segue outra convenção que impõe nomes exclusivos de SVM em um cluster.	
`-aggregate`	O nome de um agregado no cluster com espaço suficiente para a nova capacidade de armazenamento SMB.	
`-rootvolume`	Um nome exclusivo fornecido para o volume raiz da SVM.	
`-rootvolume-security-style`	Use o estilo de segurança NTFS para o SVM.	`ntfs`
`-language`	Use a configuração de idioma padrão neste fluxo de trabalho.	`C.UTF-8`

Campo	Descrição	O seu valor
`ipspace`	Opcional: Os IPspaces são espaços de endereço IP distintos nos quais os SVMs residem.	

Parâmetros para criar um LIF

Você fornece esses valores com o `network interface create` comando quando você está criando LIFs.

Campo	Descrição	O seu valor
`-lif`	Um nome que você fornece para o novo LIF.	
`-role`	Use a função de LIF de dados neste fluxo de trabalho.	`data`
`-data-protocol`	Utilize apenas o protocolo SMB neste fluxo de trabalho.	`cifs`
`-home-node`	O nó ao qual o LIF retorna quando o `network interface revert` comando é executado no LIF.	
`-home-port`	A porta ou grupo de interface para o qual o LIF retorna quando o `network interface revert` comando é executado no LIF.	
`-address`	O endereço IPv4 ou IPv6 no cluster que será usado para acesso aos dados pelo novo LIF.	
`-netmask`	A máscara de rede e o gateway para o LIF.	
`-subnet`	Um conjunto de endereços IP. Usado em vez `-address` de e `-netmask` para atribuir endereços e netmasks automaticamente.	
`-firewall-policy`	Use a política de firewall de dados padrão neste fluxo de trabalho.	`data`

Campo	Descrição	O seu valor
`-auto-revert`	Opcional: Especifica se um LIF de dados é automaticamente revertido para seu nó inicial na inicialização ou em outras circunstâncias. A predefinição é `false`.	

Parâmetros para resolução de nome de host DNS

Você fornece esses valores com o `vserver services name-service dns create` comando quando você está configurando o DNS.

Campo	Descrição	O seu valor
`-domains`	Até cinco nomes de domínio DNS.	
`-name-servers`	Até três endereços IP para cada servidor de nomes DNS.	

Configurando um servidor SMB em um domínio do ative Directory

Parâmetros para configuração do serviço de tempo

Você fornece esses valores com o `cluster time-service ntp server create` comando quando você está configurando serviços de tempo.

Campo	Descrição	O seu valor
`-server`	O nome do host ou o endereço IP do servidor NTP para o domínio do ative Directory.	

Parâmetros para criar um servidor SMB em um domínio do ative Directory

Você fornece esses valores com o `vserver cifs create` comando ao criar um novo servidor SMB e especificar informações de domínio.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM no qual criar o servidor SMB.	
`-cifs-server`	O nome do servidor SMB (até 15 carateres).	

Campo	Descrição	O seu valor
`-domain`	O nome de domínio totalmente qualificado (FQDN) do domínio do ative Directory a associar ao servidor SMB.	
`-ou`	Opcional: A unidade organizacional dentro do domínio do ative Directory a associar ao servidor SMB. Por padrão, este parâmetro é definido como computadores.	
`-netbios-aliases`	Opcional: Uma lista de aliases NetBIOS, que são nomes alternativos ao nome do servidor SMB.	
`-comment`	Opcional: Um comentário de texto para o servidor. Os clientes Windows podem ver esta descrição do servidor SMB ao navegar em servidores na rede.	

Configurando um servidor SMB em um grupo de trabalho

Parâmetros para criar um servidor SMB em um grupo de trabalho

Você fornece esses valores com o `vserver cifs create` comando ao criar um novo servidor SMB e especificar versões SMB compatíveis.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM no qual criar o servidor SMB.	
`-cifs-server`	O nome do servidor SMB (até 15 carateres).	
`-workgroup`	O nome do grupo de trabalho (até 15 carateres).	
`-comment`	Opcional: Um comentário de texto para o servidor. Os clientes Windows podem ver esta descrição do servidor SMB ao navegar em servidores na rede.	

Parâmetros para criar usuários locais

Você fornece esses valores ao criar usuários locais usando o `vserver cifs users-and-groups local-user create` comando. Eles são necessários para servidores SMB em grupos de trabalho e opcionais em domínios do AD.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM no qual criar o usuário local.	
`-user-name`	O nome do utilizador local (até 20 carateres).	
`-full-name`	Opcional: O nome completo do usuário. Se o nome completo contiver um espaço, insira o nome completo entre aspas duplas.	
`-description`	Opcional: Uma descrição para o usuário local. Se a descrição contiver um espaço, coloque o parâmetro entre aspas.	
`-is-account-disabled`	Opcional: Especifica se a conta de usuário está ativada ou desativada. Se este parâmetro não for especificado, o padrão é ativar a conta de usuário.	

Parâmetros para criar grupos locais

Você fornece esses valores ao criar grupos locais usando o `vserver cifs users-and-groups local-group create` comando. Eles são opcionais para servidores SMB em domínios e grupos de trabalho do AD.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM no qual criar o grupo local.	
`-group-name`	O nome do grupo local (até 256 carateres).	
`-description`	Opcional: Uma descrição para o grupo local. Se a descrição contiver um espaço, coloque o parâmetro entre aspas.	

Adição de capacidade de storage a uma SVM habilitada para SMB

Parâmetros para criar um volume

Você fornece esses valores com o `volume create` comando se estiver criando um volume em vez de uma qtree.

Campo	Descrição	O seu valor
`-vserver`	Nome de uma SVM nova ou existente que hospedará o novo volume.	
`-volume`	Um nome descritivo exclusivo que você fornece para o novo volume.	
`-aggregate`	O nome de um agregado no cluster com espaço suficiente para o novo volume SMB.	
`-size`	Um número inteiro fornecido para o tamanho do novo volume.	
`-security-style`	Utilize o estilo de segurança NTFS para este fluxo de trabalho.	`ntfs`
`-junction-path`	Localização sob a raiz (/) onde o novo volume deve ser montado.	

Parâmetros para criar uma qtree

Você fornece esses valores com o `volume qtree create` comando se estiver criando uma qtree em vez de um volume.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM no qual reside o volume que contém a qtree.	
`-volume`	O nome do volume que conterá a nova qtree.	
`-qtree`	Um nome descritivo exclusivo que você fornece para a nova qtree, 64 carateres ou menos.	
`-qtree-path`	O argumento de caminho de qtree no formato `/vol/volume_name/qtree_name\>` pode ser especificado em vez de especificar volume e qtree como argumentos separados.	

Parâmetros para criar compartilhamentos SMB

Você fornece esses valores com o `vserver cifs share create` comando.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM no qual criar o compartilhamento SMB.	
`-share-name`	O nome do compartilhamento SMB que você deseja criar (até 256 carateres).	
`-path`	O nome do caminho para o compartilhamento SMB (até 256 carateres). Esse caminho deve existir em um volume antes de criar o compartilhamento.	
`-share-properties`	Opcional: Uma lista de propriedades de compartilhamento. As predefinições são `oplocks`, `browsable`, `changenotify` e `show-previous-versions`.	
`-comment`	Opcional: Um comentário de texto para o servidor (até 256 carateres). Os clientes Windows podem ver esta descrição do compartilhamento SMB ao navegar na rede.	

Parâmetros para criar listas de controle de acesso (ACLs) de compartilhamento SMB

Você fornece esses valores com o `vserver cifs share access-control create` comando.

Campo	Descrição	O seu valor
`-vserver`	O nome da SVM no qual criar a ACL SMB.	
`-share`	O nome do compartilhamento SMB no qual criar.	
`-user-group-type`	O tipo de usuário ou grupo a ser adicionado à ACL do compartilhamento. O tipo padrão é `windows`	`windows`

Campo	Descrição	O seu valor
`-user-or-group`	O usuário ou grupo a adicionar à ACL do compartilhamento. Se você especificar o nome de usuário, você deve incluir o domínio do usuário usando o formato "nome de usuário".	
`-permission`	Especifica as permissões para o usuário ou grupo.	`[No_access
Read	Change	Full_Control]`

Configurar o acesso SMB a uma SVM

Configurar o acesso SMB a uma SVM

Se você ainda não tiver um SVM configurado para acesso de cliente SMB, crie e configure um novo SVM ou configure um SVM existente. A configuração do SMB envolve a abertura do acesso ao volume raiz do SVM, a criação de um servidor SMB, a criação de um LIF, a ativação da resolução do nome de host, a configuração de serviços de nome e, se desejado, a ativação da segurança Kerberos.

Criar um SVM

Se você ainda não tiver pelo menos um SVM em um cluster para fornecer acesso aos dados a clientes SMB, será necessário criar um.

Antes de começar

- A partir do ONTAP 9.13,1, é possível definir uma capacidade máxima para uma VM de armazenamento. Você também pode configurar alertas quando o SVM se aproximar de um nível de capacidade limite. Para obter mais informações, Gerenciar a capacidade do SVMconsulte .

Passos

1. Criar um SVM: `vserver create -vserver` *`svm_name`* `-rootvolume` *`root_volume_name`* `-aggregate` *`aggregate_name`* `-rootvolume-security-style ntfs -language C.UTF-8 -ipspace` *`ipspace_name`*
   - Utilize a definição NTFS para a `-rootvolume-security-style` opção.
   - Utilize a opção C.UTF-8 predefinida `-language`.
   - A `ipspace` definição é opcional.
2. Verifique a configuração e o status do SVM recém-criado: `vserver show -vserver` *`vserver_name`*

   O `Allowed Protocols` campo deve incluir CIFS. Você pode editar esta lista mais tarde.

   O `Vserver Operational State` campo tem de apresentar o `running` estado. Se ele exibir `initializing` o estado, isso significa que alguma operação intermediária, como criação de volume raiz,

falhou e você deve excluir o SVM e recriá-lo.

Exemplos

O comando a seguir cria um SVM para acesso a dados no IPspace : `ipspaceA`

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

O comando a seguir mostra que um SVM foi criado com um volume raiz de 1 GB, que foi iniciado automaticamente e está `running` no estado. O volume raiz tem uma política de exportação padrão que não inclui nenhuma regra, portanto, o volume raiz não é exportado após a criação.

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                               Vserver Type: data
                            Vserver Subtype: default
                               Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                 NIS Domain: -
                  Root Volume Security Style: ntfs
                                 LDAP Client: -
                Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                               Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                        Vserver Admin State: running
                  Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                               IPspace Name: ipspaceA
```

A partir do ONTAP 9.13,1, é possível definir um modelo de grupo de políticas de QoS adaptável, aplicando um limite mínimo de taxa de transferência e limite máximo a volumes no SVM. Só é possível aplicar essa política depois de criar o SVM. Para saber mais sobre esse processo, Defina um modelo de grupo de políticas adaptávelconsulte .

Verifique se o protocolo SMB está ativado na SVM

Antes de poder configurar e utilizar SMB em SVMs, tem de verificar se o protocolo está ativado.

Sobre esta tarefa

Isso geralmente é feito durante a configuração do SVM, mas se você não ativou o protocolo durante a configuração, poderá ativá-lo mais tarde usando o `vserver add-protocols` comando.

Não é possível adicionar ou remover um protocolo de um LIF depois de criado.

Você também pode desativar protocolos em SVMs usando o `vserver remove-protocols` comando.

Passos

1. Verifique quais protocolos estão atualmente ativados e desativados para o SVM: `vserver show -vserver vserver_name -protocols`

   Você também pode usar o `vserver show-protocols` comando para exibir os protocolos atualmente habilitados em todos os SVMs no cluster.

2. Se necessário, ative ou desative um protocolo:
   - Para ativar o protocolo SMB: `vserver add-protocols -vserver vserver_name -protocols cifs`
   - Para desativar um protocolo: `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`
3. Confirme se os protocolos ativados e desativados foram atualizados corretamente: `vserver show -vserver vserver_name -protocols`

Exemplo

O comando a seguir exibe quais protocolos estão atualmente ativados e desativados (permitidos e não permitidos) no SVM chamado VS1:

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    -----------------------
vs1.example.com   cifs                       nfs, fcp, iscsi, ndmp
```

O comando a seguir permite o acesso por SMB adicionando `cifs` à lista de protocolos habilitados no SVM chamado VS1:

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

Abra a política de exportação do volume raiz da SVM

A política de exportação padrão do volume raiz da SVM deve incluir uma regra para permitir que todos os clientes tenham acesso aberto por meio do SMB. Sem essa regra, todos os clientes SMB têm acesso negado ao SVM e seus volumes.

Sobre esta tarefa

Quando um novo SVM é criado, uma política de exportação padrão (chamada padrão) é criada automaticamente para o volume raiz do SVM. Você deve criar uma ou mais regras para a política de exportação padrão antes que os clientes possam acessar os dados no SVM.

Você deve verificar se todo o acesso SMB está aberto na política de exportação padrão e, mais tarde, restringir o acesso a volumes individuais criando políticas de exportação personalizadas para volumes individuais ou qtrees.

Passos

1. Se você estiver usando uma SVM existente, verifique a política de exportação de volume raiz padrão: `vserver export-policy rule show`

   A saída do comando deve ser semelhante ao seguinte:

   ```
   cluster::> vserver export-policy rule show -vserver vs1.example.com
   -policyname default -instance

                                      Vserver: vs1.example.com
                                  Policy Name: default
                                   Rule Index: 1
                              Access Protocol: cifs
   Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                                RO Access Rule: any
                                RW Access Rule: any
   User ID To Which Anonymous Users Are Mapped: 65534
                     Superuser Security Types: any
                 Honor SetUID Bits in SETATTR: true
                    Allow Creation of Devices: true
   ```

   Se existir uma regra que permita o acesso aberto, esta tarefa está concluída. Caso contrário, avance para o passo seguinte.

2. Crie uma regra de exportação para o volume raiz da SVM: `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. Verifique a criação de regras usando o `vserver export-policy rule show` comando.

Resultados

Qualquer cliente SMB agora pode acessar qualquer volume ou qtree criado no SVM.

Crie um LIF

Um LIF é um endereço IP associado a uma porta física ou lógica. Se houver uma falha de componente, um LIF pode falhar ou ser migrado para uma porta física diferente, continuando assim a se comunicar com a rede.

Antes de começar

- A porta de rede física ou lógica subjacente deve ter sido configurada para o status administrativo `up`.
- Se você estiver planejando usar um nome de sub-rede para alocar o endereço IP e o valor de máscara de rede para um LIF, a sub-rede já deve existir.

  As sub-redes contêm um conjunto de endereços IP que pertencem à mesma sub-rede da camada 3. Eles são criados usando o `network subnet create` comando.

- O mecanismo para especificar o tipo de tráfego Tratado por um LIF foi alterado. Para o ONTAP 9.5 e anteriores, LIFs usaram funções para especificar o tipo de tráfego que ele lidaria. A partir do ONTAP 9.6, os LIFs usam políticas de serviço para especificar o tipo de tráfego que ele lidaria.

Sobre esta tarefa

- Você pode criar LIFs IPv4 e IPv6 na mesma porta de rede.
- Se você tiver um grande número de LIFs no cluster, poderá verificar a capacidade de LIF suportada no cluster usando o `network interface capacity show` comando e a capacidade de LIF suportada em cada nó usando o `network interface capacity details show` comando (no nível de privilégio avançado).
- A partir do ONTAP 9.7, se outros LIFs já existirem para o SVM na mesma sub-rede, você não precisará especificar a porta inicial do LIF. O ONTAP escolhe automaticamente uma porta aleatória no nó inicial especificado no mesmo domínio de broadcast que os outros LIFs já configurados na mesma sub-rede.

Passos

1. Criar um LIF:

   `network interface create -vserver` *`vserver_name`* `-lif` *`lif_name`* `-role data -data -protocol cifs -home-node` *`node_name`* `-home-port` *`port_name`* `{-address` *`IP_address`* `-netmask IP_address | -subnet-name` *`subnet_name`*`} -firewall-policy data -auto -revert {true|false}`

ONTAP 9 .5 e anteriores
`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol cifs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*`
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true
false}`

ONTAP 9 1.6 e posterior

`network interface create -vserver *vserver_name* -lif *lif_name* -service-policy *service_policy_name* -home -node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true
false}`

- O `-role` parâmetro não é necessário ao criar um LIF usando uma política de serviço (começando com ONTAP 9.6).
- O `-data-protocol` parâmetro não é necessário ao criar um LIF usando uma política de serviço (começando com ONTAP 9.6). Ao usar o ONTAP 9.5 e anteriores, o `-data-protocol` parâmetro deve ser especificado quando o LIF é criado e não pode ser modificado mais tarde sem destruir e recriar o LIF de dados.
- `-home-node` É o nó para o qual o LIF retorna quando o `network interface revert` comando é executado no LIF.

  Você também pode especificar se o LIF deve reverter automaticamente para o nó inicial e porta inicial com a `-auto-revert` opção.

- `-home-port` É a porta física ou lógica para a qual o LIF retorna quando o `network interface revert` comando é executado no LIF.
- Pode especificar um endereço IP com `-address` as opções e `-netmask` ou ativar a atribuição a partir de uma sub-rede com a `-subnet_name` opção.
- Ao usar uma sub-rede para fornecer o endereço IP e a máscara de rede, se a sub-rede foi definida com um gateway, uma rota padrão para esse gateway é adicionada automaticamente ao SVM quando um LIF é criado usando essa sub-rede.
- Se você atribuir endereços IP manualmente (sem usar uma sub-rede), talvez seja necessário configurar uma rota padrão para um gateway se houver clientes ou controladores de domínio em uma sub-rede IP diferente. A `network route create` página man contém informações sobre a criação de uma rota estática dentro de um SVM.
- Para a `-firewall-policy` opção, use o mesmo padrão `data` que a função LIF.

  Você pode criar e adicionar uma política de firewall personalizada mais tarde, se desejado.

  > A partir do ONTAP 9.10,1, as políticas de firewall são obsoletas e totalmente substituídas por políticas de serviço LIF. Para obter mais informações, "Configurar políticas de firewall para LIFs"consulte .

- `-auto-revert` Permite especificar se um LIF de dados é automaticamente revertido para o seu nó inicial em circunstâncias como inicialização, alterações no status do banco de dados de gerenciamento ou quando a conexão de rede é feita. A configuração padrão é `false`, mas você pode defini-la como `false` dependendo das políticas de gerenciamento de rede em seu ambiente.

2. Verifique se o LIF foi criado com sucesso:

   `network interface show`

3. Verifique se o endereço IP configurado está acessível:

Para verificar um…	Utilizar…

Endereço IPv4	`network ping`
Endereço IPv6	`network ping6`

Exemplos

O comando a seguir cria um LIF e especifica os valores de endereço IP e máscara de rede usando os `-address` parâmetros e `-netmask`:

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol cifs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

O comando a seguir cria um LIF e atribui valores de endereço IP e máscara de rede da sub-rede especificada (chamado client1_sub):

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol cifs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

O comando a seguir mostra todas as LIFs no cluster-1. Os LIFs de dados datalif1 e datalif3 são configurados com endereços IPv4 e o datalif4 é configurado com um endereço IPv6:

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

O comando a seguir mostra como criar um LIF de dados nas atribuído com a `default-data-files` política de serviço:

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

Ative DNS para resolução de nome de host

Você pode usar o `vserver services name-service dns` comando para habilitar o DNS em uma SVM e configurá-lo para usar o DNS para resolução de nome de host. Os

nomes de host são resolvidos usando servidores DNS externos.

Antes de começar

Um servidor DNS em todo o site deve estar disponível para pesquisas de nome de host.

Você deve configurar mais de um servidor DNS para evitar um único ponto de falha. O `vserver services name-service dns create` comando emite um aviso se você inserir apenas um nome de servidor DNS.

Sobre esta tarefa

O *Network Management Guide* contém informações sobre a configuração de DNS dinâmico na SVM.

Passos

1. Habilite o DNS na SVM: `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

   O comando a seguir habilita servidores de servidor DNS externos no SVM VS1:

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   > ⓘ A partir do ONTAP 9.2, o `vserver services name-service dns create` comando executa uma validação automática de configuração e relata uma mensagem de erro se o ONTAP não puder entrar em Contato com o servidor de nomes.

2. Exiba as configurações do domínio DNS usando o `vserver services name-service dns show` comando. ""

   O comando a seguir exibe as configurações DNS para todos os SVMs no cluster:

   ```
   vserver services name-service dns show
                                              Name
   Vserver           State     Domains             Servers
   ----------------- --------- ------------------- -------------
   cluster1          enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   vs1.example.com   enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   ```

   O comando a seguir exibe informações detalhadas de configuração de DNS para SVM VS1:

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
          Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. Valide o status dos servidores de nomes usando o `vserver services name-service dns check` comando.

   O `vserver services name-service dns check` comando está disponível a partir de ONTAP 9.2.

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

Configure um servidor SMB em um domínio do ative Directory

Configurar serviços de tempo

Antes de criar um servidor SMB em um controlador de domínio ativo, você deve garantir que a hora do cluster e a hora nos controladores de domínio do domínio ao qual o servidor SMB pertencerá correspondem dentro de cinco minutos.

Sobre esta tarefa

Você deve configurar os serviços NTP do cluster para usar os mesmos servidores NTP para sincronização de tempo que o domínio do ative Directory usa.

A partir do ONTAP 9.5, você pode configurar seu servidor NTP com autenticação simétrica.

Passos

1. Configure os serviços de tempo usando o `cluster time-service ntp server create` comando.
   - Para configurar serviços de tempo sem autenticação simétrica, digite o seguinte comando: `cluster time-service ntp server create -server server_ip_address`
   - Para configurar serviços de tempo com autenticação simétrica, digite o seguinte comando: `cluster time-service ntp server create -server server_ip_address -key-id key_id cluster time-service ntp server create -server 10.10.10.1 cluster time-service ntp server create -server 10.10.10.2`
2. Verifique se os serviços de tempo estão configurados corretamente usando o `cluster time-service`

`ntp server show` comando.

```
cluster time-service ntp server show
```

```
Server                          Version
------------------------------- -------
10.10.10.1                      auto
10.10.10.2                      auto
```

Comandos para gerenciar a autenticação simétrica em servidores NTP

A partir do ONTAP 9.5, o protocolo de tempo de rede (NTP) versão 3 é suportado. O NTPv3 inclui autenticação simétrica usando chaves SHA-1, o que aumenta a segurança da rede.

Para fazer isso…	Use este comando…
Configurar um servidor NTP sem autenticação simétrica	`cluster time-service ntp server create -server server_name`
Configure um servidor NTP com autenticação simétrica	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
Ativar autenticação simétrica para um servidor NTP existente pode ser modificado para ativar a autenticação adicionando o ID de chave necessária.	`cluster time-service ntp server modify -server server_name -key-id key_id`
Configurar uma chave NTP partilhada	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` As chaves compartilhadas são referidas por um ID. O ID, seu tipo e valor devem ser idênticos no nó e no servidor NTP
Configure um servidor NTP com um ID de chave desconhecido	`cluster time-service ntp server create -server server_name -key-id key_id`
Configure um servidor com um ID de chave não configurado no servidor NTP.	`cluster time-service ntp server create -server server_name -key-id key_id` O ID, tipo e valor da chave devem ser idênticos ao ID, tipo e valor da chave configurados no servidor NTP.

Para fazer isso…	Use este comando…
Desativar a autenticação simétrica	`cluster time-service ntp server modify -server server_name -authentication disabled`

Crie um servidor SMB em um domínio do ative Directory

Você pode usar o `vserver cifs create` comando para criar um servidor SMB no SVM e especificar o domínio do ative Directory (AD) ao qual ele pertence.

Antes de começar

Os SVM e LIFs que você está usando para fornecer dados devem ter sido configurados para permitir o protocolo SMB. Os LIFs devem ser capazes de se conetar aos servidores DNS configurados no SVM e a um controlador de domínio AD do domínio ao qual você deseja ingressar no servidor SMB.

Qualquer usuário autorizado a criar contas de máquina no domínio do AD ao qual você está ingressando no servidor SMB pode criar o servidor SMB no SVM. Isso pode incluir usuários de outros domínios.

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

Sobre esta tarefa

Ao criar um servidor SMB em um domínio do diretório de atividades:

- Você deve usar o nome de domínio totalmente qualificado (FQDN) ao especificar o domínio.
- A configuração padrão é adicionar a conta de máquina do servidor SMB ao objeto de computador do ative Directory.
- Pode optar por adicionar o servidor SMB a uma unidade organizacional (ou) diferente utilizando a `-ou` opção.
- Opcionalmente, você pode optar por adicionar uma lista delimitada por vírgulas de um ou mais aliases NetBIOS (até 200) para o servidor SMB.

  A configuração de aliases NetBIOS para um servidor SMB pode ser útil quando você está consolidando dados de outros servidores de arquivos para o servidor SMB e deseja que o servidor SMB responda aos nomes dos servidores originais.

As `vserver cifs` páginas man contêm parâmetros opcionais adicionais e requisitos de nomeação.

> A partir do ONTAP 9.1, você pode habilitar o SMB versão 2,0 para se conetar a um controlador de domínio (DC). Isso é necessário se você desativou o SMB 1,0 em controladores de domínio. A partir do ONTAP 9.2, o SMB 2,0 é ativado por padrão.

A partir do ONTAP 9.8, você pode especificar que as conexões aos controladores de domínio sejam criptografadas. O ONTAP requer criptografia para comunicações do controlador de domínio quando a `-encryption-required-for-dc-connection` opção está definida como `true`; o padrão é `false`. Quando a opção está definida, apenas o protocolo SMB3 será utilizado para ligações ONTAP-DC, uma vez que a encriptação é suportada apenas pelo SMB3. .

"Gerenciamento de SMB" Contém mais informações sobre as opções de configuração do servidor SMB.

Passos

1. Verifique se o SMB está licenciado no cluster: `system license show -package cifs`

   A licença SMB está incluída no "ONTAP One". Se não tiver o ONTAP One e a licença não estiver instalada, contacte o seu representante de vendas.

   Não é necessária uma licença CIFS se o servidor SMB for utilizado apenas para autenticação.

2. Crie o servidor SMB em um domínio AD: `vserver cifs create -vserver vserver_name -cifs -server smb_server_name -domain FQDN [-ou organizational_unit][-netbios-aliases NetBIOS_name, ...][-keytab-uri {(ftp|http)://hostname|IP_address}][-comment text]`

   Ao ingressar em um domínio, esse comando pode levar vários minutos para ser concluído.

   O comando a seguir cria o servidor SMB "sssmb_server01" no domínio "'example.com`":

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   smb_server01 -domain example.com
   ```

   O comando a seguir cria o servidor SMB "sssmb_server02" no domínio "mydomain.com`" e autentica o administrador do ONTAP com um arquivo keytab:

   ```
   cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
   smb_server02 -domain mydomain.com -keytab-uri
   http://admin.mydomain.com/ontap1.keytab
   ```

3. Verifique a configuração do servidor SMB usando o `vserver cifs show` comando.

   Neste exemplo, o comando output mostra que um servidor SMB chamado "'SMB_SERVER01'" foi criado na SVM vs1.example.com e foi associado ao domínio "'example.com`".

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

                                           Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
   Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: -
   ```

4. Se desejar, ative a comunicação criptografada com o controlador de domínio (ONTAP 9.8 e posterior): `vserver cifs security modify -vserver svm_name -encryption-required-for-dc -connection true`

Exemplos

O comando a seguir cria um servidor SMB chamado "sssmb_server02" no SVM vs2.example.com no domínio "'example.com`'". A conta da máquina é criada no contentor "'ou-eng, ou-corp, DC-example, DC-com'". Ao servidor SMB é atribuído um alias NetBIOS.

```
cluster1::> vserver cifs create -vserver vs2.example.com –cifs-server
smb_server02 -domain example.com –ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1
                                        Vserver: vs2.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER02
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                           Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

O comando a seguir permite que um usuário de um domínio diferente, neste caso um administrador de um domínio confiável, crie um servidor SMB chamado "sssmb_server03" no SVM vs3.example.com. A `-domain` opção especifica o nome do domínio inicial (especificado na configuração DNS) no qual você deseja criar o servidor SMB. A `username` opção especifica o administrador do domínio confiável.

- Domínio doméstico: example.com
- Domínio confiável: trust.lab.com
- Nome de usuário para o domínio confiável: Administrator1

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com

Username: Administrator1@trust.lab.com
Password: . . .
```

Crie arquivos keytab para autenticação SMB

A partir do ONTAP 9.7, o ONTAP oferece suporte à autenticação SVM com servidores do ative Directory (AD) usando arquivos keytab. Os ADMINISTRADORES DE ANÚNCIOS geram um arquivo keytab e o disponibilizam aos administradores do ONTAP como um URI (identificador de recurso uniforme), que é fornecido quando `vserver cifs` os

comandos exigem autenticação Kerberos com o domínio AD.

Os ADMINISTRADORES DE ANÚNCIOS podem criar os arquivos keytab usando o comando padrão do Windows Server `ktpass`. O comando deve ser executado no domínio primário onde a autenticação é necessária. O `ktpass` comando pode ser usado para gerar arquivos keytab somente para usuários de domínio primário; chaves geradas usando usuários de domínio confiável não são suportadas.

Os arquivos keytab são gerados para usuários administrativos específicos do ONTAP. Desde que a senha do usuário administrativo não seja alterada, as chaves geradas para o tipo de criptografia e domínio específicos não serão alteradas. Portanto, um novo arquivo keytab é necessário sempre que a senha do usuário admin é alterada.

São suportados os seguintes tipos de encriptação:

- AES256-SHA1
- DES-CBC-MD5

  O ONTAP não oferece suporte ao tipo de criptografia DES-CBC-CRC.

- RC4-HMAC

AES256 é o tipo de criptografia mais alto e deve ser usado se ativado no sistema ONTAP.

Os arquivos keytab podem ser gerados especificando a senha de administrador ou usando uma senha gerada aleatoriamente. No entanto, a qualquer momento, apenas uma opção de senha pode ser usada, porque uma chave privada específica para o usuário admin é necessária no servidor AD para descriptografar as chaves dentro do arquivo keytab. Qualquer alteração na chave privada para um administrador específico invalidará o arquivo keytab.

Configure um servidor SMB em um grupo de trabalho

Configure um servidor SMB em uma visão geral do grupo de trabalho

A configuração de um servidor SMB como membro em um grupo de trabalho consiste em criar o servidor SMB e, em seguida, criar usuários e grupos locais.

Você pode configurar um servidor SMB em um grupo de trabalho quando a infraestrutura de domínio do Microsoft ative Directory não estiver disponível.

Um servidor SMB no modo de grupo de trabalho suporta apenas autenticação NTLM e não suporta autenticação Kerberos.

Crie um servidor SMB em um grupo de trabalho

Você pode usar o `vserver cifs create` comando para criar um servidor SMB no SVM e especificar o grupo de trabalho ao qual ele pertence.

Antes de começar

Os SVM e LIFs que você está usando para fornecer dados devem ter sido configurados para permitir o protocolo SMB. Os LIFs devem ser capazes de se conetar aos servidores DNS configurados no SVM.

Sobre esta tarefa

Os servidores SMB no modo de grupo de trabalho não suportam os seguintes recursos SMB:

- Protocolo de SMB3 testemunhas
- SMB3 ações da CA
- SQL sobre SMB
- Redirecionamento de pasta
- Perfis de roaming
- Objeto de política de grupo (GPO)
- Serviço de Snapshot de volume (VSS)

As `vserver cifs` páginas man contêm parâmetros de configuração opcionais adicionais e requisitos de nomenclatura.

Passos

1. Verifique se o SMB está licenciado no cluster: `system license show -package cifs`

   A licença SMB está incluída no "ONTAP One". Se não tiver o ONTAP One e a licença não estiver instalada, contacte o seu representante de vendas.

   Não é necessária uma licença CIFS se o servidor SMB for utilizado apenas para autenticação.

2. Crie o servidor SMB em um grupo de trabalho: `vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment text]`

   O comando a seguir cria o servidor SMB "ssssmb_server01" no grupo de trabalho "'workgroup01":

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   SMB_SERVER01 -workgroup workgroup01
   ```

3. Verifique a configuração do servidor SMB usando o `vserver cifs show` comando.

   No exemplo a seguir, o comando output mostra que um servidor SMB chamado "sssmb_server01" foi criado na SVM vs1.example.com no grupo de trabalho "'workgroup01"":

```
cluster1::> vserver cifs show -vserver vs0

                                          Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: workgroup01
                      Fully Qualified Domain Name: -
                              Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
                                   Workgroup Name: workgroup01
                              Authentication Style: workgroup
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

Depois de terminar

Para um servidor CIFS em um grupo de trabalho, você deve criar usuários locais e, opcionalmente, grupos locais, no SVM.

Informações relacionadas

"Gerenciamento de SMB"

Crie contas de usuário locais

Você pode criar uma conta de usuário local que pode ser usada para autorizar o acesso aos dados contidos no SVM em uma conexão SMB. Você também pode usar contas de usuário locais para autenticação ao criar uma sessão SMB.

Sobre esta tarefa

A funcionalidade de usuário local é ativada por padrão quando o SVM é criado.

Ao criar uma conta de usuário local, você deve especificar um nome de usuário e especificar o SVM para associar a conta.

As `vserver cifs users-and-groups local-user` páginas man contêm detalhes sobre parâmetros opcionais e requisitos de nomeação.

Passos

1. Crie o usuário local: `vserver cifs users-and-groups local-user create -vserver` *`vserver_name`* `-user-name` *`user_name optional_parameters`*

   Os seguintes parâmetros opcionais podem ser úteis:

   - `-full-name`

     O nome completo dos usuários.

   - `-description`

Uma descrição para o utilizador local.

- `-is-account-disabled {true|false}`

  Especifica se a conta de usuário está ativada ou desativada. Se este parâmetro não for especificado, o padrão é ativar a conta de usuário.

O comando solicita a senha do usuário local.

2. Introduza uma palavra-passe para o utilizador local e, em seguida, confirme a palavra-passe.
3. Verifique se o usuário foi criado com sucesso: `vserver cifs users-and-groups local-user show -vserver vserver_name`

Exemplo

O exemplo a seguir cria um usuário local ""SMB_SERVER01"", com um nome completo ""Sue Chang"", associado ao SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                   Full Name  Description
-------- --------------------------- ---------- -------------
vs1      SMB_SERVER01\Administrator             Built-in administrator
account
vs1      SMB_SERVER01\sue            Sue Chang
```

Crie grupos locais

É possível criar grupos locais que podem ser usados para autorizar o acesso aos dados associados ao SVM em uma conexão SMB. Você também pode atribuir Privileges que definem quais direitos de usuário ou recursos um membro do grupo tem.

Sobre esta tarefa

A funcionalidade de grupo local é ativada por padrão quando o SVM é criado.

Ao criar um grupo local, você deve especificar um nome para o grupo e especificar o SVM para associar o grupo. Você pode especificar um nome de grupo com ou sem o nome de domínio local e, opcionalmente, especificar uma descrição para o grupo local. Não é possível adicionar um grupo local a outro grupo local.

As `vserver cifs users-and-groups local-group` páginas man contêm detalhes sobre parâmetros opcionais e requisitos de nomeação.

Passos

1. Crie o grupo local: `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

O seguinte parâmetro opcional pode ser útil:

- `-description`

  Uma descrição para o grupo local.

2. Verifique se o grupo foi criado com sucesso: `vserver cifs users-and-groups local-group show -vserver vserver_name`

Exemplo

O exemplo a seguir cria um grupo local "SMB_SERVER01" associado ao SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering

cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
Vserver          Group Name                  Description
---------------- --------------------------- ----------------------------
vs1.example.com  BUILTIN\Administrators      Built-in Administrators
group
vs1.example.com  BUILTIN\Backup Operators    Backup Operators group
vs1.example.com  BUILTIN\Power Users         Restricted administrative
privileges
vs1.example.com  BUILTIN\Users               All users
vs1.example.com  SMB_SERVER01\engineering
vs1.example.com  SMB_SERVER01\sales
```

Depois de terminar

Você deve adicionar membros ao novo grupo.

Gerenciar a associação ao grupo local

Você pode gerenciar a associação de grupo local adicionando e removendo usuários locais ou de domínio ou adicionando e removendo grupos de domínio. Isso é útil se você quiser controlar o acesso a dados com base nos controles de acesso colocados no grupo ou se quiser que os usuários tenham o Privileges associado a esse grupo.

Sobre esta tarefa

Se você não quiser mais que um usuário local, usuário de domínio ou grupo de domínio tenha direitos de acesso ou Privileges com base na associação a um grupo, você pode remover o membro do grupo.

Você deve ter em mente o seguinte ao adicionar membros a um grupo local:

- Você não pode adicionar usuários ao grupo especial *todos*.
- Não é possível adicionar um grupo local a outro grupo local.
- Para adicionar um usuário ou grupo de domínio a um grupo local, o ONTAP deve ser capaz de resolver o nome para um SID.

Você deve ter em mente o seguinte ao remover membros de um grupo local:

- Você não pode remover membros do grupo especial *todos*.
- Para remover um membro de um grupo local, o ONTAP deve ser capaz de resolver seu nome para um SID.

Passos

1. Adicione um membro ou remova um membro de um grupo.
   - Adicionar um membro: `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     Você pode especificar uma lista delimitada por vírgulas de usuários locais, usuários de domínio ou grupos de domínio para adicionar ao grupo local especificado.
   - Remover um membro: `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     Você pode especificar uma lista delimitada por vírgulas de usuários locais, usuários de domínio ou grupos de domínio a serem removidos do grupo local especificado.

Exemplos

O exemplo a seguir adiciona um usuário local ""SMB_SERVER01"" ao grupo local ""SMB_SERVER01" engenharia" no SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

O exemplo a seguir remove os usuários locais "'SMB_SERVER01"" e "'SMB_SERVER01' james' do grupo local "'SMB_SERVER01' Engineering" no SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Verifique as versões do SMB ativadas

Sua versão do ONTAP 9 determina quais versões do SMB estão habilitadas por padrão para conexões com clientes e controladores de domínio. Você deve verificar se o servidor SMB oferece suporte aos clientes e às funcionalidades necessárias em seu ambiente.

Sobre esta tarefa

Para conexões com clientes e controladores de domínio, você deve ativar o SMB 2,0 e posterior sempre que possível. Por motivos de segurança, você deve evitar o uso do SMB 1,0 e desativá-lo se tiver verificado que não é necessário no seu ambiente.

No ONTAP 9, as versões 2,0 e posteriores do SMB são ativadas por padrão para conexões de clientes, mas a versão do SMB 1,0 habilitada por padrão depende da versão do ONTAP.

- A partir do ONTAP 9 P8.1, o SMB 1,0 pode ser desativado em SVMs.

  A `-smb1-enabled` opção para o `vserver cifs options modify` comando ativa ou desativa o SMB 1,0.

- Começando com ONTAP 9.3, ele é desativado por padrão em novos SVMs.

Se o servidor SMB estiver em um domínio do ative Directory (AD), você poderá habilitar o SMB 2,0 para se conetar a um controlador de domínio (DC) começando com o ONTAP 9.1. Isso é necessário se você tiver desabilitado o SMB 1,0 em DCs. A partir do ONTAP 9.2, o SMB 2,0 é ativado por padrão para conexões DC.

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

"Gerenciamento de SMB" Contém detalhes sobre as versões e funcionalidades do SMB suportadas.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Verifique quais versões SMB estão ativadas:

   ```
   vserver cifs options show
   ```

   Você pode rolar a lista para baixo para exibir as versões SMB habilitadas para conexões de cliente e, se estiver configurando um servidor SMB em um domínio AD, para conexões de domínio AD.

3. Ative ou desative o protocolo SMB para ligações de clientes, conforme necessário:
   - Para ativar uma versão SMB:

     ```
     vserver cifs options modify -vserver <vserver_name> -<smb_version>
     true
     ```

     Valores possíveis para `smb_version`:

     - `-smb1-enabled`
     - `-smb2-enabled`
     - `-smb3-enabled`
     - `-smb31-enabled`

     O comando a seguir habilita o SMB 3,1 no SVM vs1.example.com: `cluster1::*> vserver`

```
cifs options modify -vserver vs1.example.com -smb31-enabled true
```

- Para desativar uma versão SMB:

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
false
```

4. Se o servidor SMB estiver em um domínio do ative Directory, ative ou desative o protocolo SMB para conexões DC, conforme necessário:
   - Para ativar uma versão SMB:

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections true
```

   - Para desativar uma versão SMB:

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections false
```

5. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Mapeie o servidor SMB no servidor DNS

O servidor DNS do seu site deve ter uma entrada apontando o nome do servidor SMB e quaisquer aliases NetBIOS para o endereço IP do LIF de dados para que os usuários do Windows possam mapear uma unidade para o nome do servidor SMB.

Antes de começar

Você deve ter acesso administrativo ao servidor DNS do seu site. Se não tiver acesso administrativo, deverá pedir ao administrador DNS para executar esta tarefa.

Sobre esta tarefa

Se você usar aliases NetBIOS para o nome do servidor SMB, é uma prática recomendada criar pontos de entrada de servidor DNS para cada alias.

Passos

1. Inicie sessão no servidor DNS.
2. Criar entradas de pesquisa direta (A - Registro de endereço) e inversa (PTR - Registro de ponteiro) para mapear o nome do servidor SMB para o endereço IP do LIF de dados.
3. Se você usar aliases NetBIOS, crie uma entrada de pesquisa de nome canônico Alias (CNAME resource record) para mapear cada alias para o endereço IP do LIF de dados do servidor SMB.

Resultados

Depois que o mapeamento é propagado pela rede, os usuários do Windows podem mapear uma unidade para o nome do servidor SMB ou seus aliases NetBIOS.

Configurar o acesso de cliente SMB ao armazenamento partilhado

Configurar o acesso de cliente SMB ao armazenamento partilhado

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

Antes de começar

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

Crie um volume ou um contêiner de storage de qtree

Crie um volume

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

Sobre esta tarefa

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

Antes de começar

- O SMB deve ser configurado e executado.
- O estilo de segurança da SVM deve ser NTFS.
- A partir do ONTAP 9.13,1, você pode criar volumes com análise de capacidade e acompanhamento de atividades habilitados. Para ativar o acompanhamento de capacidade ou atividade, emita o `volume create` comando com `-analytics-state` ou `-activity-tracking-state` defina como `on`.

  Para saber mais sobre análise de capacidade e acompanhamento de atividades, "Ative a análise do sistema de ficheiros" consulte .

Passos

1. Crie o volume com um ponto de junção: `volume create -vserver` *`svm_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]}`

`-security-style ntfs -junction-path` *`junction_path`*`]`

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

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

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

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

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

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

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

Exemplos

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

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

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver          Volume  Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  users1  true     /users          RW_volume
```

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

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

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                           Junction                 Junction
Vserver          Volume  Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4   true     /eng/home       RW_volume
```

Crie uma qtree

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

Antes de começar

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

Passos

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

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

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

Exemplo

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

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

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

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

Requisitos e considerações para criar um compartilhamento SMB

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

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

Os caminhos de compartilhamento têm os seguintes requisitos:

- Um nome de caminho de diretório pode ter até 255 carateres.
- Se houver um espaço no nome do caminho, toda a cadeia de carateres deve ser colocada em aspas (por exemplo, `"/new volume/mount here"`).
- 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.

Os padrões de propriedade de compartilhamento podem ser alterados:

- As propriedades iniciais padrão para todos os compartilhamentos são `oplocks`, `browsable`, `changenotify` e `show-previous-versions`.

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

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

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

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

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

Os compartilhamentos do diretório base têm os seguintes requisitos:

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

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

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

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

Crie um compartilhamento SMB

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

Antes de começar

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

Sobre esta tarefa

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

Passos

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

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

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

Exemplos

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

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

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

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

Verifique o acesso do cliente SMB

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

Passos

1. Faça login em um cliente Windows.
2. Teste o acesso usando o nome do servidor SMB:

   a. No Explorador do Windows, mapeie uma unidade para a partilha no seguinte formato: `\\SMB_Server_Name\Share_Name`

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

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

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

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

3. Repita a Etapa 2 para qualquer alias NetBIOS.

Criar listas de controle de acesso de compartilhamento SMB

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

Antes de começar

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

Sobre esta tarefa

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

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

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

Passos

1. Excluir a ACL de compartilhamento padrão:`vserver cifs share access-control delete -vserver` *`vserver_name`* `-share` *`share_name`* `-user-or-group everyone`
2. Configure a nova ACL:

Se você quiser configurar ACLs usando um…	Digite o comando…
Usuário do Windows	`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`
Grupo Windows	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_group_name`* `-permission access_right`

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

Exemplo

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

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

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

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

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

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

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    DOMAIN\"Tiger Team"         windows     Change
vs1            datavol5    DOMAIN\"Sue Chang"          windows
Full_Control
```

Configurar permissões de arquivo NTFS em um compartilhamento

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

Antes de começar

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

Sobre esta tarefa

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

Passos

1. Inicie sessão num cliente Windows como administrador.
2. No menu **Ferramentas** no Windows Explorer, selecione **Mapear unidade de rede**.
3. Preencha a caixa **Map Network Drive**:

   a. Selecione uma letra **Drive**.

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

      Se o nome do servidor SMB for SMB_SERVER01 e o compartilhamento for chamado "'SHARE1", você digitaria `\\SMB_SERVER01\SHARE1`.

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

   c. Clique em **Finish**.

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

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

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

7. Clique em **Editar**.

   A caixa permissões para <Object> será aberta.

8. Execute as ações desejadas:

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

9. Execute as ações desejadas:

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

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

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

Verifique o acesso do usuário

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

Passos

1. Em um cliente Windows, faça login como um dos usuários que agora tem acesso ao compartilhamento.
2. No menu **Ferramentas** no Windows Explorer, selecione **Mapear unidade de rede**.
3. Preencha a caixa **Map Network Drive**:

   a. Selecione uma letra **Drive**.

   b. Na caixa **pasta**, digite o nome do compartilhamento que você fornecerá aos usuários.

   Se o nome do servidor SMB for SMB_SERVER01 e o compartilhamento for chamado "'SHARE1", você digitaria `\\SMB_SERVER01\share1`.

c. Clique em **Finish**.

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

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

Informações sobre direitos autorais

Informações sobre marcas comerciais