



Configurar o acesso SMB a uma SVM

ONTAP 9

NetApp
February 12, 2026

Índice

Configurar o acesso SMB a uma SVM	1
Configurar o acesso SMB a SVMs ONTAP	1
Crie SVMs ONTAP para fornecer acesso a dados SMB	1
Verifique se o protocolo SMB está ativado no SVM do ONTAP	2
Abra a política de exportação SMB do volume raiz do ONTAP SVM	3
Crie LIFs SMB do ONTAP	4
Ative DNS para a resolução de nome de host SMB do ONTAP	9
Configure um servidor SMB em um domínio do ativo Directory	10
Configurar serviços de tempo ONTAP para servidores SMB	10
Comandos ONTAP para gerenciar a autenticação simétrica em servidores NTP	11
Crie servidores SMB em um domínio do ativo Directory do ONTAP	12
Criar arquivos keytab para autenticação ONTAP SMB	15
Configure um servidor SMB em um grupo de trabalho	15
Saiba mais sobre a configuração do servidor SMB nos grupos de trabalho do ONTAP	15
Crie servidores SMB no ONTAP SVM com grupos de trabalho especificados	16
Crie contas de usuário locais do ONTAP SMB	17
Crie grupos SMB locais do ONTAP	18
Gerenciar a associação de grupo SMB local do ONTAP	19
Verifique as versões do ONTAP SMB ativadas	20
Mapeie servidores SMB do ONTAP no servidor DNS	22

Configurar o acesso SMB a uma SVM

Configurar o acesso SMB a SVMs ONTAP

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.

Crie SVMs ONTAP para fornecer acesso a dados SMB

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 storage. Você também pode configurar alertas quando o SVM se aproximar de um nível de capacidade limite. Para obter mais informações, [Gerenciar a capacidade do SVM](#) consulte .

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 um 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 adaptável](#) consulte .

Verifique se o protocolo SMB está ativado no SVM do ONTAP

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 SMB do volume raiz do ONTAP 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 LIFs SMB do ONTAP

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`. Saiba mais sobre `up` o ["Referência do comando ONTAP"](#) na .
- 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.

Saiba mais sobre `network subnet create` o ["Referência do comando ONTAP"](#) na .

- 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).

Saiba mais sobre `network interface` o ["Referência do comando ONTAP"](#) na .

- 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 vservice_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 vservice_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 vservice_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. Saiba mais sobre `network route create` como criar uma rota estática em um SVM no ["Referência do comando ONTAP"](#).
- 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	<code>network ping</code>
Endereço IPv6	<code>network ping6</code>

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 elc -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 elc -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
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is
Home						
-----	-----	-----	-----	-----	-----	-----
cluster-1						
true	cluster_mgmt	up/up	192.0.2.3/24	node-1	e1a	
node-1						
true	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	
node-2						
true	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	
vs1.example.com						
true	datalif1	up/down	192.0.2.145/30	node-1	e1c	
vs3.example.com						
true	datalif3	up/up	192.0.2.146/30	node-2	e0c	
true	datalif4	up/up	2001::2/64	node-2	e0c	
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 ipspacel
```

Informações relacionadas

- ["ping de rede"](#)
- ["reverter a interface de rede"](#)

Ative DNS para a resolução de nome de host SMB do ONTAP

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. Saiba mais sobre `vserver services name-service dns` o ["Referência do comando ONTAP"](#) na .

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. Saiba mais sobre `vserver services name-service dns create` o ["Referência do comando ONTAP"](#) na .

Sobre esta tarefa

Saiba mais ["Configurando DNS dinâmico no SVM"](#) sobre o .

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
```



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
```

Vserver	State	Domains	Name 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.

```
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 ativo Directory

Configurar serviços de tempo ONTAP para servidores SMB

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 que o domínio do Active 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


Informações relacionadas

- ["serviço de tempo de cluster ntp"](#)

Comandos ONTAP 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	<pre>cluster time-service ntp server create -server server_name</pre>
Configure um servidor NTP com autenticação simétrica	<pre>cluster time-service ntp server create -server server_ip_address -key-id key_id</pre>
Ativar autenticação simétrica para um servidor NTP existente pode ser modificado para ativar a autenticação adicionando o ID de chave necessária.	<pre>cluster time-service ntp server modify -server server_name -key-id key_id</pre>
Configurar uma chave NTP compartilhada	<pre>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</pre> <div> As chaves compartilhadas são referidas por um ID. O ID, seu tipo e valor devem ser idênticos no nó e no servidor NTP</div>
Configure um servidor NTP com um ID de chave desconhecido	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre>

Para fazer isso...	Use este comando...
Configure um servidor com um ID de chave não configurado no servidor NTP.	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre> <div>  <p>O ID, tipo e valor da chave devem ser idênticos ao ID, tipo e valor da chave configurados no servidor NTP.</p> </div>
Desativar a autenticação simétrica	<pre>cluster time-service ntp server modify -server server_name -authentication disabled</pre>

Informações relacionadas

- ["serviço de tempo de cluster ntp"](#)

Crie servidores SMB em um domínio do ativo Directory do ONTAP

Você pode usar o `vserver cifs create` comando para criar um servidor SMB no SVM e especificar o domínio do ativo 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 conectar 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 ativo 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.

Saiba mais sobre `vserver cifs` parâmetros opcionais e requisitos de nomenclatura no ["Referência do](#)

comando ONTAP".

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 "ssssmb_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 "ssssmb_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 "ssssmb_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 "ssssmb_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: . . .
```

Criar arquivos keytab para autenticação ONTAP SMB

A partir do ONTAP 9.7, o ONTAP oferece suporte à autenticação SVM com servidores do Active 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

Saiba mais sobre a configuração do servidor SMB nos grupos de trabalho do ONTAP

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 Active Directory não estiver disponível.

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

Crie servidores SMB no ONTAP SVM com grupos de trabalho especificados

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 conectar 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)

Saiba mais sobre `vserver cifs` parâmetros de configuração opcionais e requisitos de nomenclatura no ["Referência do comando ONTAP"](#).

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 "ssssmb_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 do ONTAP SMB

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.

Saiba mais sobre `vserver cifs users-and-groups local-user` parâmetros opcionais e requisitos de nomenclatura no ["Referência do comando ONTAP"](#).

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 SMB locais do ONTAP

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.

Saiba mais sobre `vserver cifs users-and-groups local-group` parâmetros opcionais e requisitos de nomenclatura no ["Referência do comando ONTAP"](#).

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
vs1.example.com	BUILTIN\Backup Operators	Backup Operators group
vs1.example.com	BUILTIN\Power Users	Restricted administrative
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 de grupo SMB local do ONTAP

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 ONTAP 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.

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



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 Active 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 servidores SMB do ONTAP 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.

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTE; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.