Configurar o acesso NFS a uma SVM

ONTAP 9

NetApp
January 17, 2025

Índice

Configurar o acesso NFS a uma SVM

Criar um SVM

Se você ainda não tiver pelo menos um SVM em um cluster para fornecer acesso a dados a clientes NFS, será necessário criá-lo.

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 vserver_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style unix -language C.UTF-8 -ipspace ipspace_name`

   - Utilize a definição UNIX 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`

   ```
   `Allowed Protocols`O campo deve incluir NFS. 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 unix -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: unix
                                 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 NFS está habilitado no SVM

Antes de configurar e usar NFS em SVMs, você deve 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 NFS `vserver add-protocols -vserver vserver_name -protocols nfs`
   - 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   nfs                       cifs, fcp, iscsi, ndmp
```

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

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

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 NFS. Sem essa regra, todos os clientes NFS 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 o acesso está aberto a todos os clientes NFS 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:  nfs
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 nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`

   Se o SVM contiver apenas volumes protegidos pelo Kerberos, você poderá definir as opções de regra de exportação `-rorule` , `-rwrule` e `-superuser` para o volume raiz como `krb5` ou `krb5i`. Por exemplo:

   `-rorule krb5i -rwrule krb5i -superuser krb5i`

3. Verifique a criação de regras usando o `vserver export-policy rule show` comando.

Resultado

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

Crie um servidor NFS

Depois de verificar se o NFS está licenciado no cluster, você pode usar o `vserver nfs create` comando para criar um servidor NFS no SVM e especificar as versões NFS compatíveis.

Sobre esta tarefa

O SVM pode ser configurado para dar suporte a uma ou mais versões de NFS. Se você estiver apoiando NFSv4 ou posterior:

- O nome de domínio de mapeamento de ID de usuário NFSv4 deve ser o mesmo no servidor NFSv4 e nos clientes de destino.

  Ele não precisa necessariamente ser o mesmo que um nome de domínio LDAP ou NIS, desde que o servidor NFSv4 e os clientes estejam usando o mesmo nome.

- Os clientes-alvo devem suportar a configuração de ID numérica NFSv4.
- Por motivos de segurança, você deve usar o LDAP para serviços de nome em implantações NFSv4.

Antes de começar

O SVM deve ter sido configurado para permitir o protocolo NFS.

Passos

1. Verifique se o NFS está licenciado no cluster:

   ```
   system license show -package nfs
   ```

   Se não estiver, contacte o seu representante de vendas.

2. Criar um servidor NFS:

   ```
   vserver nfs create -vserver vserver_name -v3 {enabled|disabled} -v4.0
   {enabled|disabled} -v4-id-domain nfsv4_id_domain -v4-numeric-ids
   {enabled|disabled} -v4.1 {enabled|disabled} -v4.1-pnfs {enabled|disabled}
   ```

   Você pode optar por ativar qualquer combinação de versões NFS. Se você quiser dar suporte ao pNFS, habilite as `-v4.1` opções e `-v4.1-pnfs` .

   Se você ativar o v4 ou posterior, também deve ter certeza de que as seguintes opções estão definidas corretamente:

   - `-v4-id-domain`

     Este parâmetro opcional especifica a parte do domínio da forma de cadeia de carateres de nomes de usuário e grupo, conforme definido pelo protocolo NFSv4. Por padrão, o ONTAP usa o domínio NIS se um estiver definido; caso contrário, o domínio DNS será usado. Você deve fornecer um valor que corresponda ao nome de domínio usado pelos clientes de destino.

   - `-v4-numeric-ids`

     Este parâmetro opcional especifica se o suporte para identificadores de cadeia de carateres numéricos em atributos de proprietário NFSv4 está habilitado. A configuração padrão é ativada, mas você deve verificar se os clientes de destino a suportam.

   Você pode ativar recursos NFS adicionais mais tarde usando o `vserver nfs modify` comando.

3. Verifique se o NFS está em execução:

   ```
   vserver nfs status -vserver vserver_name
   ```

4. Verifique se o NFS está configurado conforme desejado:

   `vserver nfs show -vserver vserver_name`

Exemplos

O comando a seguir cria um servidor NFS no SVM chamado VS1 com NFSv3 e NFSv4,0 ativados:

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id
-domain my_domain.com
```

Os comandos a seguir verificam os valores de status e configuração do novo servidor NFS chamado VS1:

```
vs1::> vserver nfs status -vserver vs1
The NFS server is running on Vserver "vs1".

vs1::> vserver nfs show -vserver vs1

                              Vserver: vs1
                 General NFS Access: true
                              NFS v3: enabled
                            NFS v4.0: enabled
                         UDP Protocol: enabled
                         TCP Protocol: enabled
                Default Windows User: -
                 NFSv4.0 ACL Support: disabled
    NFSv4.0 Read Delegation Support: disabled
   NFSv4.0 Write Delegation Support: disabled
            NFSv4 ID Mapping Domain: my_domain.com
...
```

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.

O que você vai precisar

- 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 estiver usando a autenticação Kerberos, ative o Kerberos em várias LIFs.
- 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.

A partir do ONTAP 9.4, o FC-NVMe é compatível. Se você estiver criando um LIF FC-NVMe, deve estar ciente do seguinte:

- O protocolo NVMe precisa ser compatível com o adaptador FC no qual o LIF é criado.
- O FC-NVMe pode ser o único protocolo de dados em LIFs de dados.
- Um tráfego de gerenciamento de manipulação de LIF deve ser configurado para cada máquina virtual de storage (SVM) que suporte SAN.
- Os LIFs e namespaces NVMe devem ser hospedados no mesmo nó.
- Somente um LIF NVMe que manipula o tráfego de dados pode ser configurado por SVM

Passos

1. Criar um LIF:

   `network interface create -vserver` *`vserver_name`* `-lif` *`lif_name`* `-role data -data -protocol nfs -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}`

Opção	Descrição
ONTAP 9 .5 e anteriores	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -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* -role data -data-protocol nfs -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}`

- `-role`O parâmetro não é necessário ao criar um LIF usando uma política de serviço (a partir do ONTAP 9,6).
- 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.

  O `-data-protocol` parâmetro não é necessário ao criar um LIF usando uma política de serviço (começando com ONTAP 9.6).

- `-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 usando o `network interface show` comando.
3. Verifique se o endereço IP configurado está acessível:

Para verificar um…	Utilizar…
Endereço IPv4	`network ping`
Endereço IPv6	`network ping6`

4. Se você estiver usando Kerberos, repita as etapas 1 a 3 para criar LIFs adicionais.

O Kerberos deve ser habilitado separadamente em cada um desses LIFs.

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 nfs -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 nfs -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.

O que você vai precisar

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
```

Configurar serviços de nomes

Configure a visão geral dos serviços de nome

Dependendo da configuração do seu sistema de storage, o ONTAP precisa ser capaz de procurar informações de host, usuário, grupo ou netgroup para fornecer acesso adequado aos clientes. Você deve configurar serviços de nomes para permitir que o ONTAP acesse serviços de nomes locais ou externos para obter essas informações.

Você deve usar um serviço de nomes como NIS ou LDAP para facilitar pesquisas de nomes durante a autenticação do cliente. É melhor usar o LDAP sempre que possível para maior segurança, especialmente ao implantar o NFSv4 ou posterior. Você também deve configurar usuários e grupos locais caso os servidores de nomes externos não estejam disponíveis.

As informações do serviço de nomes devem ser mantidas sincronizadas em todas as fontes.

Configure a tabela do switch do serviço de nomes

Você deve configurar a tabela de switch de serviço de nomes corretamente para permitir que o ONTAP consulte serviços de nome locais ou externos para recuperar informações de mapeamento de host, usuário, grupo, netgroup ou nome.

O que você vai precisar

Você deve ter decidido quais serviços de nome deseja usar para o mapeamento de host, usuário, grupo,

grupo de rede ou nome, conforme aplicável ao seu ambiente.

Se você planeja usar netgroups, todos os endereços IPv6 especificados em netgroups devem ser encurtados e compatados conforme especificado no RFC 5952.

Sobre esta tarefa

Não inclua fontes de informação que não estejam a ser utilizadas. Por exemplo, se o NIS não estiver sendo usado em seu ambiente, não especifique a `-sources nis` opção.

Passos

1. Adicione as entradas necessárias à tabela do switch de serviço de nomes:

   `vserver services name-service ns-switch create -vserver` *`vserver_name`* `-database` *`database_name`* `-sources` *`source_names`*

2. Verifique se a tabela do switch de serviço de nomes contém as entradas esperadas na ordem desejada:

   `vserver services name-service ns-switch show -vserver` *`vserver_name`*

   Se pretender efetuar quaisquer correções, tem de utilizar os `vserver services name-service ns-switch modify` comandos ou `vserver services name-service ns-switch delete`.

Exemplo

O exemplo a seguir cria uma nova entrada na tabela de opções de serviço de nomes para o SVM VS1 usar o arquivo netgroup local e um servidor NIS externo para procurar informações de netgroup nessa ordem:

```
cluster::> vserver services name-service ns-switch create -vserver vs1
-database netgroup -sources files,nis
```

Depois de terminar

- Você precisa configurar os serviços de nome especificados para o SVM para fornecer acesso aos dados.
- Se você excluir qualquer serviço de nomes para o SVM, também será necessário removê-lo da tabela de opções de serviços de nomes.

  O acesso do cliente ao sistema de armazenamento pode não funcionar como esperado, se você não conseguir excluir o serviço de nomes da tabela de opções do serviço de nomes.

Configurar usuários e grupos UNIX locais

Configure a visão geral de usuários e grupos UNIX locais

Você pode usar usuários e grupos UNIX locais no SVM para mapeamentos de nomes e autenticação. Você pode criar usuários e grupos UNIX manualmente ou carregar um arquivo contendo usuários ou grupos UNIX a partir de um identificador de recurso uniforme (URI).

Há um limite máximo padrão de 32.768 grupos de usuários UNIX locais e membros de grupo combinados no cluster. O administrador do cluster pode modificar este limite.

Crie um usuário local do UNIX

Você pode usar o `vserver services name-service unix-user create` comando para criar usuários UNIX locais. Um usuário UNIX local é um usuário UNIX criado no SVM como uma opção de serviços de nome UNIX para ser usado no processamento de mapeamentos de nomes.

Passo

1. Criar um usuário local UNIX:

   `vserver services name-service unix-user create -vserver` *`vserver_name`* `-user` *`user_name`* `-id` *`integer`* `-primary-gid` *`integer`* `-full-name` *`full_name`*

   `-user` *`user_name`* especifica o nome de usuário. O comprimento do nome de utilizador tem de ter 64 carateres ou menos.

   `-id` *`integer`* Especifica a ID de usuário que você atribui.

   `-primary-gid` *`integer`* Especifica o ID do grupo principal. Isso adiciona o usuário ao grupo principal. Depois de criar o usuário, você pode adicionar manualmente o usuário a qualquer grupo adicional desejado.

Exemplo

O comando a seguir cria um usuário UNIX local chamado johnm (nome completo "John Miller") no SVM chamado VS1. O usuário tem o ID 123 e o ID do grupo principal 100.

```
node::> vserver services name-service unix-user create -vserver vs1 -user
johnm -id 123
-primary-gid 100 -full-name "John Miller"
```

Carregue usuários UNIX locais a partir de um URI

Como alternativa à criação manual de usuários UNIX locais individuais em SVMs, você pode simplificar a tarefa carregando uma lista de usuários UNIX locais em SVMs a partir de um identificador de recurso uniforme (URI(`vserver services name-service unix-user load-from-uri`)).

Passos

1. Crie um arquivo contendo a lista de usuários UNIX locais que você deseja carregar.

   O arquivo deve conter informações do usuário no formato UNIX `/etc/passwd`:

   `user_name: password: user_ID: group_ID: full_name`

   O comando descarta o valor *`password`* do campo e os valores dos campos após o *`full_name`* campo (*`home_directory`* e *`shell`*).

   O tamanho máximo de ficheiro suportado é de 2,5 MB.

2. Verifique se a lista não contém informações duplicadas.

   Se a lista contiver entradas duplicadas, o carregamento da lista falhará com uma mensagem de erro.

3. Copie o arquivo para um servidor.

   O servidor deve ser acessível pelo sistema de armazenamento em HTTP, HTTPS, FTP ou FTPS.

4. Determine qual é o URI para o arquivo.

   O URI é o endereço que você fornece ao sistema de armazenamento para indicar onde o arquivo está localizado.

5. Carregue o arquivo que contém a lista de usuários UNIX locais em SVMs a partir do URI:

   `vserver services name-service unix-user load-from-uri -vserver` *`vserver_name`* `-uri {ftp|http|ftps|https}://`*`uri`* `-overwrite {true|false}`

   `-overwrite {true false` `especifica se pretende substituir as entradas. A predefinição é` `false`.

Exemplo

O comando a seguir carrega uma lista de usuários UNIX locais do URI `ftp://ftp.example.com/passwd` para o SVM chamado VS1. Os usuários existentes no SVM não são sobrescritos pelas informações do URI.

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

Crie um grupo UNIX local

Você pode usar o `vserver services name-service unix-group create` comando para criar grupos UNIX locais para o SVM. Grupos UNIX locais são usados com usuários UNIX locais.

Passo

1. Criar um grupo UNIX local:

   `vserver services name-service unix-group create -vserver` *`vserver_name`* `-name` *`group_name`* `-id` *`integer`*

   `-name` *`group_name`* especifica o nome do grupo. O comprimento do nome do grupo deve ter 64 carateres ou menos.

   `-id` *`integer`* Especifica o ID do grupo que você atribui.

Exemplo

O comando a seguir cria um grupo local chamado eng no SVM chamado VS1. O grupo tem o ID 101.

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name
eng -id 101
```

Adicione um usuário a um grupo UNIX local

Você pode usar o `vserver services name-service unix-group adduser` comando para adicionar um usuário a um grupo UNIX suplementar que seja local para o SVM.

Passo

1. Adicionar um usuário a um grupo UNIX local:

`vserver services name-service unix-group adduser -vserver` *`vserver_name`* `-name` *`group_name`* `-username` *`user_name`*

`-name` *`group_name`* Especifica o nome do grupo UNIX ao qual o usuário será adicionado, além do grupo principal do usuário.

Exemplo

O comando a seguir adiciona um usuário chamado Max a um grupo UNIX local chamado eng no SVM chamado VS1:

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name
eng
-username max
```

Carregue grupos UNIX locais a partir de um URI

Como alternativa à criação manual de grupos UNIX locais individuais, você pode carregar uma lista de grupos UNIX locais em SVMs a partir de um identificador de recurso uniforme (URI) usando o `vserver services name-service unix-group load-from-uri` comando.

Passos

1. Crie um arquivo contendo a lista de grupos UNIX locais que você deseja carregar.

   O arquivo deve conter informações de grupo no formato UNIX `/etc/group`:

   `group_name: password: group_ID: comma_separated_list_of_users`

   O comando descarta o valor *`password`* do campo.

   O tamanho máximo de ficheiro suportado é de 1 MB.

   O comprimento máximo de cada linha no arquivo de grupo é de 32.768 carateres.

2. Verifique se a lista não contém informações duplicadas.

A lista não deve conter entradas duplicadas, ou então carregar a lista falha. Se já houver entradas presentes no SVM, você deve definir o `-overwrite` parâmetro para `true` substituir todas as entradas existentes pelo novo arquivo ou garantir que o novo arquivo não contenha entradas que dupliquem entradas existentes.

3. Copie o arquivo para um servidor.

   O servidor deve ser acessível pelo sistema de armazenamento em HTTP, HTTPS, FTP ou FTPS.

4. Determine qual é o URI para o arquivo.

   O URI é o endereço que você fornece ao sistema de armazenamento para indicar onde o arquivo está localizado.

5. Carregue o arquivo que contém a lista de grupos UNIX locais no SVM a partir do URI:

   `vserver services name-service unix-group load-from-uri -vserver` *`vserver_name`* `-uri {ftp|http|ftps|https}://`*`uri`* `-overwrite {true|false}`

   `-overwrite true false`especifica se pretende substituir as entradas. A predefinição é `false`. Se você especificar esse parâmetro como `true`, o ONTAP substituirá todo o banco de dados de grupo UNIX local existente do SVM especificado pelas entradas do arquivo que você está carregando.

Exemplo

O comando a seguir carrega uma lista de grupos UNIX locais do URI `ftp://ftp.example.com/group` para o SVM chamado VS1. Os grupos existentes no SVM não são sobrescritos pelas informações do URI.

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1
-uri ftp://ftp.example.com/group -overwrite false
```

Trabalhar com netgroups

Trabalhando com netgroups visão geral

Você pode usar netgroups para autenticação de usuário e para corresponder clientes em regras de política de exportação. Você pode fornecer acesso a netgroups de servidores de nomes externos (LDAP ou NIS) ou pode carregar netgroups de um identificador de recurso uniforme (URI) em SVMs usando o `vserver services name-service netgroup load` comando.

O que você vai precisar

Antes de trabalhar com netgroups, você deve garantir que as seguintes condições sejam atendidas:

- Todos os hosts em netgroups, independentemente da origem (NIS, LDAP ou arquivos locais), devem ter Registros DNS de encaminhamento (A) e reverso (PTR) para fornecer pesquisas de DNS consistentes de encaminhamento e reversão.

  Além disso, se um endereço IP de um cliente tiver vários Registros PTR, todos esses nomes de host devem ser membros do netgroup e ter Registros correspondentes A.

- Os nomes de todos os hosts em netgroups, independentemente de sua origem (NIS, LDAP ou arquivos locais), devem ser corretamente escritos e usar o caso correto. As inconsistências em nomes de host usados em netgroups podem levar a um comportamento inesperado, como verificações de exportação com falha.
- Todos os endereços IPv6 especificados em netgroups devem ser encurtados e compatados conforme especificado no RFC 5952.

  Por exemplo, 2011:hu9:0:0:0:0:3:1 tem de ser encurtado para 2011:hu9::3:1.

Sobre esta tarefa

Quando você trabalha com netgroups, você pode executar as seguintes operações:

- Você pode usar o `vserver export-policy netgroup check-membership` comando para ajudar a determinar se um IP de cliente é membro de um determinado netgroup.
- Você pode usar o `vserver services name-service getxxbyyy netgrp` comando para verificar se um cliente faz parte de um netgroup.

  O serviço subjacente para fazer a pesquisa é selecionado com base na ordem configurada do switch do serviço de nomes.

Carregue netgroups em SVMs

Um dos métodos que você pode usar para combinar clientes em regras de política de exportação é usando hosts listados em netgroups. Você pode carregar netgroups de um URI (identificador de recurso uniforme) em SVMs como uma alternativa ao uso de netgroups armazenados em servidores de nomes externos (`vserver services name-service netgroup load`).

O que você vai precisar

Os arquivos netgroup devem atender aos seguintes requisitos antes de serem carregados em um SVM:

- O arquivo deve usar o mesmo formato de arquivo de texto netgroup apropriado que é usado para preencher NIS.

  O ONTAP verifica o formato do arquivo de texto do netgroup antes de carregá-lo. Se o arquivo contiver erros, ele não será carregado e uma mensagem será exibida indicando as correções que você tem que executar no arquivo. Depois de corrigir os erros, você pode recarregar o arquivo netgroup no SVM especificado.

- Todos os carateres alfabéticos nos nomes de host no arquivo netgroup devem estar em minúsculas.
- O tamanho máximo de ficheiro suportado é de 5 MB.
- O nível máximo suportado para netgroups de aninhamento é 1000.
- Somente nomes de host DNS primários podem ser usados ao definir nomes de host no arquivo netgroup.

  Para evitar problemas de acesso à exportação, os nomes de host não devem ser definidos usando Registros DNS CNAME ou round robin.

- As partes de usuário e domínio de triplos no arquivo netgroup devem ser mantidas vazias porque o ONTAP não as suporta.

Apenas a parte host/IP é suportada.

Sobre esta tarefa

O ONTAP suporta pesquisas netgroup-by-host para o arquivo netgroup local. Depois de carregar o arquivo netgroup, o ONTAP cria automaticamente um mapa netgroup.byhost para ativar as pesquisas netgroup-by-host. Isso pode acelerar significativamente as pesquisas de netgroup locais ao processar regras de política de exportação para avaliar o acesso do cliente.

Passo

1. Carregue netgroups em SVMs a partir de um URI:

   `vserver services name-service netgroup load -vserver` *`vserver_name`* `-source {ftp|http|ftps|https}://`*`uri`*

   Carregar o arquivo netgroup e construir o mapa netgroup.byhost pode levar vários minutos.

   Se quiser atualizar os netgroups, você pode editar o arquivo e carregar o arquivo netgroup atualizado no SVM.

Exemplo

O comando a seguir carrega definições de netgroup no SVM chamado VS1 a partir do URL HTTP `http://intranet/downloads/corp-netgroup`:

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

Verifique o status das definições do netgroup

Depois de carregar netgroups no SVM, você pode usar o `vserver services name-service netgroup status` comando para verificar o status das definições do netgroup. Isso permite determinar se as definições de netgroup são consistentes em todos os nós que fazem backup do SVM.

Passos

1. Defina o nível de privilégio como avançado:

   `set -privilege advanced`

2. Verifique o status das definições do netgroup:

   `vserver services name-service netgroup status`

   Pode apresentar informações adicionais numa vista mais detalhada.

3. Voltar ao nível de privilégio de administrador:

   `set -privilege admin`

Exemplo

Depois que o nível de privilégio é definido, o seguinte comando exibe o status do netgroup para todos os SVMs:

```
vs1::> set -privilege advanced

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

vs1::*> vserver services name-service netgroup status
Virtual
Server    Node            Load Time           Hash Value
--------- --------------- -------------------
--------------------------------
vs1
          node1           9/20/2006 16:04:53
e6cb38ec1396a280c0d2b77e3a84eda2
          node2           9/20/2006 16:06:26
e6cb38ec1396a280c0d2b77e3a84eda2
          node3           9/20/2006 16:08:08
e6cb38ec1396a280c0d2b77e3a84eda2
          node4           9/20/2006 16:11:33
e6cb38ec1396a280c0d2b77e3a84eda2
```

Crie uma configuração de domínio NIS

Se um NIS (Network Information Service) for usado em seu ambiente para serviços de nome, você deverá criar uma configuração de domínio NIS para o SVM usando o `vserver services name-service nis-domain create` comando.

Antes de começar

Todos os servidores NIS configurados devem estar disponíveis e acessíveis antes de configurar o domínio NIS no SVM.

Se você pretende usar NIS para pesquisas de diretório, os mapas em seus servidores NIS não podem ter mais de 1.024 carateres para cada entrada. Não especifique o servidor NIS que não está em conformidade com este limite. Caso contrário, o acesso do cliente dependente de entradas NIS pode falhar.

Sobre esta tarefa

Se o seu banco de dados NIS contiver um `netgroup.byhost` mapa, o ONTAP poderá usá-lo para pesquisas mais rápidas. Os `netgroup.byhost` mapas e `netgroup` no diretório devem ser mantidos sempre sincronizados para evitar problemas de acesso do cliente. A partir do ONTAP 9.7, as entradas do NIS `netgroup.byhost` podem ser armazenadas em cache usando os `vserver services name-service nis-domain netgroup-database` comandos.

O uso do NIS para resolução de nome de host não é suportado.

Passos

1. Criar uma configuração de domínio NIS:

   ```
   vserver services name-service nis-domain create -vserver vs1 -domain
   <domain_name> -nis-servers <IP_addresses>
   ```

   Pode especificar até 10 servidores NIS.

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

2. Verifique se o domínio foi criado:

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

Exemplo

O comando a seguir cria uma configuração de domínio NIS para um domínio NIS chamado `nisdomain` no SVM nomeado `vs1` com um servidor NIS em endereço IP `192.0.2.180` :

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -nis-servers 192.0.2.180
```

Utilize LDAP

Visão geral do uso do LDAP

Se o LDAP for usado no ambiente para serviços de nomes, você precisará trabalhar com o administrador LDAP para determinar os requisitos e as configurações do sistema de storage apropriadas e, em seguida, ativar o SVM como cliente LDAP.

A partir do ONTAP 9.10,1, a vinculação de canal LDAP é suportada por padrão para conexões LDAP do ative Directory e serviços de nome. O ONTAP tentará a vinculação de canais com conexões LDAP somente se o Start-TLS ou LDAPS estiver ativado junto com a segurança da sessão definida para assinar ou selar. Para desativar ou reativar a vinculação de canais LDAP com servidores de nomes, use o `-try-channel -binding` parâmetro com o `ldap client modify` comando.

Para obter mais informações, "2020 requisitos de vinculação de canal LDAP e assinatura LDAP para Windows"consulte .

- Antes de configurar o LDAP para ONTAP, você deve verificar se a implantação do site atende às práticas recomendadas para configuração do servidor LDAP e do cliente. Em especial, devem ser satisfeitas as seguintes condições:
  - O nome de domínio do servidor LDAP deve corresponder à entrada no cliente LDAP.
  - Os tipos de hash de senha do usuário LDAP suportados pelo servidor LDAP devem incluir aqueles suportados pelo ONTAP:
    - CRYPT (todos os tipos) e SHA-1 (SHA, SSHA).
    - A partir do ONTAP 9.8, hashes SHA-2 (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384 e

SSHA-512) também são suportados.

- Se o servidor LDAP exigir medidas de segurança de sessão, você deve configurá-las no cliente LDAP.

  As seguintes opções de segurança de sessão estão disponíveis:

  - Assinatura LDAP (fornece verificação de integridade de dados) e assinatura e vedação LDAP (fornece verificação e criptografia de integridade de dados)
  - INICIE O TLS
  - LDAPS (LDAP sobre TLS ou SSL)
- Para ativar consultas LDAP assinadas e seladas, os seguintes serviços devem ser configurados:
  - Os servidores LDAP devem suportar o mecanismo SASL GSSAPI (Kerberos).
  - Os servidores LDAP devem ter Registros DNS A/AAAA, bem como Registros PTR configurados no servidor DNS.
  - Os servidores Kerberos devem ter Registros SRV presentes no servidor DNS.
- Para ativar o TLS ou LDAPS, os seguintes pontos devem ser considerados.
  - É uma prática recomendada do NetApp usar Iniciar TLS em vez de LDAPS.
  - Se o LDAPS for usado, o servidor LDAP deve estar habilitado para TLS ou SSL no ONTAP 9.5 e posterior. O SSL não é suportado no ONTAP 9.0-9,4.
  - Um servidor de certificados já deve estar configurado no domínio.
- Para ativar a perseguição de referência LDAP (no ONTAP 9.5 e posterior), as seguintes condições devem ser satisfeitas:
  - Ambos os domínios devem ser configurados com uma das seguintes relações de confiança:
    - Bidirecional
    - One-way, onde o primário confia no domínio de referência
    - Pai-filho
  - O DNS deve ser configurado para resolver todos os nomes de servidor referidos.
  - As senhas de domínio devem ser as mesmas para autenticar quando --bind-as-cifs-server definido como true.

  As configurações a seguir não são suportadas com a busca por referência LDAP.

  - Para todas as versões do ONTAP:
    - Clientes LDAP em um SVM admin
  - Para o ONTAP 9.8 e versões anteriores (eles são suportados em 9.9.1 e posteriores):
    - Assinatura e selagem LDAP (a `-session-security` opção)
    - Conexões TLS criptografadas (a `-use-start-tls` opção)
    - Comunicações através da porta LDAPS 636 (a `-use-ldaps-for-ad-ldap` opção)

- Você deve inserir um esquema LDAP ao configurar o cliente LDAP no SVM.

  Na maioria dos casos, um dos esquemas ONTAP padrão será apropriado. No entanto, se o esquema LDAP em seu ambiente for diferente desses, você deverá criar um novo esquema de cliente LDAP para o ONTAP antes de criar o cliente LDAP. Consulte o administrador LDAP sobre os requisitos para o seu

ambiente.

- O uso do LDAP para resolução de nome de host não é suportado.

Para mais informações

- "Relatório técnico do NetApp 4835: Como configurar o LDAP no ONTAP"
- "Instale o certificado de CA raiz autoassinado no SVM"

Crie um novo esquema de cliente LDAP

Se o esquema LDAP no ambiente for diferente dos padrões do ONTAP, você deverá criar um novo esquema de cliente LDAP para o ONTAP antes de criar a configuração do cliente LDAP.

Sobre esta tarefa

A maioria dos servidores LDAP pode usar os esquemas padrão fornecidos pelo ONTAP:

- MS-AD-BIS (o esquema preferido para a maioria dos servidores AD do Windows 2012 e posteriores)
- Ad-IDMU (Windows 2008, Windows 2012 e servidores AD posteriores)
- Ad-SFU (Windows 2003 e servidores AD anteriores)
- RFC-2307 (SERVIDORES LDAP UNIX)

Se você precisar usar um esquema LDAP não padrão, você deve criá-lo antes de criar a configuração do cliente LDAP. Consulte o administrador LDAP antes de criar um novo esquema.

Os esquemas LDAP padrão fornecidos pelo ONTAP não podem ser modificados. Para criar um novo esquema, você cria uma cópia e modifica a cópia de acordo.

Passos

1. Exiba os modelos de esquema de cliente LDAP existentes para identificar o que deseja copiar:

   ```
   vserver services name-service ldap client schema show
   ```

2. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

3. Faça uma cópia de um esquema cliente LDAP existente:

   ```
   vserver services name-service ldap client schema copy -vserver vserver_name
   -schema existing_schema_name -new-schema-name new_schema_name
   ```

4. Modifique o novo esquema e personalize-o para o seu ambiente:

   ```
   vserver services name-service ldap client schema modify
   ```

5. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Crie uma configuração de cliente LDAP

Se você quiser que o ONTAP acesse os serviços LDAP ou ative Directory externos em seu ambiente, primeiro é necessário configurar um cliente LDAP no sistema de armazenamento.

O que você vai precisar

Um dos três primeiros servidores na lista de domínios resolvidos do ative Directory deve estar ativo e fornecendo dados. Caso contrário, esta tarefa falha.

> Existem vários servidores, dos quais mais de dois servidores estão inativos a qualquer momento.

Passos

1. Consulte o administrador LDAP para determinar os valores de configuração apropriados para o `vserver services name-service ldap client create` comando:

   a. Especifique uma conexão baseada em domínio ou baseada em endereço para servidores LDAP.

      As `-ad-domain` opções e `-servers` são mutuamente exclusivas.

      - Utilize a `-ad-domain` opção para ativar a deteção de servidor LDAP no domínio do ative Directory.
        - Você pode usar a `-restrict-discovery-to-site` opção para restringir a descoberta de servidor LDAP ao site padrão CIFS para o domínio especificado. Se você usar essa opção, também precisará especificar o site padrão CIFS com `-default-site`.
      - Você pode usar a `-preferred-ad-servers` opção para especificar um ou mais servidores preferenciais do ative Directory por endereço IP em uma lista delimitada por vírgulas. Depois que o cliente é criado, você pode modificar esta lista usando o `vserver services name-service ldap client modify` comando.
      - Use a `-servers` opção para especificar um ou mais servidores LDAP (ative Directory ou UNIX) por endereço IP em uma lista delimitada por vírgulas.

        > A `-servers` opção está obsoleta no ONTAP 9.2. A partir de ONTAP 9.2, o `-ldap -servers` campo substitui o `-servers` campo. Este campo pode ter um nome de host ou um endereço IP para o servidor LDAP.

   b. Especifique um esquema LDAP padrão ou personalizado.

      A maioria dos servidores LDAP pode usar os esquemas somente leitura padrão fornecidos pelo ONTAP. É melhor usar esses esquemas padrão, a menos que haja um requisito para fazer o contrário. Nesse caso, você pode criar seu próprio esquema copiando um esquema padrão (eles são somente leitura) e, em seguida, modificando a cópia.

      Esquemas predefinidos:

      - MS-AD-BIS

        Baseado em RFC-2307bis, este é o esquema LDAP preferido para a maioria das implantações padrão do Windows 2012 e LDAP posteriores.

- `AD-IDMU`

  Baseado no ative Directory Identity Management para UNIX, esse esquema é apropriado para a maioria dos servidores Windows 2008, Windows 2012 e AD posteriores.

- `AD-SFU`

  Baseado nos Serviços do ative Directory para UNIX, esse esquema é apropriado para a maioria dos servidores do Windows 2003 e AD anteriores.

- `RFC-2307`

  Baseado em RFC-2307 (*an Approach for using LDAP as Network Information Service*), este esquema é apropriado para a maioria dos servidores UNIX AD.

c. Selecione vincular valores.

- `-min-bind-level {anonymous|simple|sasl}` especifica o nível mínimo de autenticação bind.

  O valor padrão é **`anonymous`**.

- `-bind-dn` *`LDAP_DN`* especifica o usuário de vinculação.

  Para servidores do ative Directory, você deve especificar o usuário no formulário conta (DOMÍNIO/usuário) ou principal (user@domain.com). Caso contrário, você deve especificar o usuário em forma de nome distinto.

- `-bind-password` *`password`* especifica a senha de vinculação.

d. Selecione as opções de segurança da sessão, se necessário.

Pode ativar a assinatura e a selagem LDAP ou o LDAP através de TLS, se necessário pelo servidor LDAP.

- `--session-security {none|sign|seal}`

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

  Você também deve definir `-min-bind-level {sasl`, a menos que você queira que a autenticação de vinculação retorne **`anonymous`** ou **`simple`** se a vinculação de assinatura e vedação falhar.

- `-use-start-tls {true|`false`Selecione`

  Se definido como **`true`** e o servidor LDAP o suportar, o cliente LDAP utiliza uma ligação TLS encriptada ao servidor. O valor padrão é **`false`**. Você deve instalar um certificado de CA raiz autoassinado do servidor LDAP para usar essa opção.

Se a VM de armazenamento tiver um servidor SMB adicionado a um domínio e o servidor LDAP for um dos controladores de domínio do domínio inicial do servidor SMB, poderá modificar a `-session-security-for-ad-ldap` opção utilizando o `vserver cifs security modify` comando.

e. Selecione valores de porta, consulta e base.

Os valores padrão são recomendados, mas você deve verificar com o administrador LDAP se eles são apropriados para o seu ambiente.

- `-port` *`port`* Especifica a porta do servidor LDAP.

  O valor padrão é `389`.

Se pretender utilizar Iniciar TLS para proteger a ligação LDAP, tem de utilizar a porta predefinida 389. Iniciar TLS começa como uma conexão de texto simples através da porta padrão LDAP 389, e essa conexão é então atualizada para TLS. Se você alterar a porta, Iniciar TLS falhará.

- `-query-timeout` *`integer`* especifica o tempo limite da consulta em segundos.

  O intervalo permitido é de 1 a 10 segundos. O valor padrão é `3` segundos.

- `-base-dn` *`LDAP_DN`* Especifica o DN base.

  Vários valores podem ser inseridos se necessário (por exemplo, se a busca por referência LDAP estiver ativada). O valor padrão é `""` (root).

- `-base-scope` {`base`|`onelevel`|`subtree`especifica o escopo de pesquisa base.

  O valor padrão é `subtree`.

- `-referral-enabled` {`true`|`false`Especifica se a busca por referência LDAP está ativada.

  A partir do ONTAP 9.5, isso permite que o cliente LDAP ONTAP consulte solicitações de pesquisa para outros servidores LDAP se uma resposta de referência LDAP for retornada pelo servidor LDAP primário indicando que os Registros desejados estão presentes nos servidores LDAP referidos. O valor padrão é **`false`**.

Para pesquisar Registros presentes nos servidores LDAP referidos, o base-DN dos Registros referidos deve ser adicionado ao base-DN como parte da configuração do cliente LDAP.

2. Crie uma configuração de cliente LDAP na VM de armazenamento:

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```

Você deve fornecer o nome da VM de armazenamento ao criar uma configuração de cliente LDAP.

3. Verifique se a configuração do cliente LDAP foi criada com sucesso:

```
vserver services name-service ldap client show -client-config
client_config_name
```

Exemplos

O comando a seguir cria uma nova configuração de cliente LDAP chamada ldap1 para que a VM de armazenamento VS1 funcione com um servidor do ative Directory para LDAP:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

O comando a seguir cria uma nova configuração de cliente LDAP chamada ldap1 para que a VM de armazenamento VS1 funcione com um servidor do ative Directory para LDAP no qual a assinatura e a vedação são necessárias, e a descoberta de servidor LDAP é restrita a um site específico para o domínio especificado:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

O comando a seguir cria uma nova configuração de cliente LDAP chamada ldap1 para que a VM de armazenamento VS1 funcione com um servidor do ative Directory para LDAP onde a busca por referência LDAP é necessária:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

O comando a seguir modifica a configuração do cliente LDAP chamada ldap1 para a VM de armazenamento VS1 especificando o DN base:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

O comando a seguir modifica a configuração do cliente LDAP chamada ldap1 para a VM de armazenamento VS1, ativando a busca de referência:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com"  -referral-enabled true
```

Associe a configuração do cliente LDAP a SVMs

Para ativar o LDAP em um SVM, você deve usar o `vserver services name-service ldap create` comando para associar uma configuração de cliente LDAP ao SVM.

O que você vai precisar

- Um domínio LDAP já deve existir na rede e deve estar acessível ao cluster no qual o SVM está localizado.
- Uma configuração de cliente LDAP deve existir no SVM.

Passos

1. Ative o LDAP no SVM:

   `vserver services name-service ldap create -vserver` *`vserver_name`* `-client-config` *`client_config_name`*

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

   O comando a seguir habilita o LDAP no "VS1"SVM e o configura para usar a configuração de cliente LDAP "ldap1":

   ```
   cluster1::> vserver services name-service ldap create -vserver vs1
   -client-config ldap1 -client-enabled true
   ```

2. Valide o status dos servidores de nomes usando o comando de verificação ldap do serviço de nomes dos serviços vserver.

   O comando a seguir valida servidores LDAP no SVM VS1.

```
cluster1::> vserver services name-service ldap check -vserver vs1

| Vserver: vs1                                                    |
| Client Configuration Name: c1                                   |
| LDAP Status: up                                                 |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                   |
```

O comando name Service check está disponível a partir de ONTAP 9.2.

Verifique as fontes LDAP na tabela do switch do serviço de nomes

Você deve verificar se as fontes LDAP para serviços de nome estão listadas corretamente na tabela de opções de serviço de nomes para o SVM.

Passos

1. Exibir o conteúdo da tabela de opções de serviço de nomes atual:

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

   O comando a seguir mostra os resultados do SVM My_SVM:

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
                                Source
Vserver         Database        Order
--------------- ------------    ---------
My_SVM          hosts           files,
                                dns
My_SVM          group           files,ldap
My_SVM          passwd          files,ldap
My_SVM          netgroup        files
My_SVM          namemap         files
5 entries were displayed.
```

   `namemap` especifica as fontes para procurar informações de mapeamento de nomes e em que ordem. Em um ambiente somente UNIX, essa entrada não é necessária. O mapeamento de nomes só é necessário em um ambiente misto usando UNIX e Windows.

2. Atualize a `ns-switch` entrada conforme apropriado:

Se quiser atualizar a entrada ns-switch para…	Digite o comando…
Informações do utilizador	`vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files`

Se quiser atualizar a entrada ns-switch para…	Digite o comando…
Informações do grupo	`vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files`
Informações do netgroup	`vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files`

Use Kerberos com NFS para segurança forte

Visão geral do uso do Kerberos com NFS para segurança forte

Se o Kerberos for usado em seu ambiente para autenticação forte, você precisará trabalhar com o administrador do Kerberos para determinar os requisitos e as configurações apropriadas do sistema de armazenamento e, em seguida, ativar o SVM como um cliente Kerberos.

Seu ambiente deve atender às seguintes diretrizes:

- A implantação do seu site deve seguir as práticas recomendadas para a configuração do servidor Kerberos e do cliente antes de configurar o Kerberos para ONTAP.
- Se possível, use NFSv4 ou posterior se a autenticação Kerberos for necessária.

  NFSv3 pode ser usado com Kerberos. No entanto, os benefícios completos de segurança do Kerberos só são realizados em implantações ONTAP de NFSv4 ou posterior.

- Para promover o acesso redundante ao servidor, o Kerberos deve ser habilitado em várias LIFs de dados em vários nós no cluster usando o mesmo SPN.
- Quando o Kerberos está habilitado no SVM, um dos seguintes métodos de segurança deve ser especificado em regras de exportação para volumes ou qtrees, dependendo da configuração do cliente NFS.
  - `krb5` (Protocolo Kerberos v5)
  - `krb5i` (Protocolo Kerberos v5 com verificação de integridade usando checksums)
  - `krb5p` (Protocolo Kerberos v5 com serviço de privacidade)

Além do servidor Kerberos e clientes, os seguintes serviços externos devem ser configurados para que o ONTAP suporte Kerberos:

- Serviço de diretório

  Você deve usar um serviço de diretório seguro em seu ambiente, como o ative Directory ou o OpenLDAP, configurado para usar LDAP em SSL/TLS. Não use NIS, cujos pedidos são enviados em texto não criptografado e, portanto, não são seguros.

- NTP

Você deve ter um servidor de tempo de trabalho executando NTP. Isso é necessário para evitar a falha de autenticação Kerberos devido ao desvio de tempo.

- Resolução de nome de domínio (DNS)

  Cada cliente UNIX e cada SVM LIF devem ter um Registro de serviço (SRV) adequado registrado no KDC em zonas de pesquisa direta e inversa. Todos os participantes devem ser solucionáveis corretamente via DNS.

Verifique as permissões para a configuração Kerberos

O Kerberos requer que certas permissões UNIX sejam definidas para o volume raiz do SVM e para usuários e grupos locais.

Passos

1. Exiba as permissões relevantes no volume raiz da SVM:

   `volume show -volume` *`root_vol_name`*`-fields user,group,unix-permissions`

   O volume raiz do SVM precisa ter a seguinte configuração:

Nome…	A definir…
UID	Raiz ou ID 0
GID	Raiz ou ID 0
Permissões da UNIX	755

   Se esses valores não forem exibidos, use o `volume modify` comando para atualizá-los.

2. Exibir os usuários locais do UNIX:

   `vserver services name-service unix-user show -vserver` *`vserver_name`*

   O SVM deve ter os seguintes usuários UNIX configurados:

Nome de utilizador	ID de utilizador	ID do grupo principal	Comentário
nfs	500	0	Necessário para a fase INIT do GSS. O primeiro componente do usuário cliente NFS SPN é usado como usuário. O usuário nfs não é necessário se existir um mapeamento de nomes Kerberos-UNIX para o SPN do usuário cliente NFS.
raiz	0	0	Necessário para a montagem.

Se esses valores não forem exibidos, você pode usar o `vserver services name-service unix-user modify` comando para atualizá-los.

3. Exibir os grupos UNIX locais:

   `vserver services name-service unix-group show -vserver` *`vserver`* `_name`

   O SVM deve ter os seguintes grupos UNIX configurados:

Nome do grupo	ID do grupo
daemon	1
raiz	0

Se esses valores não forem exibidos, você pode usar o `vserver services name-service unix-group modify` comando para atualizá-los.

Crie uma configuração NFS Kerberos realm

Se você quiser que o ONTAP acesse servidores Kerberos externos em seu ambiente, primeiro configure o SVM para usar um realm Kerberos existente. Para fazer isso, você precisa reunir valores de configuração para o servidor KDC Kerberos e, em seguida, usar o `vserver nfs kerberos realm create` comando para criar a configuração de realm Kerberos em um SVM.

O que você vai precisar

O administrador do cluster deve ter configurado o NTP no sistema de armazenamento, cliente e servidor KDC para evitar problemas de autenticação. As diferenças de tempo entre um cliente e um servidor (desvio de relógio) são uma causa comum de falhas de autenticação.

Passos

1. Consulte o administrador do Kerberos para determinar os valores de configuração apropriados para fornecer com o `vserver nfs kerberos realm create` comando.
2. Crie uma configuração de realm Kerberos no SVM:

   `vserver nfs kerberos realm create -vserver` *`vserver_name`* `-realm` *`realm_name`* *`{AD_KDC_server_values |AD_KDC_server_values}`* `-comment "`*`text`*`"`

3. Verifique se a configuração do realm Kerberos foi criada com sucesso:

   `vserver nfs kerberos realm show`

Exemplos

O comando a seguir cria uma configuração NFS Kerberos Realm para o SVM VS1 que usa um servidor Microsoft ative Directory como servidor KDC. O Reino Kerberos é AUTH.EXAMPLE.COM. O servidor do ative Directory tem o nome ad-1 e seu endereço IP é 10.10.8.14. O desvio de relógio permitido é de 300 segundos (o padrão). O endereço IP do servidor KDC é 10.10.8.14, e seu número de porta é 88 (o padrão). "Configuração do Microsoft Kerberos" é o comentário.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

O comando a seguir cria uma configuração NFS Kerberos realm para o SVM VS1 que usa um MIT KDC. O Reino Kerberos é SECURITY.EXAMPLE.COM. A inclinação permitida do relógio é de 300 segundos. O endereço IP do servidor KDC é 10.10.9.1, e seu número de porta é 88. O fornecedor KDC é outro para indicar um fornecedor UNIX. O endereço IP do servidor administrativo é 10.10.9.1, e seu número de porta é 749 (o padrão). O endereço IP do servidor de senhas é 10.10.9.1, e seu número de porta é 464 (o padrão). "UNIX Kerberos config" é o comentário.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

Configurar os tipos de criptografia permitidos do NFS Kerberos

Por padrão, o ONTAP oferece suporte aos seguintes tipos de criptografia para o Kerberos NFS: DES, 3DES, AES-128 e AES-256. Você pode configurar os tipos de criptografia permitidos para cada SVM de acordo com os requisitos de segurança do seu ambiente específico usando o `vserver nfs modify` comando com o `-permitted -enc-types` parâmetro.

Sobre esta tarefa

Para maior compatibilidade com clientes, o ONTAP suporta criptografia DES fraca e AES forte por padrão. Isso significa, por exemplo, que se você quiser aumentar a segurança e seu ambiente a suportar, você pode usar este procedimento para desativar DES e 3DES e exigir que os clientes usem apenas criptografia AES.

Você deve usar a criptografia mais forte disponível. Para ONTAP, isso é AES-256. Deve confirmar com o administrador do KDC que este nível de encriptação é suportado no seu ambiente.

- Ativar ou desativar totalmente AES (AES-128 e AES-256) em SVMs é disruptivo porque destrói o arquivo DES principal/keytab original, exigindo assim que a configuração Kerberos seja desativada em todos os LIFs para o SVM.

  Antes de fazer essa alteração, você deve verificar se os clientes NFS não dependem da criptografia AES no SVM.

- Ativar ou desativar DES ou 3DES não requer alterações na configuração Kerberos em LIFs.

Passo

1. Ative ou desative o tipo de encriptação permitido que pretende:

Se quiser ativar ou desativar…	Siga estes passos…
DES ou 3DES	a. Configure os tipos de criptografia permitidos do NFS Kerberos da SVM `vserver nfs modify -vserver` *`vserver_name`* `-permitted -enc-types` *`encryption_types`* Separe vários tipos de criptografia com uma vírgula. b. Verifique se a alteração foi bem-sucedida `vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`

Se quiser ativar ou desativar…	Siga estes passos…
AES-128 ou AES-256	a. Identifique em que SVM e LIF Kerberos estão ativados `vserver nfs kerberos interface show` b. Desative o Kerberos em todos os LIFs no SVM cujo tipo de criptografia NFS Kerberos permitido você deseja modificar `vserver nfs kerberos interface disable -lif` *`lif_name`* c. Configure os tipos de criptografia permitidos do NFS Kerberos da SVM `vserver nfs modify -vserver` *`vserver_name`* `-permitted -enc-types` *`encryption_types`* Separe vários tipos de criptografia com uma vírgula. d. Verifique se a alteração foi bem-sucedida `vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types` e. Reative o Kerberos em todos os LIFs na SVM `vserver nfs kerberos interface enable -lif` *`lif_name`* `-spn` *`service_principal_name`* f. Verifique se o Kerberos está ativado em todos os LIFs `vserver nfs kerberos interface show`

Ative o Kerberos em um LIF de dados

Você pode usar o `vserver nfs kerberos interface enable` comando para habilitar o Kerberos em um LIF de dados. Isso permite que o SVM use os serviços de segurança Kerberos para NFS.

Sobre esta tarefa

Se você estiver usando um KDC do ative Directory, os primeiros 15 carateres de qualquer SPNs usados devem ser exclusivos em SVMs dentro de um Reino ou domínio.

Passos

1. Crie a configuração NFS Kerberos:

   `vserver nfs kerberos interface enable -vserver` *`vserver_name`* `-lif` *`logical_interface`* `-spn` *`service_principal_name`*

   O ONTAP requer a chave secreta para o SPN do KDC para habilitar a interface Kerberos.

   Para os KDCs da Microsoft, o KDC é contatado e um prompt de nome de usuário e senha são emitidos na

CLI para obter a chave secreta. Se você precisar criar o SPN em uma ou diferente do realm Kerberos, você poderá especificar o parâmetro opcional `-ou`.

Para KDCs não Microsoft, a chave secreta pode ser obtida usando um de dois métodos:

Se você…	Você também deve incluir o seguinte parâmetro com o comando…
Peça às credenciais do administrador do KDC para recuperar a chave diretamente do KDC	`-admin-username` *`kdc_admin_username`*
Não tem as credenciais de administrador do KDC, mas tem um arquivo keytab do KDC que contém a chave	`-keytab-uri` digite seu comentário aqui:// *`uri`*

2. Verifique se o Kerberos foi ativado no LIF:

   ```
   vserver nfs kerberos-config show
   ```

3. Repita as etapas 1 e 2 para ativar o Kerberos em várias LIFs.

Exemplo

O comando a seguir cria e verifica uma configuração NFS Kerberos para o SVM chamado VS1 na interface lógica ves03-D1, com o SPN nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM na ou lab2ou:

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
        Logical
Vserver Interface Address       Kerberos  SPN
------- --------- -------       --------- ------------------------------
vs0     ves01-a1
                  10.10.10.30   disabled  -
vs2     ves01-d1
                  10.10.10.40   enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

Use o TLS com NFS para ter uma segurança forte

Visão geral do uso do TLS com NFS para uma segurança forte

O TLS permite comunicações de rede criptografadas com segurança equivalente e menos complexidade do que o Kerberos e o IPsec. Como administrador, você pode habilitar, configurar e desabilitar o TLS para segurança forte com conexões NFSv3 e NFSv4.x usando o Gerenciador de sistema, a CLI do ONTAP ou a API REST do ONTAP.

O NFS em TLS está disponível no ONTAP 9.15,1 como prévia pública. Como oferta de prévia, o NFS em TLS não é compatível com workloads de produção no ONTAP 9.15,1.

O ONTAP usa o TLS 1,3 para conexões NFS em TLS.

Requisitos

O NFS em TLS requer certificados X,509. Você pode criar e instalar um certificado de servidor assinado pela CA no cluster do ONTAP ou instalar um certificado que o serviço NFS usa diretamente. Seus certificados devem atender às seguintes diretrizes:

- O nome comum (CN) de cada certificado deve ser configurado com o nome de domínio totalmente qualificado (FQDN) do LIF de dados no qual o TLS será ativado.
- O nome alternativo do assunto (SAN) de cada certificado deve ser configurado com o endereço IP do LIF de dados no qual o TLS será ativado. Opcionalmente, você também pode adicionar FQDN do LIF de dados. Se o endereço IP e o FQDN estiverem configurados, os clientes NFS podem se conetar usando o endereço IP ou o FQDN.
- Você pode instalar vários certificados de serviço NFS para o mesmo LIF, mas apenas um deles pode ser usado de cada vez como parte da configuração TLS NFS.

Ativar ou desativar TLS para clientes NFS no ONTAP

Você pode ativar ou desativar o TLS em um data LIF para clientes NFS. Quando você ativa o NFS em TLS, o SVM usa o TLS para criptografar todos os dados enviados pela rede entre o cliente NFS e o ONTAP. Isso aumenta a segurança das conexões NFS.

O NFS em TLS está disponível no ONTAP 9.15,1 como prévia pública. Como oferta de prévia, o NFS em TLS não é compatível com workloads de produção no ONTAP 9.15,1.

Ativar TLS

Você pode habilitar a criptografia TLS para clientes NFS para aumentar a segurança dos dados em trânsito.

Antes de começar

- Consulte "requisitos"o para NFS sobre TLS antes de começar.
- Saiba mais sobre `vserver nfs tls interface enable` o "Referência do comando ONTAP"na .

Passos

1. Escolha uma VM de armazenamento e uma interface lógica (LIF) na qual ativar o TLS.
2. Habilite o TLS para conexões NFS nessa VM e interface de storage. Substitua os valores entre parêntesis> por informações do seu ambiente:

```
vserver nfs tls interface enable -vserver <STORAGE_VM> -lif <LIF_NAME>
-certificate-name <CERTIFICATE_NAME>
```

3. Use o `vserver nfs tls interface show` comando para visualizar os resultados:

```
vserver nfs tls interface show
```

Exemplo

O comando a seguir habilita o NFS sobre TLS no `data1` LIF da `vs1` VM de storage:

```
vserver nfs tls interface enable -vserver vs1 -lif data1 -certificate-name
cert_vs1
```

```
vserver nfs tls interface show
```

```
               Logical
Vserver        Interface     Address         TLS Status TLS Certificate
Name
-------------- ------------- --------------- ----------
-----------------------
vs1            data1         10.0.1.1        enabled    cert_vs1
vs2            data2         10.0.1.2        disabled   -
2 entries were displayed.
```

Desativar TLS

Você pode desativar o TLS para clientes NFS se não precisar mais da segurança aprimorada para dados em trânsito.

> Quando você desativa o NFS em TLS, o certificado TLS usado para a conexão NFS é removido. Se você precisar habilitar o NFS em TLS no futuro, precisará especificar novamente um nome de certificado durante a capacitação.

Antes de começar

Saiba mais sobre `vserver nfs tls interface disable` o "Referência do comando ONTAP"na .

Passos

1. Escolha uma VM de armazenamento e uma interface lógica (LIF) para desativar o TLS.
2. Desative TLS para conexões NFS nessa VM e interface de storage. Substitua os valores entre parêntesis> por informações do seu ambiente:

```
vserver nfs tls interface disable -vserver <STORAGE_VM> -lif <LIF_NAME>
```

3. Use o `vserver nfs tls interface show` comando para visualizar os resultados:

```
vserver nfs tls interface show
```

Exemplo

O comando a seguir desativa NFS sobre TLS no `data1` LIF da `vs1` VM de armazenamento:

```
vserver nfs tls interface disable -vserver vs1 -lif data1
```

```
vserver nfs tls interface show
```

```
               Logical
Vserver        Interface     Address         TLS Status TLS Certificate
Name
-------------- ------------- --------------- ----------
-----------------------
vs1            data1         10.0.1.1        disabled   -
vs2            data2         10.0.1.2        disabled   -
2 entries were displayed.
```

Editar uma configuração TLS

Você pode alterar as configurações de uma configuração NFS em TLS existente. Por exemplo, você pode usar este procedimento para atualizar o certificado TLS.

Antes de começar

Saiba mais sobre `vserver nfs tls interface modify` o "Referência do comando ONTAP"na .

Passos

1. Escolha uma VM de storage e uma interface lógica (LIF) para modificar a configuração TLS para clientes NFS.
2. Modificar a configuração. Se especificar um `status` de `enable`, também terá de especificar o `certificate-name` parâmetro. Substitua os valores entre parêntesis> por informações do seu ambiente:

```
vserver nfs tls interface modify -vserver <STORAGE_VM> -lif <LIF_NAME>
-status <STATUS> -certificate-name <CERTIFICATE_NAME>
```

3. Use o `vserver nfs tls interface show` comando para visualizar os resultados:

```
vserver nfs tls interface show
```

Exemplo

O comando a seguir modifica a configuração NFS sobre TLS no `data2` LIF da `vs2` VM de armazenamento:

```
vserver nfs tls interface modify -vserver vs2 -lif data2 -status enable
-certificate-name new_cert
```

```
vserver nfs tls interface show
```

```
               Logical
Vserver        Interface     Address         TLS Status TLS Certificate
Name
-------------- ------------- --------------- ----------
-----------------------
vs1            data1         10.0.1.1        disabled   -
vs2            data2         10.0.1.2        enabled    new_cert
2 entries were displayed.
```

Informações sobre direitos autorais

Informações sobre marcas comerciais