Gerenciar o acesso a arquivos usando NFS

ONTAP 9

NetApp
January 17, 2025

Índice

Gerenciar o acesso a arquivos usando NFS

Ativar ou desativar NFSv3

Pode ativar ou desativar o NFSv3 modificando a `-v3` opção. Isto permite o acesso a ficheiros para clientes que utilizam o protocolo NFSv3. Por padrão, NFSv3 está ativado.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Ativar NFSv3	`vserver nfs modify -vserver vserver_name -v3 enabled`
Desativar NFSv3	`vserver nfs modify -vserver vserver_name -v3 disabled`

Ativar ou desativar NFSv4,0

Pode ativar ou desativar o NFSv4,0 modificando a `-v4.0` opção. Isto permite o acesso a ficheiros para clientes que utilizam o protocolo NFSv4,0. No ONTAP 9.9,1, o NFSv4,0 é ativado por padrão; em versões anteriores, ele é desativado por padrão.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	**Digite o seguinte comando…**
Ativar NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 enabled`
Desativar NFSv4,0	`vserver nfs modify -vserver vserver_name -v4.0 disabled`

Ativar ou desativar NFSv4,1

Pode ativar ou desativar o NFSv4,1 modificando a `-v4.1` opção. Isto permite o acesso a ficheiros para clientes que utilizam o protocolo NFSv4,1. No ONTAP 9.9,1, o NFSv4,1 é ativado por padrão; em versões anteriores, ele é desativado por padrão.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Digite o seguinte comando…
Ativar NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 enabled`
Desativar NFSv4,1	`vserver nfs modify -vserver vserver_name -v4.1 disabled`

Gerenciar NFSv4 limites de storepool

A partir do ONTAP 9.13, os administradores podem habilitar seus servidores NFSv4 para negar recursos a clientes NFSv4 quando eles tiverem atingido os limites de recursos do storepool de clientes. Quando os clientes consomem muitos recursos do storepool de NFSv4 isso pode levar a outros clientes NFSv4 serem bloqueados devido à indisponibilidade de recursos do storepool de NFSv4.

Ativar esse recurso também permite que os clientes visualizem o consumo de recursos do storepool ativo por cada cliente. Isso facilita a identificação de clientes que esgotam os recursos do sistema e possibilita impor limites de recursos por cliente.

Veja os recursos do storepool consumidos

O `vserver nfs storepool show` comando mostra o número de recursos do storepool consumidos. Um storepool é um pool de recursos usado por clientes NFSv4.

Passo

1. Como administrador, execute o `vserver nfs storepool show` comando para exibir as informações do storepool de clientes NFSv4.

Exemplo

Este exemplo exibe as informações do storepool de clientes NFSv4.

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-Ip: 10.0.1.1

Client-Ip Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount

-------------- --------- --------- ---------- ---------- ----------
---------

10.0.2.1          nfs4.1     true    2 1 0 4

10.0.2.2          nfs4.2     true    2 1 0 4

2 entries were displayed.
```

Ative ou desative os controles de limite do storepool

Os administradores podem usar os seguintes comandos para ativar ou desativar os controles de limite do storepool.

Passo

1. Como administrador, execute uma das seguintes ações:

Se você quiser…	Digite o seguinte comando…
Ative os controles de limite do storepool	`vserver nfs storepool config modify -limit-enforce enabled`
Desative os controles de limite do storepool	`vserver nfs storepool config modify -limit-enforce disabled`

Exibir uma lista de clientes bloqueados

Se o limite storepool estiver ativado, os administradores poderão ver quais clientes foram bloqueados ao atingir o limite de recursos por cliente. Os administradores podem usar o seguinte comando para ver quais clientes foram marcados como clientes bloqueados.

Passos

1. Use o `vserver nfs storepool blocked-client show` comando para exibir a lista de clientes bloqueados do NFSv4.

Remova um cliente da lista de clientes bloqueados

Os clientes que atingirem seu limite por cliente serão desconetados e adicionados ao cache block-client. Os administradores podem usar o seguinte comando para remover o cliente do cache de cliente de bloco. Isso permitirá que o cliente se conete ao servidor ONTAP NFSv4.

Passos

1. Use o `vserver nfs storepool blocked-client flush -client-ip <ip address>` comando para lavar o cache de cliente bloqueado storepool.
2. Use o `vserver nfs storepool blocked-client show` comando para verificar se o cliente foi removido do cache de cliente de bloco.

Exemplo

Este exemplo exibe um cliente bloqueado com o endereço IP "10,2.1,1" sendo lavado de todos os nós.

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
----------
10.1.1.1

1 entries were displayed.
```

Ative ou desative o pNFS

O pNFS melhora o desempenho permitindo que os clientes NFS executem operações de leitura/gravação em dispositivos de storage diretamente e em paralelo, ignorando o servidor NFS como um potencial gargalo. Para ativar ou desativar pNFS (NFS paralelo), pode modificar a `-v4.1-pnfs` opção.

Se a versão ONTAP for…	O padrão pNFS é…
9,8 ou posterior	desativado
9,7 ou anterior	ativado

O que você vai precisar

O suporte NFSv4,1 é necessário para poder usar o pNFS.

Se você quiser ativar o pNFS, primeiro você deve desativar as referências NFS. Ambos não podem ser ativados ao mesmo tempo.

Se você usar pNFS com Kerberos em SVMs, você deverá habilitar o Kerberos em cada LIF na SVM.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Ativar pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled`
Desativar pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled`

Informações relacionadas

- Visão geral do trunking NFS

Controle o acesso NFS por TCP e UDP

Você pode ativar ou desativar o acesso NFS a máquinas virtuais de armazenamento (SVMs) em TCP e UDP, modificando os `-tcp` parâmetros e `-udp`, respetivamente. Isso permite que você controle se os clientes NFS podem acessar dados via TCP ou UDP em seu ambiente.

Sobre esta tarefa

Estes parâmetros aplicam-se apenas ao NFS. Não afetam protocolos auxiliares. Por exemplo, se o NFS sobre TCP estiver desativado, as operações de montagem sobre TCP ainda terão êxito. Para bloquear completamente o tráfego TCP ou UDP, você pode usar regras de política de exportação.

> Você deve desativar o SnapDiff RPC Server antes de desativar o TCP para NFS para evitar um erro de falha de comando. Você pode desativar o TCP usando o comando `vserver snapdiff-rpc-server off -vserver vserver name`.

Passo

1. Execute uma das seguintes ações:

Se você quiser que o acesso NFS seja…	Digite o comando…
Ativado em TCP	`vserver nfs modify -vserver vserver_name -tcp enabled`
Desativado por TCP	`vserver nfs modify -vserver vserver_name -tcp disabled`
Ativado em UDP	`vserver nfs modify -vserver vserver_name -udp enabled`
Desativado por UDP	`vserver nfs modify -vserver vserver_name -udp disabled`

Controle solicitações NFS de portas não reservadas

Você pode rejeitar solicitações de montagem NFS de portas não reservadas habilitando a `-mount-rootonly` opção. Para rejeitar todas as solicitações NFS de portas não reservadas, você pode ativar a `-nfs-rootonly` opção.

Sobre esta tarefa

Por padrão, a opção `-mount-rootonly` é `enabled`.

Por padrão, a opção `-nfs-rootonly` é `disabled`.

Estas opções não se aplicam ao procedimento NULL.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Permitir solicitações de montagem NFS de portas não reservadas	`vserver nfs modify -vserver vserver_name -mount -rootonly disabled`
Rejeitar solicitações de montagem NFS de portas não reservadas	`vserver nfs modify -vserver vserver_name -mount -rootonly enabled`
Permitir todas as solicitações NFS de portas não reservadas	`vserver nfs modify -vserver vserver_name -nfs -rootonly disabled`
Rejeitar todas as solicitações NFS de portas não reservadas	`vserver nfs modify -vserver vserver_name -nfs -rootonly enabled`

Lidar com o acesso NFS a volumes NTFS ou qtrees para usuários UNIX desconhecidos

Se o ONTAP não conseguir identificar usuários UNIX tentando se conetar a volumes ou qtrees com estilo de segurança NTFS, ele não poderá mapear explicitamente o usuário para um usuário do Windows. Você pode configurar o ONTAP para negar acesso a esses usuários para segurança mais rigorosa ou mapeá-los para um usuário padrão do Windows para garantir um nível mínimo de acesso para todos os usuários.

O que você vai precisar

Um usuário padrão do Windows deve ser configurado se você quiser habilitar essa opção.

Sobre esta tarefa

Se um usuário UNIX tentar acessar volumes ou qtrees com estilo de segurança NTFS, o usuário UNIX deve primeiro ser mapeado para um usuário do Windows para que o ONTAP possa avaliar adequadamente as permissões NTFS. No entanto, se o ONTAP não conseguir procurar o nome do usuário UNIX nas fontes de

serviço de nome de informações de usuário configuradas, ele não poderá mapear explicitamente o usuário UNIX para um usuário específico do Windows. Você pode decidir como lidar com esses usuários UNIX desconhecidos das seguintes maneiras:

- Negar acesso a usuários UNIX desconhecidos.

  Isso impõe segurança mais rigorosa, exigindo mapeamento explícito para todos os usuários UNIX para obter acesso a volumes NTFS ou qtrees.

- Mapeie usuários UNIX desconhecidos para um usuário padrão do Windows.

  Isso fornece menos segurança, mas mais conveniência, garantindo que todos os usuários obtenham um nível mínimo de acesso a volumes NTFS ou qtrees por meio de um usuário padrão do Windows.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute uma das seguintes ações:

Se você quiser o usuário padrão do Windows para usuários UNIX desconhecidos…	Digite o comando…
Ativado	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled`
Desativado	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled`

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Considerações para clientes que montam exportações NFS usando uma porta não reservada

A `-mount-rootonly` opção deve ser desativada em um sistema de armazenamento que deve suportar clientes que montam exportações NFS usando uma porta não reservada mesmo quando o usuário está conetado como raiz. Tais clientes incluem clientes Hummingbird e clientes Solaris NFS/IPv6.

Se a `-mount-rootonly` opção estiver ativada, o ONTAP não permitirá que clientes NFS que usam portas não reservadas, ou seja, portas com números superiores a 1.023, montem exportações NFS.

Execute uma verificação de acesso mais rigorosa para netgroups verificando domínios

Por padrão, o ONTAP executa uma verificação adicional ao avaliar o acesso do cliente para um netgroup. A verificação adicional garante que o domínio do cliente corresponda à configuração do domínio da máquina virtual de armazenamento (SVM). Caso contrário, o ONTAP nega acesso ao cliente.

Sobre esta tarefa

Quando o ONTAP avalia regras de política de exportação para acesso de cliente e uma regra de política de exportação contém um netgroup, o ONTAP deve determinar se o endereço IP de um cliente pertence ao netgroup. Para isso, o ONTAP converte o endereço IP do cliente para um nome de host usando DNS e obtém um nome de domínio totalmente qualificado (FQDN).

Se o arquivo netgroup apenas listar um nome curto para o host e o nome curto para o host existir em vários domínios, é possível que um cliente de um domínio diferente obtenha acesso sem essa verificação.

Para evitar isso, o ONTAP compara o domínio retornado do DNS para o host com a lista de nomes de domínio DNS configurados para o SVM. Se corresponder, o acesso é permitido. Se não corresponder, o acesso é negado.

Esta verificação está ativada por predefinição. Você pode gerenciá-lo modificando o `-netgroup-dns -domain-search` parâmetro, que está disponível no nível de privilégio avançado.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute a ação desejada:

Se você deseja que a verificação de domínio para netgroups seja…	Digite…
Ativado	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled`
Desativado	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled`

3. Defina o nível de privilégio como admin:

   ```
   set -privilege admin
   ```

Modifique as portas usadas para serviços NFSv3

O servidor NFS no sistema de armazenamento usa serviços como o daemon de

montagem e o Gerenciador de bloqueio de rede para se comunicar com clientes NFS através de portas de rede padrão específicas. Na maioria dos ambientes NFS, as portas padrão funcionam corretamente e não exigem modificação, mas se você quiser usar diferentes portas de rede NFS em seu ambiente NFSv3, você pode fazer isso.

O que você vai precisar

A alteração das portas NFS no sistema de storage exige que todos os clientes NFS se reconetem ao sistema. Portanto, você deve comunicar essas informações aos usuários antes de fazer a alteração.

Sobre esta tarefa

Você pode definir as portas usadas pelos serviços de daemon de montagem NFS, Network Lock Manager, Network Status Monitor e NFS quota daemon para cada máquina virtual de armazenamento (SVM). A alteração do número da porta afeta os clientes NFS que acessam dados por TCP e UDP.

As portas para NFSv4 e NFSv4,1 não podem ser alteradas.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Desativar o acesso ao NFS:

   ```
   vserver nfs modify -vserver vserver_name -access false
   ```

3. Defina a porta NFS para o serviço NFS específico:

   ```
   vserver nfs modify -vserver vserver_namenfs_port_parameterport_number
   ```

Parâmetro da porta NFS	Descrição	Porta predefinida
`-mountd-port`	Daemon de montagem NFS	635
`-nlm-port`	Gerenciador de bloqueio de rede	4045
`-nsm-port`	Monitor de estado da rede	4046
`-rquotad-port`	Daemon de cota NFS	4049

   Além da porta padrão, o intervalo permitido de números de porta é de 1024 a 65535. Cada serviço NFS precisa usar uma porta única.

4. Ativar acesso ao NFS:

   ```
   vserver nfs modify -vserver vserver_name -access true
   ```

5. Use o `network connections listening show` comando para verificar as alterações no número da porta.
6. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Exemplo

Os comandos a seguir definem a porta NFS Mount Daemon como 1113 no SVM chamado VS1:

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true

vs1::*> network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: cluster1-01
Cluster          cluster1-01_clus_1:7700          TCP/ctlopcp
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:1113                       TCP/mount
vs1              data1:1113                       UDP/mount
...
vs1::*> set -privilege admin
```

Comandos para gerenciar servidores NFS

Existem comandos ONTAP específicos para gerenciar servidores NFS.

Se você quiser…	Use este comando…
Crie um servidor NFS	`vserver nfs create`
Exibir servidores NFS	`vserver nfs show`
Modificar um servidor NFS	`vserver nfs modify`
Excluir um servidor NFS	`vserver nfs delete`

Oculte a `.snapshot` lista de diretórios em NFSv3 pontos de montagem O acesso explícito ao `.snapshot` diretório ainda será permitido mesmo que a opção esteja ativada.	`vserver nfs` comandos com a `-v3-hide-snapshot` opção ativada

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

Solucionar problemas do serviço de nomes

Quando os clientes experimentam falhas de acesso devido a problemas de serviço de nome, você pode usar a `vserver services name-service getxxbyyy` família de comandos para executar manualmente várias pesquisas de serviço de nome e examinar os detalhes e resultados da pesquisa para ajudar na solução de problemas.

Sobre esta tarefa

- Para cada comando, você pode especificar o seguinte:
  - Nome do nó ou da máquina virtual de storage (SVM) para realizar a pesquisa.

    Isso permite testar pesquisas de serviços de nomes para um nó específico ou SVM para restringir a pesquisa de um possível problema de configuração de serviço de nomes.
  - Se deve mostrar a fonte usada para a pesquisa.

    Isso permite verificar se a fonte correta foi usada.
- O ONTAP seleciona o serviço para realizar a pesquisa com base na ordem configurada do switch do serviço de nomes.
- Esses comandos estão disponíveis no nível avançado de privilégio.

Passos

1. Execute uma das seguintes ações:

Para recuperar…	Use o comando…
Endereço IP de um nome de host	`vserver services name-service getxxbyyy getaddrinfo` `vserver services name-service getxxbyyy gethostbyname` (Apenas endereços IPv4)
Membros de um grupo por ID de grupo	`vserver services name-service getxxbyyy getgrbygid`

Membros de um grupo por nome de grupo	`vserver services name-service getxxbyyy getgrbyname`
Lista de grupos aos quais um usuário pertence	`vserver services name-service getxxbyyy getgrlist`
Nome do host de um endereço IP	`vserver services name-service getxxbyyy getnameinfo` `vserver services name-service getxxbyyy gethostbyaddr` (Apenas endereços IPv4)
Informações do usuário por nome de usuário	`vserver services name-service getxxbyyy getpwbyname` É possível testar a resolução de nomes de usuários do RBAC especificando o `-use-rbac` parâmetro como `true`.
Informações do usuário por ID do usuário	`vserver services name-service getxxbyyy getpwbyuid` É possível testar a resolução de nomes de usuários do RBAC especificando o `-use-rbac` parâmetro como `true`.
A associação netgroup de um cliente	`vserver services name-service getxxbyyy netgrp`
A associação netgroup de um cliente usando a pesquisa netgroup-by-host	`vserver services name-service getxxbyyy netgrpbyhost`

O exemplo a seguir mostra um teste de pesquisa de DNS para o SVM VS1 ao tentar obter o endereço IP do host acast1.eng.example.com:

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

O exemplo a seguir mostra um teste de pesquisa NIS para o SVM VS1 ao tentar recuperar informações de usuário para um usuário com o UID 501768:

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvc2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

O exemplo a seguir mostra um teste de pesquisa LDAP para o SVM VS1 ao tentar recuperar informações de usuário para um usuário com o nome ldap1:

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

O exemplo a seguir mostra um teste de pesquisa de netgroup para o SVM VS1 ao tentar descobrir se o cliente dnshost0 é membro do netgroup lnetgroup136:

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. Analise os resultados do teste realizado e tome a ação necessária.

Se o…	Veja o…
A pesquisa de nome de host ou endereço IP falhou ou gerou resultados incorretos	Configuração DNS
A pesquisa consultou uma fonte incorreta	Configuração do switch do serviço de nomes

Se o…	Veja o…
A pesquisa de usuário ou grupo falhou ou produziu resultados incorretos	• Configuração do switch do serviço de nomes • Configuração de origem (arquivos locais, domínio NIS, cliente LDAP) • Configuração de rede (por exemplo, LIFs e rotas)
A pesquisa de nomes de host falhou ou expirou, e o servidor DNS não resolve nomes curtos de DNS (por exemplo, host1)	Configuração de DNS para consultas de domínio de topo (TLD). Você pode desabilitar consultas TLD usando a `-is-tld-query-enabled false` opção para o `vserver services name-service dns modify` comando.

Informações relacionadas

"Relatório técnico da NetApp 4668: Guia de práticas recomendadas para serviços de nomes"

Verifique as conexões do serviço de nomes

A partir do ONTAP 9.2, pode verificar os servidores de nomes DNS e LDAP para verificar se estão ligados ao ONTAP. Esses comandos estão disponíveis no nível de privilégios de administrador.

Sobre esta tarefa

Você pode verificar se há uma configuração válida do serviço de nomes DNS ou LDAP conforme necessário usando o verificador de configuração do serviço de nomes. Esta verificação de validação pode ser iniciada na linha de comando ou no System Manager.

Para configurações de DNS, todos os servidores são testados e precisam estar funcionando para que a configuração seja considerada válida. Para configurações LDAP, desde que qualquer servidor esteja ativo, a configuração é válida. Os comandos do serviço de nomes aplicam o verificador de configuração a menos que o `skip-config-validation` campo seja verdadeiro (o padrão é falso).

Passo

1. Use o comando apropriado para verificar uma configuração do serviço de nomes. A IU exibe o status dos servidores configurados.

Para verificar…	Use este comando…
Estado da configuração DNS	`vserver services name-service dns check`
Estado da configuração LDAP	`vserver services name-service ldap check`

```
cluster1::> vserver services name-service dns check -vserver vs0

Vserver         Name Server     Status  Status Details
--------------  --------------- ------- -------------------------
 vs0            10.11.12.13     up      Response time (msec): 55
 vs0            10.11.12.14     up      Response time (msec): 70
 vs0            10.11.12.15     down    Connection refused.
+-------------------------------------------------------------+
```

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                |
| Client Configuration Name: c1                               |
| LDAP Status: up                                             |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                              |
```

A validação da configuração é bem-sucedida se pelo menos um dos servidores configurados (name-serviders/ldap-serviders) estiver acessível e fornecendo o serviço. É apresentado um aviso se alguns dos servidores não estiverem acessíveis.

Comandos para gerenciar entradas do switch do serviço de nomes

Você pode gerenciar entradas de switch de serviço de nomes criando, exibindo, modificando e excluindo-as.

Se você quiser…	Use este comando…
Crie uma entrada de switch de serviço de nomes	`vserver services name-service ns-switch create`
Exibir entradas do switch de serviço de nomes	`vserver services name-service ns-switch show`
Modificar uma entrada de switch de serviço de nomes	`vserver services name-service ns-switch modify`
Excluir uma entrada de switch de serviço de nomes	`vserver services name-service ns-switch delete`

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

Informações relacionadas

"Relatório técnico da NetApp 4668: Guia de práticas recomendadas para serviços de nomes"

Comandos para gerenciar o cache do serviço de nomes

Você pode gerenciar o cache do serviço de nomes modificando o valor time to live (TTL). O valor TTL determina quanto tempo as informações do serviço de nome são persistentes no cache.

Se você quiser modificar o valor TTL para…	Use este comando…
Usuários UNIX	`vserver services name-service cache unix-user settings`
Grupos UNIX	`vserver services name-service cache unix-group settings`
Netgroups UNIX	`vserver services name-service cache netgroups settings`
Hosts	`vserver services name-service cache hosts settings`
Associação ao grupo	`vserver services name-service cache group-membership settings`

Informações relacionadas

"Referência do comando ONTAP"

Comandos para gerenciar mapeamentos de nomes

Existem comandos ONTAP específicos para gerenciar mapeamentos de nomes.

Se você quiser…	Use este comando…
Crie um mapeamento de nomes	`vserver name-mapping create`
Insira um mapeamento de nomes em uma posição específica	`vserver name-mapping insert`
Exibir mapeamentos de nomes	`vserver name-mapping show`

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

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

Comandos para gerenciar usuários UNIX locais

Existem comandos ONTAP específicos para gerenciar usuários UNIX locais.

Se você quiser…	Use este comando…
Crie um usuário local do UNIX	`vserver services name-service unix-user create`
Carregue usuários UNIX locais a partir de um URI	`vserver services name-service unix-user load-from-uri`
Exibir usuários locais do UNIX	`vserver services name-service unix-user show`
Modifique um usuário local UNIX	`vserver services name-service unix-user modify`
Excluir um usuário local UNIX	`vserver services name-service unix-user delete`

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

Comandos para gerenciar grupos UNIX locais

Existem comandos ONTAP específicos para gerenciar grupos UNIX locais.

Se você quiser…	Use este comando…
Crie um grupo UNIX local	`vserver services name-service unix-group create`

Adicione um usuário a um grupo UNIX local	`vserver services name-service unix-group adduser`
Carregue grupos UNIX locais a partir de um URI	`vserver services name-service unix-group load-from-uri`
Exibir grupos UNIX locais	`vserver services name-service unix-group show`
Modifique um grupo UNIX local	`vserver services name-service unix-group modify`
Excluir um usuário de um grupo UNIX local	`vserver services name-service unix-group deluser`
Exclua um grupo UNIX local	`vserver services name-service unix-group delete`

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

Limites para usuários, grupos e membros do grupo UNIX locais

O ONTAP introduziu limites para o número máximo de usuários e grupos UNIX no cluster e comandos para gerenciar esses limites. Esses limites podem ajudar a evitar problemas de desempenho, impedindo que os administradores criem muitos usuários e grupos UNIX locais no cluster.

Há um limite para o número combinado de grupos de usuários UNIX locais e membros de grupo. Há um limite separado para usuários UNIX locais. Os limites são em todo o cluster. Cada um desses novos limites é definido como um valor padrão que você pode modificar até um limite rígido pré-atribuído.

Banco de dados	Limite padrão	Limite rígido
Usuários locais do UNIX	32.768	65.536
Grupos UNIX locais e membros do grupo	32.768	65.536

Gerenciar limites para usuários e grupos UNIX locais

Existem comandos ONTAP específicos para gerenciar limites para usuários e grupos UNIX locais. Os administradores de cluster podem usar esses comandos para solucionar problemas de desempenho no cluster que se acredita estar relacionado a um número excessivo de usuários e grupos UNIX locais.

Sobre esta tarefa

Esses comandos estão disponíveis para o administrador do cluster no nível avançado de privilégio.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Use o comando…
Exibir informações sobre os limites de usuários UNIX locais	`vserver services unix-user max-limit show`
Exibir informações sobre os limites de grupos UNIX locais	`vserver services unix-group max-limit show`
Modifique os limites de usuários UNIX locais	`vserver services unix-user max-limit modify`
Modificar limites de grupo UNIX local	`vserver services unix-group max-limit modify`

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

Comandos para gerenciar netgroups locais

É possível gerenciar grupos de redes locais carregando-os a partir de um URI, verificando seu status entre nós, exibindo-os e excluindo-os.

Se você quiser…	Use o comando…
Carregue netgroups de um URI	`vserver services name-service netgroup load`
Verifique o status dos grupos de redes entre nós	`vserver services name-service netgroup status` Disponível no nível de privilégio avançado e superior.
Exibir grupos de redes locais	`vserver services name-service netgroup file show`
Exclua um netgroup local	`vserver services name-service netgroup file delete`

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

Comandos para gerenciar configurações de domínio NIS

Existem comandos ONTAP específicos para gerenciar configurações de domínio NIS.

Se você quiser…	Use este comando…

Crie uma configuração de domínio NIS	`vserver services name-service nis-domain create`
Exibir configurações de domínio NIS	`vserver services name-service nis-domain show`
Exibir status de vinculação de uma configuração de domínio NIS	`vserver services name-service nis-domain show-bound`
Apresentar estatísticas NIS	`vserver services name-service nis-domain show-statistics` Disponível no nível de privilégio avançado e superior.
Limpar estatísticas NIS	`vserver services name-service nis-domain clear-statistics` Disponível no nível de privilégio avançado e superior.
Modificar uma configuração de domínio NIS	`vserver services name-service nis-domain modify`
Excluir uma configuração de domínio NIS	`vserver services name-service nis-domain delete`
Ative o armazenamento em cache para pesquisas netgroup-by-host	`vserver services name-service nis-domain netgroup-database config modify` Disponível no nível de privilégio avançado e superior.

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

Comandos para gerenciar configurações de cliente LDAP

Existem comandos ONTAP específicos para gerenciar configurações de cliente LDAP.

> Os administradores do SVM não podem modificar ou excluir configurações de cliente LDAP criadas pelos administradores de cluster.

Se você quiser…	Use este comando…
Crie uma configuração de cliente LDAP	`vserver services name-service ldap client create`
Exibir configurações de cliente LDAP	`vserver services name-service ldap client show`
Modificar uma configuração de cliente LDAP	`vserver services name-service ldap client modify`
Altere a senha DE VINCULAÇÃO do cliente LDAP	`vserver services name-service ldap client modify-bind-password`

Eliminar uma configuração de cliente LDAP	`vserver services name-service ldap client delete`

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

Comandos para gerenciar configurações LDAP

Existem comandos ONTAP específicos para gerenciar configurações LDAP.

Se você quiser…	Use este comando…
Crie uma configuração LDAP	`vserver services name-service ldap create`
Exibir configurações LDAP	`vserver services name-service ldap show`
Modificar uma configuração LDAP	`vserver services name-service ldap modify`
Eliminar uma configuração LDAP	`vserver services name-service ldap delete`

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

Comandos para gerenciar modelos de esquema de cliente LDAP

Existem comandos ONTAP específicos para gerenciar modelos de esquema de cliente LDAP.

Os administradores do SVM não podem modificar ou excluir esquemas de cliente LDAP criados por administradores de cluster.

Se você quiser…	Use este comando…
Copie um modelo de esquema LDAP existente	`vserver services name-service ldap client schema copy` Disponível no nível de privilégio avançado e superior.
Exibir modelos de esquema LDAP	`vserver services name-service ldap client schema show`
Modifique um modelo de esquema LDAP	`vserver services name-service ldap client schema modify` Disponível no nível de privilégio avançado e superior.
Excluir um modelo de esquema LDAP	`vserver services name-service ldap client schema delete` Disponível no nível de privilégio avançado e superior.

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

Comandos para gerenciar configurações de interface NFS Kerberos

Existem comandos ONTAP específicos para gerenciar configurações de interface do NFS Kerberos.

Se você quiser…	Use este comando…
Ative o NFS Kerberos em um LIF	`vserver nfs kerberos interface enable`
Exibir configurações de interface NFS Kerberos	`vserver nfs kerberos interface show`
Modificar uma configuração de interface NFS Kerberos	`vserver nfs kerberos interface modify`
Desative o NFS Kerberos em um LIF	`vserver nfs kerberos interface disable`

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

Comandos para gerenciar configurações NFS Kerberos Realm

Existem comandos ONTAP específicos para gerenciar configurações de realm Kerberos NFS.

Se você quiser…	**Use este comando…**
Crie uma configuração NFS Kerberos realm	`vserver nfs kerberos realm create`
Exibir configurações do NFS Kerberos Realm	`vserver nfs kerberos realm show`
Modifique uma configuração de realm do Kerberos NFS	`vserver nfs kerberos realm modify`
Excluir uma configuração NFS Kerberos realm	`vserver nfs kerberos realm delete`

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

Comandos para gerenciar políticas de exportação

Existem comandos ONTAP específicos para gerenciar políticas de exportação.

Se você quiser…	Use este comando…
Exibir informações sobre políticas de exportação	`vserver export-policy show`
Renomeie uma política de exportação	`vserver export-policy rename`
Copiar uma política de exportação	`vserver export-policy copy`
Eliminar uma política de exportação	`vserver export-policy delete`

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

Comandos para gerenciar regras de exportação

Existem comandos ONTAP específicos para gerenciar regras de exportação.

Se você quiser…	Use este comando…
Crie uma regra de exportação	`vserver export-policy rule create`
Exibir informações sobre regras de exportação	`vserver export-policy rule show`
Modificar uma regra de exportação	`vserver export-policy rule modify`
Excluir uma regra de exportação	`vserver export-policy rule delete`

Se você tiver configurado várias regras de exportação idênticas que correspondam a diferentes clientes, certifique-se de mantê-las sincronizadas ao gerenciar regras de exportação.

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

Configurar o cache de credenciais NFS

Motivos para modificar o tempo de funcionamento do cache de credenciais NFS

O ONTAP usa um cache de credenciais para armazenar as informações necessárias para autenticação de usuário para acesso de exportação NFS para fornecer acesso mais rápido e melhorar o desempenho. Você pode configurar por quanto tempo as informações são armazenadas no cache de credenciais para personalizá-las para o seu ambiente.

Há vários cenários ao modificar o cache de credenciais NFS Time-to-live (TTL) pode ajudar a resolver problemas. Você deve entender quais são esses cenários, bem como as consequências de fazer essas

modificações.

Razões

Considere alterar o TTL padrão nas seguintes circunstâncias:

Problema	Medidas corretivas
Os servidores de nomes no seu ambiente estão sofrendo degradação no desempenho devido a uma alta carga de solicitações do ONTAP.	Aumente o TTL para credenciais positivas e negativas armazenadas em cache para reduzir o número de solicitações do ONTAP para servidores de nomes.
O administrador do servidor de nomes fez alterações para permitir o acesso a usuários NFS que foram negados anteriormente.	Diminua o TTL para credenciais negativas armazenadas em cache para reduzir o tempo que os usuários NFS precisam esperar que o ONTAP solicite novas credenciais de servidores de nomes externos para que eles possam obter acesso.
O administrador do servidor de nomes fez alterações para negar acesso a usuários NFS que anteriormente eram permitidos.	Reduza o TTL para credenciais positivas armazenadas em cache para reduzir o tempo antes que o ONTAP solicite novas credenciais de servidores de nomes externos para que os usuários NFS agora tenham acesso negado.

Consequências

Você pode modificar o tempo individualmente para armazenar credenciais positivas e negativas em cache. No entanto, você deve estar ciente das vantagens e desvantagens de fazê-lo.

Se você…	A vantagem é…	A desvantagem é…
Aumente o tempo de cache de credenciais positivas	O ONTAP envia solicitações de credenciais para nomear servidores com menos frequência, reduzindo a carga nos servidores de nomes.	Leva mais tempo para negar acesso a usuários NFS que anteriormente eram permitidos acesso, mas não são mais.
Diminua o tempo de cache positivo de credenciais	Leva menos tempo para negar acesso a usuários NFS que anteriormente eram permitidos acesso, mas não são mais.	O ONTAP envia solicitações de credenciais para nomear servidores com mais frequência, aumentando a carga nos servidores de nomes.
Aumente o tempo de cache de credenciais negativas	O ONTAP envia solicitações de credenciais para nomear servidores com menos frequência, reduzindo a carga nos servidores de nomes.	Leva mais tempo para conceder acesso a usuários NFS que anteriormente não tinham acesso permitido, mas agora.

Se você…	A vantagem é…	A desvantagem é…
Diminua o tempo de cache de credenciais negativas	Leva menos tempo para conceder acesso a usuários NFS que anteriormente não tinham acesso permitido, mas agora.	O ONTAP envia solicitações de credenciais para nomear servidores com mais frequência, aumentando a carga nos servidores de nomes.

Configure o tempo de ativação para credenciais de usuário NFS armazenadas em cache

Você pode configurar o período de tempo que o ONTAP armazena credenciais para usuários NFS em seu cache interno (time-to-live ou TTL) modificando o servidor NFS da máquina virtual de armazenamento (SVM). Isso permite que você solucione certos problemas relacionados à alta carga nos servidores de nomes ou alterações nas credenciais que afetam o acesso do usuário NFS.

Sobre esta tarefa

Estes parâmetros estão disponíveis no nível de privilégio avançado.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute a ação desejada:

Se você quiser modificar o TTL para cache…	Use o comando…
Credenciais positivas	`vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live` O TTL é medido em milissegundos. A partir do ONTAP 9.10,1 e posterior, o padrão é de 1 hora (3.600.000 milissegundos). No ONTAP 9.9,1 e anterior, o padrão é 24 horas (86.400.000 milissegundos). O intervalo permitido para este valor é de 1 minuto (60000 milissegundos) a 7 dias (604.800.000 milissegundos).
Credenciais negativas	`vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live` O TTL é medido em milissegundos. O padrão é 2 horas (7.200.000 milissegundos). O intervalo permitido para este valor é de 1 minuto (60000 milissegundos) a 7 dias (604.800.000 milissegundos).

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Gerenciar caches de política de exportação

Lavar caches de política de exportação

O ONTAP usa vários caches de política de exportação para armazenar informações relacionadas a políticas de exportação para acesso mais rápido. A eliminação de caches de política de exportação manualmente (`vserver export-policy cache flush`) remove informações potencialmente desatualizadas e força o ONTAP a recuperar informações atuais dos recursos externos apropriados. Isso pode ajudar a resolver uma variedade de problemas relacionados ao acesso do cliente às exportações NFS.

Sobre esta tarefa

As informações de cache de política de exportação podem estar desatualizadas devido aos seguintes motivos:

- Uma alteração recente às regras de política de exportação
- Uma alteração recente nos registos de nome de anfitrião nos servidores de nomes
- Uma alteração recente para entradas de netgroup em servidores de nomes
- Recuperando-se de uma interrupção de rede que impedia que os netgroups fossem totalmente carregados

Passos

1. Se você não tiver o cache do serviço de nomes habilitado, execute uma das seguintes ações no modo de privilégio avançado:

Se você quiser flush…	Digite o comando…
Todos os caches de política de exportação (exceto showmount)	`vserver export-policy cache flush -vserver vserver_name`
As regras de política de exportação acedem à cache	`vserver export-policy cache flush -vserver vserver_name -cache access` Você pode incluir o parâmetro opcional `-node` para especificar o nó no qual deseja limpar o cache de acesso.
O cache do nome do host	`vserver export-policy cache flush -vserver vserver_name -cache host`
O cache netgroup	`vserver export-policy cache flush -vserver vserver_name -cache netgroup` O processamento de netgroups é intensivo em recursos. Você só deve limpar o cache do netgroup se estiver tentando resolver um problema de acesso de cliente causado por um netgroup obsoleto.

Se você quiser flush…	Digite o comando…
O cache showmount	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

2. Se o cache do serviço de nomes estiver ativado, execute uma das seguintes ações:

Se você quiser flush…	Digite o comando…
As regras de política de exportação acedem à cache	`vserver export-policy cache flush -vserver vserver_name -cache access` Você pode incluir o parâmetro opcional `-node` para especificar o nó no qual deseja limpar o cache de acesso.
O cache do nome do host	`vserver services name-service cache hosts forward-lookup delete-all`
O cache netgroup	`vserver services name-service cache netgroups ip-to-netgroup delete-all` `vserver services name-service cache netgroups members delete-all` O processamento de netgroups é intensivo em recursos. Você só deve limpar o cache do netgroup se estiver tentando resolver um problema de acesso de cliente causado por um netgroup obsoleto.
O cache showmount	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

Exiba a fila e o cache do netgroup da política de exportação

O ONTAP usa a fila netgroup ao importar e resolver netgroups e usa o cache netgroup para armazenar as informações resultantes. Ao solucionar problemas relacionados ao netgroup da política de exportação, você pode usar os `vserver export-policy netgroup queue show` comandos e `vserver export-policy netgroup cache show` para exibir o status da fila do netgroup e o conteúdo do cache do netgroup.

Passo

1. Execute uma das seguintes ações:

Para exibir o netgroup da política de exportação…	Digite o comando…
Fila de espera	`vserver export-policy netgroup queue show`

Cache	`vserver export-policy netgroup cache show -vserver vserver_name`

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

Verifique se um endereço IP de cliente é membro de um netgroup

Ao solucionar problemas de acesso de cliente NFS relacionados a netgroups, 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.

Sobre esta tarefa

Verificar a associação ao netgroup permite determinar se o ONTAP está ciente de que um cliente é ou não membro de um netgroup. Ele também permite que você saiba se o cache do ONTAP netgroup está em um estado transitório enquanto atualiza informações do netgroup. Essas informações podem ajudá-lo a entender por que um cliente pode ter acesso inesperadamente concedido ou negado.

Passo

1. Verifique a associação do netgroup de um endereço IP de cliente: `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

   O comando pode retornar os seguintes resultados:

   - O cliente é um membro do netgroup.

     Isso foi confirmado por meio de uma pesquisa de pesquisa reversa ou de uma pesquisa netgroup-by-host.

   - O cliente é um membro do netgroup.

     Ele foi encontrado no cache do ONTAP netgroup.

   - O cliente não é membro do netgroup.
   - A associação ao cliente ainda não pode ser determinada porque o ONTAP está atualizando o cache do netgroup.

     Até que isso seja feito, a associação não pode ser explicitamente descartada dentro ou fora. Use o `vserver export-policy netgroup queue show` comando para monitorar o carregamento do netgroup e tentar novamente a verificação depois que ela estiver concluída.

Exemplo

O exemplo a seguir verifica se um cliente com o endereço IP 172.17.16.72 é membro do netgroup Mercury no SVM VS1:

```
 cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.72
```

Otimizar o desempenho do cache de acesso

Você pode configurar vários parâmetros para otimizar o cache de acesso e encontrar o equilíbrio certo entre o desempenho e a corrente das informações armazenadas no cache de acesso.

Sobre esta tarefa

Quando configurar os períodos de atualização do cache de acesso, tenha em mente o seguinte:

- Valores mais altos significam que as entradas permanecem mais longas no cache de acesso.

  A vantagem é o melhor desempenho porque o ONTAP gasta menos recursos na atualização de entradas de cache de acesso. A desvantagem é que se as regras de política de exportação mudarem e as entradas de cache de acesso ficarem obsoletas como resultado, leva mais tempo para atualizá-las. Como resultado, os clientes que devem obter acesso podem ser negados e os clientes que devem ser negados podem obter acesso.

- Valores mais baixos significam que o ONTAP atualiza as entradas do cache de acesso com mais frequência.

  A vantagem é que as entradas são mais atuais e os clientes são mais propensos a ter acesso correto ou negado. A desvantagem é uma diminuição no desempenho porque o ONTAP gasta mais recursos atualizando entradas de cache de acesso.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute a ação desejada:

Para modificar o…	Digite…
Período de atualização para entradas positivas	`vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value`
Período de atualização para entradas negativas	`vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value`
Período de tempo limite para entradas antigas	`vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value`

3. Verifique as novas configurações de parâmetros:

   ```
   vserver export-policy access-cache config show-all-vservers
   ```

4. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Gerenciar bloqueios de arquivos

Acerca do bloqueio de ficheiros entre protocolos

Bloqueio de arquivos é um método usado por aplicativos cliente para impedir que um usuário acesse um arquivo aberto anteriormente por outro usuário. A forma como o ONTAP bloqueia ficheiros depende do protocolo do cliente.

Se o cliente for um cliente NFS, os bloqueios são consultivos; se o cliente for um cliente SMB, os bloqueios são obrigatórios.

Devido às diferenças entre os bloqueios de arquivos NFS e SMB, um cliente NFS pode não conseguir acessar um arquivo aberto anteriormente por um aplicativo SMB.

O seguinte ocorre quando um cliente NFS tenta aceder a um ficheiro bloqueado por uma aplicação SMB:

- Em volumes mistos ou NTFS, operações de manipulação de arquivos como `rm` , `rmdir` e `mv` podem causar falha no aplicativo NFS.
- As operações de leitura e gravação NFS são negadas pelos modos abertos SMB deny-read e deny-write, respetivamente.
- As operações de gravação NFS falham quando o intervalo escrito do arquivo é bloqueado com um bytelock SMB exclusivo.

Em volumes de estilo de segurança UNIX, as operações NFS desvincular e renomear ignoram o estado de bloqueio SMB e permitem o acesso ao arquivo. Todas as outras operações NFS em volumes estilo segurança UNIX honram o estado de bloqueio SMB.

Como o ONTAP trata bits somente de leitura

O bit somente leitura é definido em uma base arquivo por arquivo para refletir se um arquivo é gravável (desativado) ou somente leitura (habilitado).

Os clientes SMB que usam o Windows podem definir um bit somente leitura por arquivo. Os clientes NFS não definem um bit somente leitura por arquivo porque os clientes NFS não têm operações de protocolo que usam um bit somente leitura por arquivo.

O ONTAP pode definir um bit somente leitura em um arquivo quando um cliente SMB que usa o Windows cria esse arquivo. O ONTAP também pode definir um bit somente leitura quando um arquivo é compartilhado entre clientes NFS e clientes SMB. Alguns softwares, quando usados por clientes NFS e clientes SMB, exigem que o bit somente leitura seja ativado.

Para que o ONTAP mantenha as permissões de leitura e gravação apropriadas em um arquivo compartilhado entre clientes NFS e clientes SMB, ele trata o bit somente leitura de acordo com as seguintes regras:

- O NFS trata qualquer arquivo com o bit somente leitura ativado como se ele não tivesse bits de permissão de gravação ativados.
- Se um cliente NFS desativar todos os bits de permissão de gravação e pelo menos um desses bits tiver sido ativado anteriormente, o ONTAP ativa o bit somente leitura para esse arquivo.

- Se um cliente NFS ativar qualquer bit de permissão de gravação, o ONTAP desativa o bit somente leitura para esse arquivo.
- Se o bit somente leitura de um arquivo estiver ativado e um cliente NFS tentar descobrir permissões para o arquivo, os bits de permissão para o arquivo não serão enviados para o cliente NFS; em vez disso, o ONTAP enviará os bits de permissão para o cliente NFS com os bits de permissão de gravação mascarados.
- Se o bit somente leitura de um arquivo estiver ativado e um cliente SMB desabilitar o bit somente leitura, o ONTAP ativa o bit de permissão de gravação do proprietário para o arquivo.
- Os arquivos com o bit somente leitura habilitado são graváveis somente pelo root.

> As alterações às permissões de arquivo entram em vigor imediatamente em clientes SMB, mas podem não ter efeito imediatamente em clientes NFS se o cliente NFS ativar o armazenamento em cache de atributos.

Como o ONTAP difere do Windows ao lidar com bloqueios em componentes de caminho de compartilhamento

Ao contrário do Windows, o ONTAP não bloqueia cada componente do caminho para um arquivo aberto enquanto o arquivo está aberto. Esse comportamento também afeta os caminhos de compartilhamento SMB.

Como o ONTAP não bloqueia cada componente do caminho, é possível renomear um componente do caminho acima do arquivo aberto ou do compartilhamento, o que pode causar problemas para determinados aplicativos ou fazer com que o caminho de compartilhamento na configuração do SMB seja inválido. Isso pode fazer com que o compartilhamento seja inacessível.

Para evitar problemas causados pela renomeação de componentes de caminho, você pode aplicar configurações de segurança da Lista de Controle de Acesso (ACL) do Windows que impedem que usuários ou aplicativos renomeem diretórios críticos.

Saiba mais "Como impedir que diretórios sejam renomeados enquanto os clientes os acessam"sobre o .

Apresentar informações sobre bloqueios

Você pode exibir informações sobre os bloqueios de arquivo atuais, incluindo quais tipos de bloqueios são mantidos e qual é o estado de bloqueio, detalhes sobre bloqueios de intervalo de bytes, modos de sharelock, bloqueios de delegação e bloqueios oportunistas, e se os bloqueios são abertos com alças duráveis ou persistentes.

Sobre esta tarefa

O endereço IP do cliente não pode ser exibido para bloqueios estabelecidos através de NFSv4 ou NFSv4,1.

Por padrão, o comando exibe informações sobre todos os bloqueios. Você pode usar parâmetros de comando para exibir informações sobre bloqueios de uma máquina virtual de armazenamento específica (SVM) ou para filtrar a saída do comando por outros critérios.

O `vserver locks show` comando exibe informações sobre quatro tipos de bloqueios:

- Bloqueios de intervalo de bytes, que bloqueiam apenas uma parte de um arquivo.
- Bloqueios de compartilhamento, que bloqueiam arquivos abertos.

- Bloqueios oportunistas, que controlam o cache do lado do cliente sobre SMB.
- Delegações, que controlam o cache do lado do cliente sobre NFSv4.x.

Ao especificar parâmetros opcionais, você pode determinar informações importantes sobre cada tipo de bloqueio. Consulte a página de manual para obter mais informações.

Passo

1. Exiba informações sobre bloqueios usando o `vserver locks show` comando.

Exemplos

O exemplo a seguir exibe informações de resumo de um bloqueio NFSv4 em um arquivo com o `/vol1/file1` caminho . O modo de acesso sharelock é write-deny_none, e o bloqueio foi concedido com delegação de gravação:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                         delegation  -
               Delegation Type: write
```

O exemplo a seguir exibe informações detalhadas de oplock e sharelock sobre o bloqueio SMB em um arquivo com o `/data2/data2_2/intro.pptx` caminho . Um manipulador durável é concedido no arquivo com um modo de acesso de bloqueio de compartilhamento de write-deny_none para um cliente com um endereço IP de 10,3.1,3. Uma locação de oplock é concedida com um nível de lote de oplock:

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

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
              Lock Protocol: cifs
                  Lock Type: share-level
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
```

```
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                   Vserver: vs1
                    Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/test.pptx
                  Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Travas de quebra

Quando os bloqueios de arquivos estão impedindo o acesso do cliente aos arquivos, você pode exibir informações sobre os bloqueios atualmente mantidos e, em seguida, quebrar bloqueios específicos. Exemplos de cenários em que você pode precisar quebrar bloqueios incluem depuração de aplicativos.

Sobre esta tarefa

O `vserver locks break` comando está disponível apenas no nível de privilégio avançado e superior. A página de manual do comando contém informações detalhadas.

Passos

1. Para encontrar as informações que você precisa para quebrar um bloqueio, use o `vserver locks show` comando.

   A página de manual do comando contém informações detalhadas.

2. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

3. Execute uma das seguintes ações:

Se você quiser quebrar um bloqueio especificando…	Digite o comando…
O nome do SVM, o nome do volume, o nome LIF e o caminho do arquivo	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
A ID de bloqueio	`vserver locks break -lockid UUID`

4. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Como os filtros de primeira leitura e primeira gravação do FPolicy funcionam com o NFS

Os clientes NFS experimentam um alto tempo de resposta durante o alto tráfego de solicitações de leitura/gravação quando o FPolicy é habilitado usando um servidor FPolicy externo com operações de leitura/gravação como eventos monitorados. Para clientes NFS, o uso de filtros de primeira leitura e primeira gravação no FPolicy reduz o número de notificações do FPolicy e melhora o desempenho.

No NFS, o cliente faz a e/S em um arquivo, buscando sua alça. Esse identificador pode permanecer válido nas reinicializações do servidor e do cliente. Portanto, o cliente está livre para armazenar em cache o identificador e enviar solicitações nele sem recuperar alças novamente. Em uma sessão regular, muitas solicitações de leitura/gravação são enviadas para o servidor de arquivos. Se as notificações forem geradas para todas essas solicitações, isso pode resultar nos seguintes problemas:

- Uma carga maior devido ao processamento de notificação adicional e maior tempo de resposta.
- Um grande número de notificações sendo enviadas para o servidor FPolicy, mesmo que o servidor não seja afetado por todas as notificações.

Depois de receber a primeira solicitação de leitura/gravação de um cliente para um arquivo específico, uma entrada de cache é criada e a contagem de leitura/gravação é incrementada. Essa solicitação é marcada como a operação de primeira leitura/gravação e um evento FPolicy é gerado. Antes de Planejar e criar seus

filtros FPolicy para um cliente NFS, você deve entender os conceitos básicos de como os filtros FPolicy funcionam.

- Primeira leitura: Filtra as solicitações de leitura do cliente para primeira leitura.

  Quando esse filtro é usado para eventos NFS, as `-file-session-io-grouping-count` configurações e `-file-session-io-grouping-duration` determinam a solicitação de primeira leitura para a qual o FPolicy é processado.

- Primeira gravação: Filtra as solicitações de gravação do cliente para a primeira gravação.

  Quando esse filtro é usado para eventos NFS, as `-file-session-io-grouping-count` configurações e `-file-session-io-grouping-duration` determinam a solicitação de primeira gravação para a qual o FPolicy foi processado.

As seguintes opções são adicionadas no banco de dados de servidores NFS.

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

Modifique a ID de implementação do servidor NFSv4,1

O protocolo NFSv4,1 inclui uma ID de implementação de servidor que documenta o domínio, o nome e a data do servidor. Você pode modificar os valores padrão da ID de implementação do servidor. Alterar os valores padrão pode ser útil, por exemplo, ao coletar estatísticas de uso ou solucionar problemas de interoperabilidade. Para obter mais informações, consulte RFC 5661.

Sobre esta tarefa

Os valores padrão para as três opções são os seguintes:

Opção	Nome da opção	Valor padrão
Domínio ID de implementação NFSv4,1	`-v4.1-implementation -domain`	NetApp.com
NFSv4,1 Nome ID implementação	`-v4.1-implementation-name`	Nome da versão do cluster
NFSv4,1 Data ID implementação	`-v4.1-implementation-date`	Data da versão do cluster

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Execute uma das seguintes ações:

Se você quiser modificar o ID de implementação do NFSv4,1…	Digite o comando…
Domínio	`vserver nfs modify -v4.1 -implementation-domain domain`
Nome	`vserver nfs modify -v4.1 -implementation-name name`
Data	`vserver nfs modify -v4.1 -implementation-date date`

3. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Gerenciar ACLs NFSv4

Benefícios de habilitar ACLs NFSv4

Há muitos benefícios em habilitar ACLs NFSv4.

Os benefícios de habilitar ACLs NFSv4 incluem o seguinte:

- Controle mais refinado do acesso do usuário para arquivos e diretórios
- Melhor segurança NFS
- Interoperabilidade aprimorada com CIFS
- Remoção da limitação NFS de 16 grupos por usuário

Como as ACLs NFSv4 funcionam

Um cliente que usa ACLs NFSv4 pode definir e exibir ACLs em arquivos e diretórios no sistema. Quando um novo arquivo ou subdiretório é criado em um diretório que tem uma ACL, o novo arquivo ou subdiretório herda todas as entradas de controle de acesso (ACEs) na ACL que foram marcadas com os sinalizadores de herança apropriados.

Quando um arquivo ou diretório é criado como resultado de uma solicitação NFSv4, a ACL no arquivo ou diretório resultante depende se a solicitação de criação de arquivo inclui uma ACL ou apenas permissões de acesso de arquivo UNIX padrão e se o diretório pai tem uma ACL:

- Se a solicitação incluir uma ACL, essa ACL é usada.
- Se a solicitação incluir apenas permissões de acesso a arquivos UNIX padrão, mas o diretório pai tiver uma ACL, os ACEs na ACL do diretório pai serão herdados pelo novo arquivo ou diretório, desde que os ACEs tenham sido marcados com os sinalizadores de herança apropriados.

Uma ACL pai é herdada mesmo se `-v4.0-acl` estiver definida como `off`.

- Se a solicitação incluir apenas permissões de acesso a arquivos UNIX padrão e o diretório pai não tiver uma ACL, o modo de arquivo cliente será usado para definir permissões de acesso a arquivos UNIX padrão.
- Se a solicitação incluir apenas permissões de acesso de arquivo UNIX padrão e o diretório pai tiver uma ACL não herdável, o novo objeto será criado apenas com bits de modo.

Se o `-chown-mode` parâmetro tiver sido definido como `restricted` com comandos nas `vserver nfs` famílias ou `vserver export-policy rule`, a propriedade do arquivo só pode ser alterada pelo superusuário, mesmo que as permissões no disco definidas com ACLs NFSv4 permitam que um usuário não-root altere a propriedade do arquivo. Para obter mais informações, consulte as páginas de manual relevantes.

Ativar ou desativar a modificação das ACLs NFSv4

Quando o ONTAP recebe um `chmod` comando para um arquivo ou diretório com uma ACL, por padrão a ACL é mantida e modificada para refletir a alteração de bit de modo. Você pode desativar o `-v4-acl-preserve` parâmetro para alterar o comportamento se quiser que a ACL seja descartada.

Sobre esta tarefa

Ao usar estilo de segurança unificado, esse parâmetro também especifica se as permissões de arquivo NTFS são preservadas ou descartadas quando um cliente envia um comando chmod, chgroup ou chown para um arquivo ou diretório.

A predefinição para este parâmetro está ativada.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute uma das seguintes ações:

Se você quiser…	Digite o seguinte comando…
Ativar retenção e modificação de ACLs NFSv4 existentes (padrão)	`vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled`
Desative a retenção e solte as ACLs NFSv4 ao alterar os bits de modo	`vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled`

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Como o ONTAP usa ACLs NFSv4 para determinar se ele pode excluir um arquivo

Para determinar se ele pode excluir um arquivo, o ONTAP usa uma combinação do bit DE EXCLUSÃO do arquivo e o bit DELETE_CHILD do diretório que contém. Para obter mais informações, consulte o NFS 4,1 RFC 5661.

Ativar ou desativar ACLs NFSv4

Para ativar ou desativar as ACLs NFSv4, pode modificar as `-v4.0-acl` opções e. `-v4.1-acl` Estas opções estão desativadas por predefinição.

Sobre esta tarefa

A `-v4.0-acl` opção ou `-v4.1-acl` controla a configuração e visualização de ACLs NFSv4; ela não controla a aplicação dessas ACLs para verificação de acesso.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Então…
Ativar ACLs NFSv4,0	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`
Desativar ACLs NFSv4,0	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`
Ativar ACLs NFSv4,1	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`
Desativar ACLs NFSv4,1	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

Modifique o limite máximo de ACE para ACLs NFSv4

É possível modificar o número máximo de ACEs permitidos para cada ACL NFSv4 modificando o parâmetro `-v4-acl-max-aces`. Por padrão, o limite é definido como 400 ACEs para cada ACL. Aumentar esse limite pode ajudar a garantir a migração bem-sucedida de dados com ACLs que contêm mais de 400 ACEs para sistemas de storage que executam ONTAP.

Sobre esta tarefa

Aumentar esse limite pode afetar o desempenho dos clientes que acessam arquivos com ACLs NFSv4.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Modifique o limite máximo de ACE para ACLs NFSv4:

   ```
   vserver nfs modify -v4-acl-max-aces max_ace_limit
   ```

   O intervalo válido de

   `max_ace_limit` é a. `192` `1024.`

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Gerenciar delegações de arquivos do NFSv4

Ativar ou desativar as delegações de ficheiros de leitura do NFSv4

Para ativar ou desativar as delegações de ficheiros de leitura do NFSv4, pode modificar a `-v4.0-read-delegation`opção ou . Ao ativar as delegações de arquivos de leitura, você pode eliminar grande parte da sobrecarga de mensagens associada à abertura e fechamento de arquivos.

Sobre esta tarefa

Por padrão, as delegações de arquivos de leitura são desativadas.

A desvantagem de habilitar delegações de arquivos de leitura é que o servidor e seus clientes devem recuperar delegações após o servidor reiniciar ou reiniciar, um cliente reiniciar ou reiniciar, ou uma partição de rede ocorrer.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Então…
Ativar as delegações de ficheiros de leitura NFSv4	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled`

Ativar as delegações de ficheiros de leitura NFSv4,1	Introduza o seguinte comando: E `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled`
Desativar as delegações de ficheiros de leitura NFSv4	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled`
Desativar as delegações de ficheiros de leitura NFSv4,1	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled`

Resultado

As opções de delegação de arquivos entram em vigor assim que são alteradas. Não há necessidade de reinicializar ou reiniciar o NFS.

Ativar ou desativar as delegações de ficheiros de gravação NFSv4

Para ativar ou desativar as delegações de ficheiros de gravação, pode modificar a `-v4.0-write-delegation`opção ou . Ao ativar as delegações de arquivos de gravação, você pode eliminar grande parte da sobrecarga de mensagens associada ao bloqueio de arquivos e Registros, além de abrir e fechar arquivos.

Sobre esta tarefa

Por padrão, as delegações de arquivos de gravação são desativadas.

A desvantagem de habilitar delegações de arquivos de gravação é que o servidor e seus clientes devem executar tarefas adicionais para recuperar delegações após o servidor reiniciar ou reiniciar, um cliente reiniciar ou reiniciar ou uma partição de rede ocorrer.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Então…
Ativar as delegações de ficheiros de gravação NFSv4	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled`
Ativar as delegações de ficheiros de gravação NFSv4,1	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled`

Se você quiser…	Então…
Desativar as delegações de ficheiros de gravação NFSv4	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled`
Desativar as delegações de ficheiros de gravação NFSv4,1	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled`

Resultado

As opções de delegação de arquivos entram em vigor assim que são alteradas. Não há necessidade de reinicializar ou reiniciar o NFS.

Configure o bloqueio de arquivos NFSv4 e Registro

Cerca de NFSv4 arquivo e Registro de bloqueio

Para clientes NFSv4, o ONTAP suporta o mecanismo de bloqueio de arquivos NFSv4, mantendo o estado de todos os bloqueios de arquivos em um modelo baseado em leasing.

"Relatório técnico da NetApp 3580: NFSv4 melhorias e melhores práticas Guia de implementação do Data ONTAP"

Especifique o período de locação de bloqueio NFSv4

Para especificar o período de locação de bloqueio NFSv4 (ou seja, o período de tempo em que o ONTAP concede irrevogavelmente um bloqueio a um cliente), você pode modificar a `-v4-lease-seconds` opção. Períodos de leasing mais curtos aceleram a recuperação do servidor, enquanto períodos de leasing mais longos são benéficos para servidores que lidam com uma grande quantidade de clientes.

Sobre esta tarefa

Por padrão, essa opção está definida como `30`. O valor mínimo para esta opção é `10`. O valor máximo para esta opção é o período de tolerância de bloqueio, que pode ser definido com a `locking.lease_seconds` opção.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Introduza o seguinte comando:

   ```
   vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
   ```

3. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Especifique o período de tolerância de bloqueio NFSv4

Para especificar o período de carência de bloqueio NFSv4 (ou seja, o período de tempo em que os clientes tentam recuperar seu estado de bloqueio do ONTAP durante a recuperação do servidor), você pode modificar a `-v4-grace-seconds` opção.

Sobre esta tarefa

Por padrão, essa opção está definida como `45`.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Introduza o seguinte comando:

   ```
   vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
   ```

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Como NFSv4 referências funcionam

Quando você ativa referências NFSv4, o ONTAP fornece referências "intra-SVM" para clientes NFSv4. A referência intra-SVM ocorre quando um nó de cluster que recebe a solicitação NFSv4 refere o cliente NFSv4 a outra interface lógica (LIF) na máquina virtual de storage (SVM).

O cliente NFSv4 deve acessar o caminho que recebeu a referência no LIF de destino a partir desse ponto. O nó do cluster original fornece tal referência quando determina que existe um LIF no SVM que reside no nó do cluster no qual o volume de dados reside, permitindo assim aos clientes acesso mais rápido aos dados e evitando comunicação extra do cluster.

Ativar ou desativar referências NFSv4

Você pode habilitar referências NFSv4D em máquinas virtuais de armazenamento (SVMs) habilitando as opções `-v4-fsid-change` e `-v4.0-referrals`ou. Habilitar referências NFSv4 pode resultar em acesso mais rápido aos dados para clientes NFSv4 que suportam esse recurso.

O que você vai precisar

Se você quiser ativar as referências NFS, primeiro desative o NFS paralelo. Não é possível ativar ambos ao mesmo tempo.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Ativar NFSv4 referências	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled`
Desative as referências NFSv4	`vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled`
Ativar NFSv4,1 referências	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled`
Desative as referências NFSv4,1	`vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled`

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Exibir estatísticas NFS

É possível exibir estatísticas NFS para máquinas virtuais de storage (SVMs) no sistema de storage para monitorar a performance e diagnosticar problemas.

Passos

1. Use o `statistics catalog object show` comando para identificar os objetos NFS a partir dos quais você pode exibir dados.

   ```
   statistics catalog object show -object nfs*
   ```

2. Use os `statistics start` comandos e opcionais `statistics stop` para coletar uma amostra de dados de um ou mais objetos.
3. Use o `statistics show` comando para exibir os dados de amostra.

Exemplo: Monitorando o desempenho do NFSv3

O exemplo a seguir mostra os dados de desempenho do protocolo NFSv3.

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

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

O comando a seguir mostra os dados da amostra especificando contadores que mostram o número de solicitações de leitura e gravação bem-sucedidas versus o número total de solicitações de leitura e gravação:

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                     Value
    --------------------------- ----------------------------
    read_success                                  40042
    read_total                                    40042
    write_success                               1492052
    write_total                                 1492052
```

Informações relacionadas

"Configuração do monitoramento de desempenho"

Exibir estatísticas de DNS

Você pode exibir estatísticas de DNS para máquinas virtuais de armazenamento (SVMs) no sistema de armazenamento para monitorar o desempenho e diagnosticar problemas.

Passos

1. Use o `statistics catalog object show` comando para identificar os objetos DNS a partir dos quais você pode exibir dados.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Use os `statistics start` comandos e `statistics stop` para coletar uma amostra de dados de um ou mais objetos.
3. Use o `statistics show` comando para exibir os dados de amostra.

Monitoramento de estatísticas de DNS

Os exemplos a seguir mostram dados de desempenho para consultas DNS. Os seguintes comandos iniciam a coleta de dados para uma nova amostra:

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

O comando a seguir exibe dados da amostra especificando contadores que exibem o número de consultas DNS enviadas versus o número de consultas DNS recebidas, com falha ou com tempo limite:

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            0
    num_requests_sent                                               1
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

O comando a seguir exibe dados da amostra especificando contadores que exibem o número de vezes que um erro específico foi recebido para uma consulta DNS no servidor específico:

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                             NXDOMAIN
    server_ip_address                                   10.72.219.109
3 entries were displayed.
```

Informações relacionadas

"Configuração do monitoramento de desempenho"

Apresentar estatísticas NIS

Você pode exibir estatísticas NIS para máquinas virtuais de armazenamento (SVMs) no sistema de armazenamento para monitorar o desempenho e diagnosticar problemas.

Passos

1. Use o `statistics catalog object show` comando para identificar os objetos NIS a partir dos quais você pode exibir dados.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Use os `statistics start` comandos e `statistics stop` para coletar uma amostra de dados de um ou mais objetos.
3. Use o `statistics show` comando para exibir os dados de amostra.

Monitoramento de estatísticas NIS

Os exemplos a seguir exibem dados de desempenho para consultas NIS. Os seguintes comandos iniciam a coleta de dados para uma nova amostra:

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

O comando a seguir exibe dados da amostra especificando contadores que mostram o número de consultas NIS enviadas versus o número de consultas NIS recebidas, com falha ou com tempo limite:

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            1
    num_requests_sent                                               2
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

O comando a seguir exibe dados da amostra especificando contadores que mostram o número de vezes que um erro específico foi recebido para uma consulta NIS no servidor específico:

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                            YP_NOTFOUND
    server_ip_address                                     10.227.13.221
3 entries were displayed.
```

Informações relacionadas

"Configuração do monitoramento de desempenho"

Suporte para VMware vStorage sobre NFS

O ONTAP dá suporte a determinados recursos de APIs de storage do VMware vStorage para integração de array (VAAI) em um ambiente NFS.

Recursos suportados

Os seguintes recursos são suportados:

- Descarga de cópia

  Permite que um host ESXi copie máquinas virtuais ou discos de máquinas virtuais (VMDKs) diretamente entre o local de armazenamento de dados de origem e destino sem envolver o host. Isso conserva os ciclos de CPU do host ESXi e a largura de banda da rede. A descarga de cópia preserva a eficiência de espaço se o volume de origem for esparso.

- Reserva de espaço

  Garante espaço de armazenamento para um arquivo VMDK reservando espaço para ele.

Limitações

O VMware vStorage sobre NFS tem as seguintes limitações:

- As operações de descarga de cópia podem falhar nos seguintes cenários:
  - Ao executar o wafliron no volume de origem ou destino, porque ele temporariamente coloca o volume off-line
  - Ao mover o volume de origem ou destino
  - Ao mover o LIF de origem ou destino
  - Durante a realização de operações de takeover ou giveback
  - Durante a execução de operações de comutação ou switchback
- A cópia do lado do servidor pode falhar devido a diferenças de formato de identificador de arquivo no seguinte cenário:

  Você tenta copiar dados de SVMs que exportaram qtrees atualmente ou anteriormente para SVMs que nunca exportaram qtrees. Para contornar essa limitação, você pode exportar pelo menos uma qtree no SVM de destino.

Informações relacionadas

"Quais operações descarregadas da VAAI são suportadas pelo Data ONTAP?"

Ative ou desative o VMware vStorage em NFS

Você pode ativar ou desativar o suporte para VMware vStorage sobre NFS em máquinas virtuais de armazenamento (SVMs) usando o `vserver nfs modify` comando.

Sobre esta tarefa

Por padrão, o suporte ao VMware vStorage sobre NFS está desativado.

Passos

1. Exibir o status atual de suporte do vStorage para SVMs:

   ```
   vserver nfs show -vserver vserver_name -instance
   ```

2. Execute uma das seguintes ações:

Se você quiser…	Digite o seguinte comando…
Habilite o suporte ao VMware vStorage	`vserver nfs modify -vserver vserver_name -vstorage enabled`
Desative o suporte ao VMware vStorage	`vserver nfs modify -vserver vserver_name -vstorage disabled`

Depois de terminar

Você deve instalar o plug-in NFS para VMware VAAI antes de usar essa funcionalidade. Para obter mais informações, consulte *Instalando o plug-in NFS do NetApp para VMware VAAI*.

Informações relacionadas

"Documentação do NetApp: Plug-in NFS do NetApp para VMware VAAI"

Ativar ou desativar o suporte rquota

O ONTAP suporta o protocolo de cota remota versão 1 (rquota v1). O protocolo rquota permite que os clientes NFS obtenham informações de quota para os utilizadores a partir de uma máquina remota. Você pode ativar o rquota em máquinas virtuais de armazenamento (SVMs) usando o `vserver nfs modify` comando.

Sobre esta tarefa

Por padrão, rquota está desativada.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Digite o seguinte comando…
Habilite o suporte a rquota para SVMs	`vserver nfs modify -vserver vserver_name -rquota enable`
Desative o suporte rquota para SVMs	`vserver nfs modify -vserver vserver_name -rquota disable`

Para obter mais informações sobre cotas, "Gerenciamento de storage lógico"consulte .

Melhoria do desempenho NFSv3 e NFSv4 modificando o tamanho da transferência TCP

Você pode melhorar o desempenho de clientes NFSv3 e NFSv4 conetados a sistemas de armazenamento em uma rede de alta latência, modificando o tamanho máximo de transferência TCP.

Quando os clientes acessam sistemas de armazenamento em uma rede de alta latência, como uma rede de área ampla (WAN) ou uma rede de área metropolitana (MAN) com latência superior a 10 milissegundos, talvez você consiga melhorar o desempenho da conexão modificando o tamanho máximo da transferência TCP. Os clientes que acessam sistemas de storage em uma rede de baixa latência, como uma rede de área local (LAN), podem esperar pouco ou nenhum benefício ao modificar esses parâmetros. Se a melhoria da taxa de transferência não exceder o impactos da latência, você não deve usar esses parâmetros.

Para determinar se o ambiente de storage se beneficiaria da modificação desses parâmetros, primeiro você deve realizar uma avaliação abrangente de desempenho de um cliente NFS com baixa performance. Analise se o baixo desempenho é devido à latência excessiva da viagem de ida e volta e à pequena solicitação no cliente. Nestas condições, o cliente e o servidor não podem utilizar totalmente a largura de banda disponível porque gastam a maioria dos seus ciclos de serviço esperando que pequenas solicitações e respostas sejam transmitidas através da conexão.

Ao aumentar o tamanho da solicitação NFSv3 e NFSv4, o cliente e o servidor podem usar a largura de banda disponível de forma mais eficaz para mover mais dados por unidade de tempo; portanto, aumentando a eficiência geral da conexão.

Tenha em mente que a configuração entre o sistema de armazenamento e o cliente pode variar. O sistema de armazenamento e o cliente suportam o tamanho máximo de 1 MB para operações de transferência. No entanto, se você configurar o sistema de armazenamento para suportar o tamanho máximo de transferência de 1 MB, mas o cliente só suporta 64 KB, então o tamanho de transferência de montagem é limitado a 64 KB ou menos.

Antes de modificar esses parâmetros, você deve estar ciente de que isso resulta em consumo de memória adicional no sistema de armazenamento pelo período de tempo necessário para montar e transmitir uma grande resposta. Quanto mais conexões de alta latência para o sistema de armazenamento, maior o consumo de memória adicional. Sistemas de armazenamento com alta capacidade de memória podem ter muito pouco efeito com essa mudança. Os sistemas de armazenamento com baixa capacidade de memória podem sofrer uma degradação notável do desempenho.

O uso bem-sucedido desses parâmetros depende da capacidade de recuperar dados de vários nós de um cluster. A latência inerente da rede do cluster pode aumentar a latência geral da resposta. A latência geral tende a aumentar ao usar esses parâmetros. Como resultado, workloads sensíveis à latência podem mostrar impacto negativo.

Modifique o tamanho máximo de transferência do TCP NFSv3 e NFSv4

Você pode modificar a `-tcp-max-xfer-size` opção para configurar tamanhos máximos de transferência para todas as conexões TCP usando os protocolos NFSv3 e NFSv4.x.

Sobre esta tarefa

Você pode modificar essas opções individualmente para cada máquina virtual de storage (SVM).

A partir do ONTAP 9, as `v3-tcp-max-read-size` opções e `v3-tcp-max-write-size` são obsoletas. Você deve usar a `-tcp-max-xfer-size` opção em vez disso.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Modifique o tamanho máximo de transferência do TCP NFSv3 ou NFSv4	`vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size`

Opção	Alcance	Padrão
`-tcp-max-xfer-size`	8192 a 1048576 bytes	65536 bytes

> O tamanho máximo de transferência que você inserir deve ser um múltiplo de 4 KB (4096 bytes). As solicitações que não estão alinhadas corretamente afetam negativamente o desempenho.

3. Use o `vserver nfs show -fields tcp-max-xfer-size` comando para verificar as alterações.
4. Se algum cliente usar montagens estáticas, desmonte e remonte para que o novo tamanho de parâmetro entre em vigor.

Exemplo

O comando a seguir define o tamanho máximo de transferência TCP NFSv3 e NFSv4.x para 1048576 bytes no SVM chamado VS1:

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

Configure o número de IDs de grupo permitidas para usuários NFS

Por padrão, o ONTAP suporta até 32 IDs de grupo ao lidar com credenciais de usuário NFS usando autenticação Kerberos (RPCSEC_GSS). Ao usar a autenticação AUTH_SYS, o número máximo padrão de IDs de grupo é 16, conforme definido na RFC 5531. Você pode aumentar o máximo até 1.024 se tiver usuários que são membros de mais do que o número padrão de grupos.

Sobre esta tarefa

Se um usuário tiver mais do que o número padrão de IDs de grupo em suas credenciais, os IDs de grupo restantes serão truncados e o usuário poderá receber erros ao tentar acessar arquivos do sistema de armazenamento. Você deve definir o número máximo de grupos, por SVM, para um número que represente o máximo de grupos no ambiente.

Para entender os pré-requisitos de autenticação AUTH_SYS para ativar grupos estendidos (`-auth-sys-extended-groups`) que usam IDs de grupo além do máximo padrão de 16, consulte este artigo da base de dados de Conhecimento: "AUTH_SYS grupos estendidos alterações para autenticação NFS para ONTAP 9".

A tabela a seguir mostra os dois parâmetros `vserver nfs modify` do comando que determinam o número máximo de IDs de grupo em três configurações de amostra:

Parâmetros	Definições	Limite de IDs de grupo resultantes

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`32`
	
	`disabled`
	
	Estas são as predefinições.
		RPCSEC_GSS: 32
		
		AUTH_SYS: 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`256`
	
	`disabled`
		RPCSEC_GSS: 256
		
		AUTH_SYS: 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`512`
	
	`enabled`
		RPCSEC_GSS: 512
		
		AUTH_SYS: 512

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute a ação desejada:

Se pretender definir o número máximo de grupos auxiliares permitidos…	Digite o comando…
Apenas para RPCSEC_GSS e deixar AUTH_SYS definido para o valor padrão 16	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled`
Para RPCSEC_GSS e AUTH_SYS	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled`

3. Verifique o `-extended-groups-limit` valor e verifique se AUTH_SYS está usando grupos estendidos: `vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`
4. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Exemplo

O exemplo a seguir habilita grupos estendidos para autenticação AUTH_SYS e define o número máximo de grupos estendidos para 512 para autenticação AUTH_SYS e RPCSEC_GSS. Essas alterações são feitas apenas para clientes que acessam o SVM chamado VS1:

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
------- ------------------------ --------------------
vs1     enabled                  512

vs1::*> set -privilege admin
```

Controle o acesso do usuário raiz aos dados de estilo de segurança NTFS

Você pode configurar o ONTAP para permitir que clientes NFS acessem dados de estilo de segurança NTFS e clientes NTFS para acessar dados de estilo de segurança NFS. Ao usar o estilo de segurança NTFS em um armazenamento de dados NFS, você deve decidir como tratar o acesso pelo usuário raiz e configurar a máquina virtual de armazenamento (SVM) de acordo.

Sobre esta tarefa

Quando um usuário raiz acessa dados de estilo de segurança NTFS, você tem duas opções:

- Mapeie o usuário raiz para um usuário do Windows como qualquer outro usuário NFS e gerencie o acesso de acordo com ACLs NTFS.
- Ignore as ACLs NTFS e forneça acesso total à raiz.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute a ação desejada:

Se você quiser que o usuário root…	Digite o comando…
Ser mapeado para um usuário do Windows	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled`
Ignorar a verificação da ACL NT	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled`

   Por predefinição, este parâmetro está desativado.

   Se este parâmetro estiver ativado, mas não houver mapeamento de nomes para o usuário raiz, o ONTAP usará uma credencial de administrador SMB padrão para auditoria.

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Informações sobre direitos autorais

Informações sobre marcas comerciais