Gerenciar NFS

ONTAP 9

NetApp
February 12, 2026

Índice

Gerenciar NFS . . . 1
Saiba mais sobre o acesso a arquivos ONTAP para o protocolo NFS . . . 1
Entenda o acesso a arquivos nas . . . 1
Namespaces e pontos de junção . . . 1
Como o ONTAP controla o acesso aos arquivos . . . 6
Como o ONTAP lida com a autenticação de cliente NFS . . . 7
Crie e gerencie volumes de dados em namespaces nas . . . 9
Crie volumes ONTAP NAS com pontos de junção especificados . . . 9
Crie volumes ONTAP NAS sem pontos de junção específicos . . . 11
Montar ou desmontar volumes ONTAP NFS no namespace NAS . . . 12
Apresentar informações sobre a montagem de volume e ponto de junção do NAS do ONTAP . . . 14
Configurar estilos de segurança . . . 15
Como os estilos de segurança afetam o acesso aos dados . . . 15
Configurar estilos de segurança em volumes raiz ONTAP NFS SVM . . . 18
Configurar estilos de segurança em volumes ONTAP NFS FlexVol . . . 19
Configurar estilos de segurança em qtrees ONTAP NFS . . . 19
Configurar o acesso a arquivos usando NFS . . . 20
Saiba mais sobre como configurar o acesso a arquivos NFS em SVMs ONTAP . . . 20
Proteja o acesso NFS usando políticas de exportação . . . 20
Usando Kerberos com NFS para segurança forte . . . 33
Configurar serviços de nomes . . . 38
Configurar mapeamentos de nomes . . . 50
Habilitar acesso para clientes NFS do Windows para SVMs ONTAP . . . 56
Habilitar a exibição de exportações em clientes NFS para SVMs ONTAP . . . 57
Gerenciar o acesso a arquivos usando NFS . . . 57
Habilitar ou desabilitar NFSv3 para SVMs ONTAP . . . 57
Habilitar ou desabilitar NFSv4.0 para SVMs ONTAP . . . 58
Habilitar ou desabilitar NFSv4.1 para SVMs ONTAP . . . 58
Gerenciar limites do pool de armazenamento ONTAP NFSv4 . . . 58
Habilitar ou desabilitar pNFS para SVMs ONTAP . . . 60
Controle o acesso NFS via TCP e UDP para SVMs ONTAP . . . 61
Controle solicitações NFS de portas não reservadas para SVMs ONTAP . . . 62
Lidar com acesso NFS a volumes NTFS ONTAP ou qtrees para usuários UNIX desconhecidos . . . 62
Considerações para clientes que montam exportações ONTAP NFS em portas não reservadas . . . 64
Execute uma verificação de acesso mais rigorosa para netgroups verificando domínios para SVMs ONTAP NFS . . . 64
Modificar portas usadas para serviços NFSv3 para SVMs ONTAP . . . 65
Comandos ONTAP para gerenciar servidores NFS . . . 67
Solucionar problemas de serviço de nomes para SVMs ONTAP NAS . . . 68
Verificar conexões de serviço de nomes para SVMs ONTAP NAS . . . 71
Comandos ONTAP para gerenciar entradas de switch de serviço de nomes NAS . . . 72
Comandos ONTAP para gerenciar o cache do serviço de nomes NAS . . . 73
Comandos ONTAP para gerenciar mapeamentos de nomes NFS . . . 73

Comandos ONTAP para gerenciar usuários UNIX locais do NAS . . . 74
Comandos ONTAP para gerenciar grupos UNIX locais NAS . . . 74
Limites para usuários, grupos e membros de grupo UNIX locais para SVMs ONTAP NFS . . . 75
Gerenciar limites para usuários e grupos UNIX locais para SVMs ONTAP NFS . . . 75
Comandos ONTAP para gerenciar grupos de rede locais NFS . . . 76
Comandos ONTAP para gerenciar configurações de domínio NFS NIS . . . 76
Comandos ONTAP para gerenciar configurações de cliente NFS LDAP . . . 77
Comandos ONTAP para gerenciar configurações NFS LDAP . . . 77
Comandos ONTAP para gerenciar modelos de esquema de cliente NFS LDAP . . . 78
Comandos ONTAP para gerenciar configurações de interface NFS Kerberos . . . 78
Comandos ONTAP para gerenciar configurações de domínio NFS Kerberos . . . 79
Comandos ONTAP para gerenciamento de políticas de exportação . . . 79
Comandos ONTAP para gerenciar regras de exportação . . . 80
Configurar o cache de credenciais NFS . . . 80
Gerenciar caches de política de exportação . . . 82
Gerenciar bloqueios de arquivos . . . 86
Aprenda como os filtros de primeira leitura e primeira gravação do ONTAP FPolicy funcionam com o NFS . . . 91
Modificar o ID de implementação do servidor NFSv4.1 para SVMs ONTAP . . . 92
Gerenciar ACLs NFSv4 . . . 93
Gerenciar delegações de arquivos do NFSv4 . . . 96
Configure o bloqueio de arquivos NFSv4 e Registro . . . 98
Saiba mais sobre referências NFSv4 para SVMs ONTAP . . . 99
Habilitar ou desabilitar referências NFSv4 para SVMs ONTAP . . . 99
Exibir estatísticas para SVMs ONTAP NFS . . . 100
Exibir estatísticas de DNS para SVMs ONTAP NFS . . . 101
Exibir estatísticas NIS para SVMs ONTAP NFS . . . 103
Saiba mais sobre o suporte para VMware vStorage sobre ONTAP NFS . . . 105
Habilitar ou desabilitar VMware vStorage sobre ONTAP NFS . . . 106
Habilitar ou desabilitar o suporte a rquota em SVMs ONTAP NFS . . . 107
Saiba mais sobre melhorias de desempenho do NFSv3 e NFSv4 e tamanho de transferência TCP para SVMs ONTAP . . . 107
Modificar o tamanho máximo de transferência TCP NFSv3 e NFSv4 para SVMs ONTAP . . . 108
Configurar o número de IDs de grupo permitidos para usuários NFS para SVMs ONTAP . . . 109
Controlar o acesso do usuário root aos dados de segurança NTFS para SVMs ONTAP . . . 111
Versões e clientes de NFS compatíveis . . . 112
Saiba mais sobre as versões e clientes ONTAP NFS suportados . . . 112
Saiba mais sobre o suporte ONTAP para a funcionalidade NFSv4.0 . . . 112
Saiba mais sobre as limitações de suporte ONTAP para NFSv4 . . . 113
Saiba mais sobre o suporte ONTAP para NFSv4.1 . . . 114
Saiba mais sobre o suporte ONTAP para NFSv4.2 . . . 114
Saiba mais sobre o nconnect para otimizar o desempenho do NFS. . . . 115
Saiba mais sobre o suporte ONTAP para NFS paralelo . . . 116
Saiba mais sobre montagens rígidas ONTAP NFS . . . 116
NFS paralelo . . . 116

Introdução . . . 116
Plano . . . 131
Dependências de nomes de arquivos e diretórios NFS e SMB . . . 141
Aprenda sobre dependências de nomenclatura de arquivos e diretórios ONTAP NFS e SMB . . . 141
Aprenda sobre caracteres válidos em diferentes sistemas operacionais para SVMs ONTAP NFS . . . 141
Aprenda sobre a diferenciação entre maiúsculas e minúsculas de nomes de arquivos e diretórios em um ambiente multiprotocolo ONTAP NFS . . . 141
Aprenda sobre como criar nomes de arquivos e diretórios NFS do ONTAP . . . 142
Aprenda sobre o tratamento de nomes de arquivos, diretórios e qtrees multibyte do ONTAP NFS . . . 143
Configurar mapeamento de caracteres para tradução de nome de arquivo SMB em volumes ONTAP NFS . . . 144
Comandos ONTAP NFS para gerenciar mapeamentos de caracteres para tradução de nomes de arquivos SMB . . . 147

Gerenciar NFS

Saiba mais sobre o acesso a arquivos ONTAP para o protocolo NFS

O ONTAP inclui recursos de acesso a arquivos disponíveis para o protocolo NFS. Você pode habilitar um servidor NFS e exportar volumes ou qtrees.

Você executa este procedimento nas seguintes circunstâncias:

- Você quer entender a variedade de funcionalidades do protocolo NFS da ONTAP.
- Você deseja executar tarefas menos comuns de configuração e manutenção, não configuração básica de NFS.
- Você deseja usar a interface de linha de comando (CLI), não o System Manager ou uma ferramenta de script automatizado.

Entenda o acesso a arquivos nas

Namespaces e pontos de junção

Saiba mais sobre namespaces e pontos de junção do ONTAP NAS

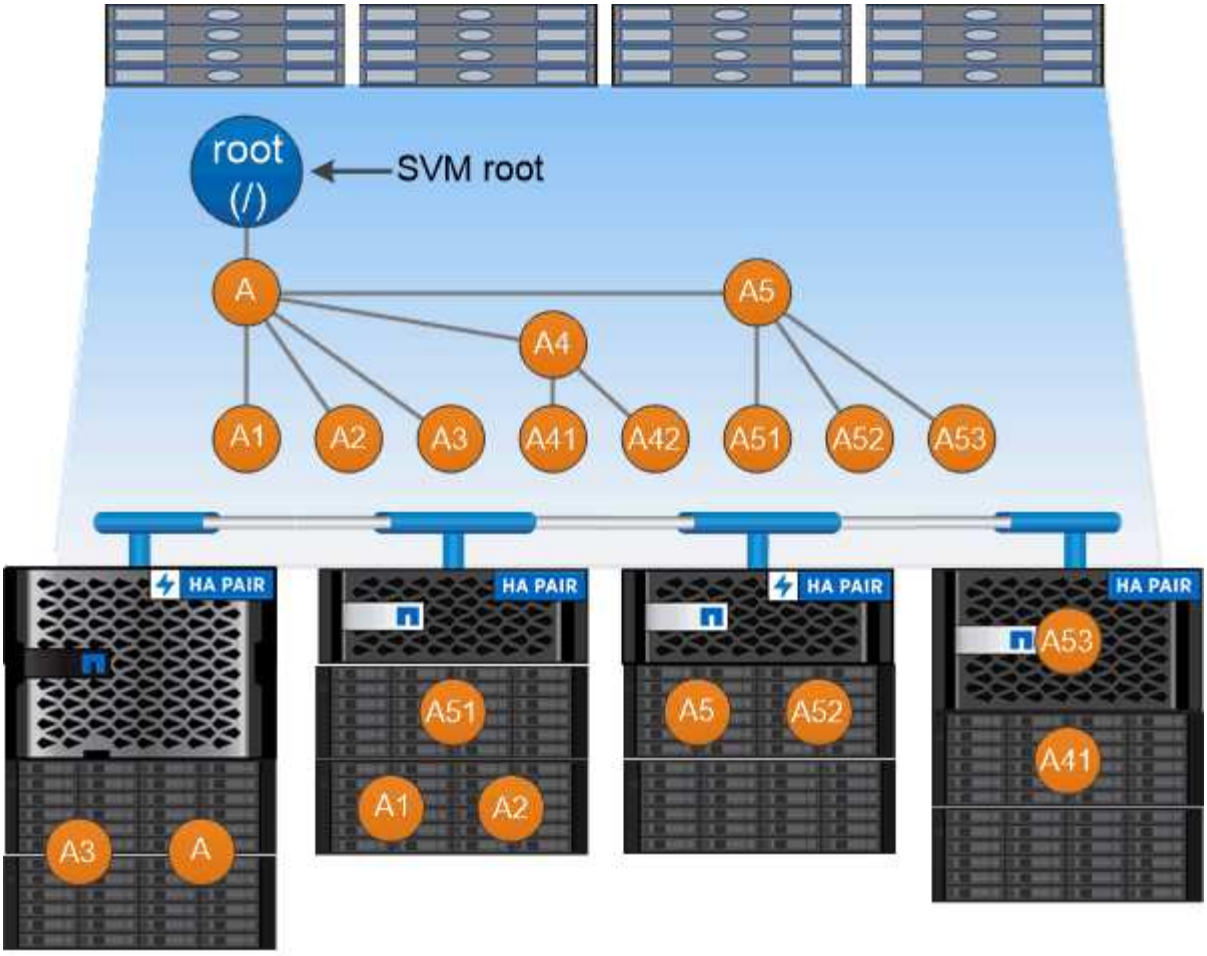
Um nas *namespace* é um agrupamento lógico de volumes Unidos em *pontos de junção* para criar uma única hierarquia de sistema de arquivos. Um cliente com permissões suficientes pode acessar arquivos no namespace sem especificar a localização dos arquivos no armazenamento. Os volumes Junctioned podem residir em qualquer lugar do cluster.

Em vez de montar cada volume contendo um arquivo de interesse, os clientes nas montam um NFS *export* ou acessam um SMB *share.* a exportação ou compartilhamento representa todo o namespace ou um local intermediário dentro do namespace. O cliente acessa apenas os volumes montados abaixo do seu ponto de acesso.

Você pode adicionar volumes ao namespace conforme necessário. Você pode criar pontos de junção diretamente abaixo de uma junção de volume pai ou em um diretório dentro de um volume. Um caminho para uma junção de volume para um volume chamado "'vol3" pode ser `/vol1/vol2/vol3`, ou `/vol1/dir2/vol3`, ou mesmo `/dir1/dir2/vol3`. O caminho é chamado de *caminho de junção.*

Cada SVM tem um namespace único. O volume raiz da SVM é o ponto de entrada para a hierarquia de namespace.

Para garantir que os dados permaneçam disponíveis no caso de uma interrupção do nó ou failover, você deve criar uma cópia de *load-sharing mirror* para o volume raiz da SVM.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

Exemplo

O exemplo a seguir cria um volume chamado "home4" localizado na SVM VS1 que tem um caminho de junção `/eng/home` :

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

Saiba mais sobre arquiteturas de namespace ONTAP NAS

Há várias arquiteturas típicas de namespace nas que você pode usar ao criar seu espaço de nomes SVM. Você pode escolher a arquitetura de namespace que corresponde às necessidades da sua empresa e do fluxo de trabalho.

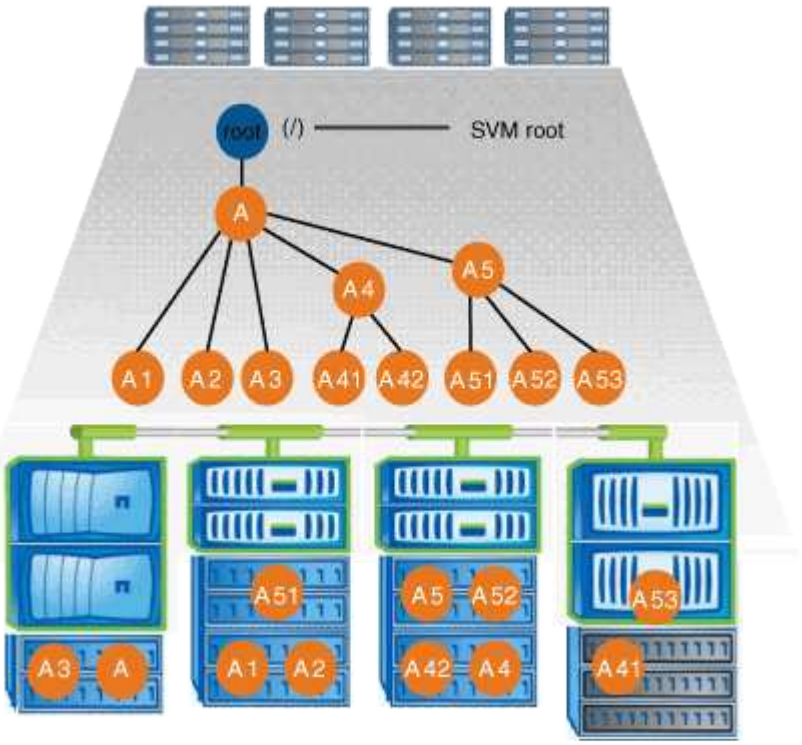
A parte superior do namespace é sempre o volume raiz, que é representado por uma barra (/). A arquitetura de namespace sob a raiz se enquadra em três categorias básicas:

- Uma única árvore ramificada, com apenas uma única junção para a raiz do namespace

- Várias árvores ramificadas, com vários pontos de junção para a raiz do namespace
- Vários volumes independentes, cada um com um ponto de junção separado para a raiz do espaço de nomes

Namespace com árvore ramificada única

Uma arquitetura com uma única árvore ramificada tem um único ponto de inserção para a raiz do namespace SVM. O ponto de inserção único pode ser um volume juntado ou um diretório sob a raiz. Todos os outros volumes são montados em pontos de junção abaixo do ponto de inserção único (que pode ser um volume ou um diretório).

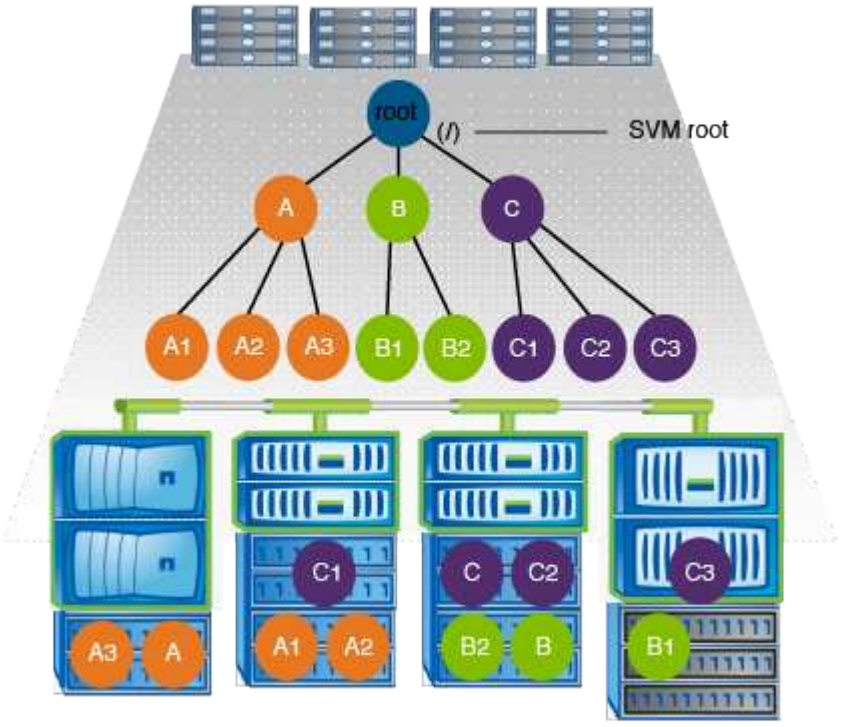


Por exemplo, uma configuração típica de junção de volume com a arquitetura de namespace acima pode parecer com a seguinte configuração, onde todos os volumes são juntados abaixo do ponto de inserção único, que é um diretório chamado "data":

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- -------------------    -----------
vs1     corp1       true     /data/dir1/corp1       RW_volume
vs1     corp2       true     /data/dir1/corp2       RW_volume
vs1     data1       true     /data/data1            RW_volume
vs1     eng1        true     /data/data1/eng1       RW_volume
vs1     eng2        true     /data/data1/eng2       RW_volume
vs1     sales       true     /data/data1/sales      RW_volume
vs1     vol1        true     /data/vol1             RW_volume
vs1     vol2        true     /data/vol2             RW_volume
vs1     vol3        true     /data/vol3             RW_volume
vs1     vs1_root    -        /                      -
```

Namespace com várias árvores ramificadas

Uma arquitetura com várias árvores ramificadas tem vários pontos de inserção na raiz do namespace SVM. Os pontos de inserção podem ser volumes juntados ou diretórios abaixo da raiz. Todos os outros volumes são montados em pontos de junção abaixo dos pontos de inserção (que podem ser volumes ou diretórios).

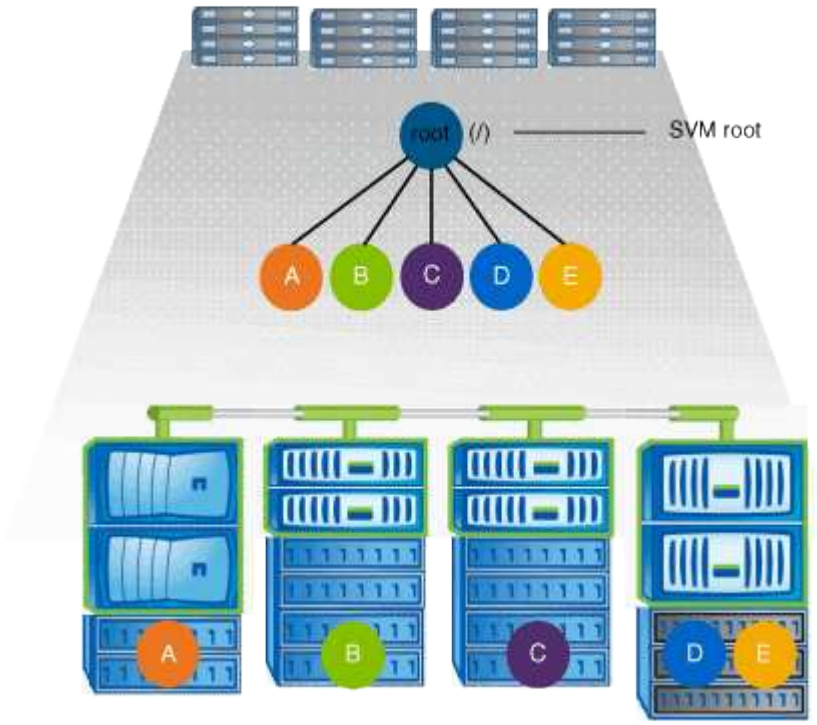


Por exemplo, uma configuração típica de junção de volume com a arquitetura de namespace acima pode parecer com a seguinte configuração, onde há três pontos de inserção para o volume raiz do SVM. Dois pontos de inserção são diretórios denominados "data" e "projetos". Um ponto de inserção é um volume juntado chamado "audit":

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- -------------------    -----------
vs1     audit       true     /audit                 RW_volume
vs1     audit_logs1 true     /audit/logs1           RW_volume
vs1     audit_logs2 true     /audit/logs2           RW_volume
vs1     audit_logs3 true     /audit/logs3           RW_volume
vs1     eng         true     /data/eng              RW_volume
vs1     mktg1       true     /data/mktg1            RW_volume
vs1     mktg2       true     /data/mktg2            RW_volume
vs1     project1    true     /projects/project1     RW_volume
vs1     project2    true     /projects/project2     RW_volume
vs1     vs1_root    -        /                      -
```

Namespace com vários volumes autônomos

Em uma arquitetura com volumes autônomos, cada volume tem um ponto de inserção para a raiz do namespace SVM. No entanto, o volume não é juntado abaixo de outro volume. Cada volume tem um caminho exclusivo e é juntado diretamente abaixo da raiz ou é juntado sob um diretório abaixo da raiz.



Por exemplo, uma configuração típica de junção de volume com a arquitetura de namespace acima pode parecer com a seguinte configuração, onde há cinco pontos de inserção para o volume raiz do SVM, com cada ponto de inserção representando um caminho para um volume.

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- -------------------    -----------
vs1     eng         true     /eng                   RW_volume
vs1     mktg        true     /vol/mktg              RW_volume
vs1     project1    true     /project1              RW_volume
vs1     project2    true     /project2              RW_volume
vs1     sales       true     /sales                 RW_volume
vs1     vs1_root    -        /                      -
```

Como o ONTAP controla o acesso aos arquivos

Saiba mais sobre o controle de acesso a arquivos ONTAP NAS

O ONTAP controla o acesso aos arquivos de acordo com as restrições baseadas em autenticação e em arquivo especificadas.

Quando um cliente se coneta ao sistema de armazenamento para acessar arquivos, o ONTAP tem que executar duas tarefas:

- Autenticação

  O ONTAP tem que autenticar o cliente verificando a identidade com uma fonte confiável. Além disso, o tipo de autenticação do cliente é um método que pode ser usado para determinar se um cliente pode acessar dados ao configurar políticas de exportação (opcional para CIFS).

- Autorização

  O ONTAP tem que autorizar o usuário comparando as credenciais do usuário com as permissões configuradas no arquivo ou diretório e determinando que tipo de acesso, se houver, a fornecer.

Para gerenciar adequadamente o controle de acesso a arquivos, o ONTAP deve se comunicar com serviços externos, como NIS, LDAP e servidores do ative Directory. A configuração de um sistema de storage para acesso a arquivos usando CIFS ou NFS requer a configuração dos serviços apropriados, dependendo do seu ambiente no ONTAP.

Saiba mais sobre restrições baseadas em autenticação para SVMs ONTAP NAS

Com restrições baseadas em autenticação, você pode especificar quais máquinas cliente e quais usuários podem se conetar à máquina virtual de armazenamento (SVM).

O ONTAP suporta autenticação Kerberos de servidores UNIX e Windows.

Saiba mais sobre restrições baseadas em arquivo para SVMs ONTAP NAS

O ONTAP avalia três níveis de segurança para determinar se uma entidade está autorizada a executar uma ação solicitada em arquivos e diretórios localizados em um SVM. O acesso é determinado pelas permissões efetivas após a avaliação dos três níveis de segurança.

Qualquer objeto de armazenamento pode conter até três tipos de camadas de segurança:

- Segurança de exportação (NFS) e compartilhamento (SMB)

  A segurança de exportação e compartilhamento se aplica ao acesso do cliente a uma determinada exportação NFS ou compartilhamento SMB. Os usuários com Privileges administrativo podem gerenciar a segurança de exportação e compartilhamento a partir de clientes SMB e NFS.

- Segurança de arquivo e diretório do Access Guard no nível de armazenamento

  A segurança do Access Guard no nível de storage se aplica ao acesso de clientes SMB e NFS aos volumes SVM. Apenas as permissões de acesso NTFS são suportadas. Para que o ONTAP execute verificações de segurança em usuários UNIX para obter acesso a dados em volumes para os quais o Guarda de Acesso em nível de storage foi aplicado, o usuário do UNIX deve mapear para um usuário do Windows na SVM que possua o volume.

  > Se você exibir as configurações de segurança em um arquivo ou diretório de um cliente NFS ou SMB, não verá a segurança do Storage-Level Access Guard. A segurança do Access Guard no nível de armazenamento não pode ser revogada de um cliente, mesmo por um administrador do sistema (Windows ou UNIX).

- Segurança nativa em nível de arquivo NTFS, UNIX e NFSv4

  A segurança de nível de arquivo nativo existe no arquivo ou diretório que representa o objeto de storage. Você pode definir a segurança no nível do arquivo de um cliente. As permissões de arquivo são efetivas independentemente de SMB ou NFS serem usados para acessar os dados.

Como o ONTAP lida com a autenticação de cliente NFS

Saiba mais sobre autenticação ONTAP para clientes NAS

Os clientes NFS devem ser devidamente autenticados antes de poderem acessar os dados no SVM. O ONTAP autentica os clientes verificando suas credenciais UNIX em relação aos serviços de nome que você configura.

Quando um cliente NFS se coneta ao SVM, o ONTAP obtém as credenciais UNIX para o usuário verificando diferentes serviços de nome, dependendo da configuração dos serviços de nome do SVM. O ONTAP pode verificar credenciais para contas UNIX locais, domínios NIS e domínios LDAP. Pelo menos um deles deve ser configurado para que o ONTAP possa autenticar com êxito o usuário. Você pode especificar vários serviços de nomes e a ordem em que o ONTAP os procura.

Em um ambiente NFS puro com estilos de segurança de volume UNIX, essa configuração é suficiente para autenticar e fornecer o acesso de arquivo adequado para um usuário conetado a partir de um cliente NFS.

Se você estiver usando estilos de segurança de volume misto, NTFS ou unificado, o ONTAP deve obter um nome de usuário SMB para o usuário UNIX para autenticação com um controlador de domínio do Windows. Isso pode acontecer mapeando usuários individuais usando contas UNIX locais ou domínios LDAP, ou usando um usuário SMB padrão em vez disso. Você pode especificar quais serviços de nome o ONTAP pesquisa em qual ordem ou especificar um usuário SMB padrão.

Aprenda como o ONTAP usa serviços de nomes

O ONTAP usa serviços de nome para obter informações sobre usuários e clientes. O ONTAP usa essas informações para autenticar usuários acessando dados ou administrando o sistema de storage e mapear credenciais de usuário em um ambiente misto.

Ao configurar o sistema de storage, você deve especificar quais serviços de nome deseja que o ONTAP use para obter credenciais de usuário para autenticação. O ONTAP oferece suporte aos seguintes serviços de nomes:

- Utilizadores locais (ficheiro)
- Domínios NIS externos (NIS)
- Domínios LDAP externos (LDAP)

Você usa a `vserver services name-service ns-switch` família de comandos para configurar SVMs com as fontes para procurar informações de rede e a ordem na qual pesquisá-las. Esses comandos fornecem a funcionalidade equivalente do `/etc/nsswitch.conf` arquivo em sistemas UNIX.

Quando um cliente NFS se coneta ao SVM, o ONTAP verifica os serviços de nome especificados para obter as credenciais UNIX do usuário. Se os serviços de nome estiverem configurados corretamente e o ONTAP puder obter as credenciais UNIX, o ONTAP autentica o usuário com êxito.

Em um ambiente com estilos de segurança mistos, o ONTAP pode ter que mapear as credenciais do usuário. Você deve configurar os serviços de nome adequadamente para o seu ambiente para permitir que o ONTAP mapeie corretamente as credenciais do usuário.

O ONTAP também usa serviços de nomes para autenticar contas de administrador da SVM. Você deve ter isso em mente ao configurar ou modificar o switch do serviço de nomes para evitar desabilitar acidentalmente a autenticação para contas de administrador SVM. Para obter mais informações sobre usuários de administração do SVM, "Autenticação de administrador e RBAC"consulte .

Conceder acesso ao arquivo ONTAP SMB de clientes NFS

O ONTAP usa a semântica de segurança do sistema de arquivos do Windows NT (NTFS) para determinar se um usuário UNIX, em um cliente NFS, tem acesso a um arquivo com permissões NTFS.

O ONTAP faz isso convertendo o ID de usuário UNIX do usuário (UID) em uma credencial SMB e, em seguida, usando a credencial SMB para verificar se o usuário tem direitos de acesso ao arquivo. Uma credencial SMB consiste em um SID (Identificador de Segurança primário), geralmente o nome de usuário do Windows do usuário e um ou mais SIDs de grupo que correspondem aos grupos do Windows dos quais o usuário é membro.

O Time ONTAP leva a conversão do UID UNIX em uma credencial SMB pode ser de dezenas de milissegundos a centenas de milissegundos, porque o processo envolve entrar em Contato com um controlador de domínio. O ONTAP mapeia o UID para a credencial SMB e insere o mapeamento em um cache de credenciais para reduzir o tempo de verificação causado pela conversão.

Como funciona o cache de credenciais ONTAP NFS

Quando um usuário NFS solicita acesso às exportações de NFS no sistema de storage,

o ONTAP deve recuperar as credenciais de usuário de servidores de nomes externos ou de arquivos locais para autenticar o usuário. Em seguida, o ONTAP armazena essas credenciais em um cache interno de credenciais para referência posterior. Entender como os caches de credenciais NFS funcionam permite que você lide com possíveis problemas de desempenho e acesso.

Sem o cache de credenciais, o ONTAP teria que consultar serviços de nomes sempre que um usuário NFS solicitou acesso. Em um sistema de armazenamento ocupado que é acessado por muitos usuários, isso pode rapidamente levar a sérios problemas de desempenho, causando atrasos indesejados ou até mesmo negações ao acesso do cliente NFS.

Com o cache de credenciais, o ONTAP recupera as credenciais do usuário e as armazena por um período predeterminado de tempo para acesso rápido e fácil caso o cliente NFS envie outra solicitação. Este método oferece as seguintes vantagens:

- Ele facilita a carga no sistema de armazenamento, manipulando menos solicitações para servidores de nomes externos (como NIS ou LDAP).
- Ele facilita a carga em servidores de nomes externos, enviando menos solicitações para eles.
- Ele acelera o acesso do usuário eliminando o tempo de espera para obter credenciais de fontes externas antes que o usuário possa ser autenticado.

O ONTAP armazena credenciais positivas e negativas no cache de credenciais. Credenciais positivas significa que o usuário foi autenticado e recebeu acesso. Credenciais negativas significa que o usuário não foi autenticado e foi negado o acesso.

Por padrão, o ONTAP armazena credenciais positivas por 24 horas; ou seja, após a autenticação inicial de um usuário, o ONTAP usa as credenciais em cache para quaisquer solicitações de acesso por esse usuário por 24 horas. Se o usuário solicitar acesso após 24 horas, o ciclo será iniciado novamente: O ONTAP descarta as credenciais armazenadas em cache e obtém as credenciais novamente a partir da fonte de serviço de nome apropriada. Se as credenciais tiverem sido alteradas no servidor de nomes durante as 24 horas anteriores, o ONTAP armazena em cache as credenciais atualizadas para uso nas próximas 24 horas.

Por padrão, o ONTAP armazena credenciais negativas por duas horas; ou seja, depois de inicialmente negar acesso a um usuário, o ONTAP continua negando quaisquer solicitações de acesso por esse usuário por duas horas. Se o usuário solicitar acesso após 2 horas, o ciclo será iniciado novamente: O ONTAP obtém as credenciais novamente da fonte de serviço de nome apropriada. Se as credenciais tiverem sido alteradas no servidor de nomes durante as duas horas anteriores, o ONTAP armazena em cache as credenciais atualizadas para uso nas próximas duas horas.

Crie e gerencie volumes de dados em namespaces nas

Crie volumes ONTAP NAS com pontos de junção especificados

Pode especificar o ponto de junção quando cria um volume de dados. O volume resultante é montado automaticamente no ponto de junção e está imediatamente disponível para configurar para acesso nas.

Antes de começar

- O agregado no qual você deseja criar o volume já deve existir.
- A partir do ONTAP 9.13.1, você pode criar volumes com análise de capacidade e acompanhamento de

atividades habilitados. Para ativar o acompanhamento de capacidade ou atividade, emita o `volume create` comando com `-analytics-state` ou `-activity-tracking-state` defina como `on`.

Para saber mais sobre análise de capacidade e acompanhamento de atividades, "Ative a análise do sistema de ficheiros" consulte . Saiba mais sobre `volume create` o "Referência do comando ONTAP"na .

Os seguintes carateres não podem ser usados no caminho de junção: `* # " > < | ? \`

Além disso, o comprimento do caminho de junção não pode ter mais de 255 carateres.

Passos

1. Crie o volume com um ponto de junção:

```
volume create -vserver <vserver_name> -volume <volume_name> -aggregate
<aggregate_name> -size {integer[KB|MB|GB|TB|PB]} -security-style
{ntfs|unix|mixed} -junction-path <junction_path>
```

   O caminho de junção deve começar com a raiz (/) e pode conter diretórios e volumes juntados. O caminho de junção não precisa conter o nome do volume. Os caminhos de junção são independentes do nome do volume.

   Especificar um estilo de segurança de volume é opcional. Se você não especificar um estilo de segurança, o ONTAP criará o volume com o mesmo estilo de segurança aplicado ao volume raiz da máquina virtual de storage (SVM). No entanto, o estilo de segurança do volume raiz pode não ser o estilo de segurança que você deseja aplicar ao volume de dados criado. A recomendação é especificar o estilo de segurança quando você cria o volume para minimizar problemas de acesso a arquivos difíceis de solucionar.

   O caminho de junção é insensível a maiúsculas e minúsculas; `/ENG` é o mesmo que `/eng`. Se você criar um compartilhamento CIFS, o Windows tratará o caminho de junção como se ele fosse sensível a maiúsculas e minúsculas. Por exemplo, se a junção for `/ENG`, o caminho de um compartilhamento SMB deve começar com `/ENG`, não `/eng`.

   Há muitos parâmetros opcionais que você pode usar para personalizar um volume de dados. Saiba mais sobre `volume create` o "Referência do comando ONTAP"na .

2. Verifique se o volume foi criado com o ponto de junção desejado:

```
volume show -vserver <vserver_name> -volume <volume_name> -junction
```

Exemplo

O exemplo a seguir cria um volume chamado `home4` localizado no SVM VS1 que tem um caminho de junção `/eng/home` :

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

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

Crie volumes ONTAP NAS sem pontos de junção específicos

Você pode criar um volume de dados sem especificar um ponto de junção. O volume resultante não é montado automaticamente e não está disponível para configuração para acesso nas. É necessário montar o volume antes de configurar compartilhamentos SMB ou exportações NFS para esse volume.

Antes de começar

- O agregado no qual você deseja criar o volume já deve existir.
- A partir do ONTAP 9.13.1, você pode criar volumes com análise de capacidade e acompanhamento de atividades habilitados. Para ativar o acompanhamento de capacidade ou atividade, emita o `volume create` comando com `-analytics-state` ou `-activity-tracking-state` defina como `on`.

  Para saber mais sobre análise de capacidade e acompanhamento de atividades, "Ative a análise do sistema de ficheiros" consulte . Saiba mais sobre `volume create` o "Referência do comando ONTAP"na .

Passos

1. Crie o volume sem um ponto de junção usando o seguinte comando:

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate
   aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
   {ntfs|unix|mixed}
   ```

   Especificar um estilo de segurança de volume é opcional. Se você não especificar um estilo de segurança, o ONTAP criará o volume com o mesmo estilo de segurança aplicado ao volume raiz da máquina virtual de storage (SVM). No entanto, o estilo de segurança do volume raiz pode não ser o estilo de segurança que você deseja aplicar ao volume de dados. A recomendação é especificar o estilo de segurança quando você cria o volume para minimizar problemas de acesso a arquivos difíceis de solucionar.

   Há muitos parâmetros opcionais que você pode usar para personalizar um volume de dados. Saiba mais sobre `volume create` o "Referência do comando ONTAP"na .

2. Verifique se o volume foi criado sem um ponto de junção:

   ```
   volume show -vserver vserver_name -volume volume_name -junction
   ```

Exemplo

O exemplo a seguir cria um volume chamado "vendas" localizado no SVM VS1 que não está montado em um ponto de junção:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                    Junction                 Junction
Vserver   Volume    Active   Junction Path   Path Source
--------- --------- -------- --------------- -----------
vs1       data      true     /data           RW_volume
vs1       home4     true     /eng/home       RW_volume
vs1       vs1_root  -        /               -
vs1       sales     -        -               -
```

Montar ou desmontar volumes ONTAP NFS no namespace NAS

Um volume deve ser montado no namespace nas antes de poder configurar o acesso do cliente nas aos dados contidos nos volumes de máquina virtual de storage (SVM). Você pode montar um volume em um ponto de junção se ele não estiver montado no momento. Você também pode desmontar volumes.

Sobre esta tarefa

Se você desmontar e colocar um volume off-line, todos os dados dentro do ponto de junção, incluindo dados em volumes com pontos de junção contidos no namespace do volume não montado, ficarão inacessíveis para clientes nas.

> Para interromper o acesso de cliente nas a um volume, não é suficiente simplesmente desmontar o volume. Você deve colocar o volume off-line ou tomar outras medidas para garantir que os caches de manipulação de arquivos do lado do cliente sejam invalidados. Para obter mais informações, consulte o seguinte artigo da base de dados de Conhecimento:
>
> "Os clientes NFSv3 ainda têm acesso a um volume depois de serem removidos do namespace no ONTAP"

Quando você desmontar e off-line um volume, os dados dentro do volume não são perdidos. Além disso, políticas de exportação de volume existentes e compartilhamentos SMB criados no volume ou em diretórios e pontos de junção dentro do volume não montado são retidos. Se você remontar o volume não montado, os clientes nas poderão acessar os dados contidos no volume usando políticas de exportação e compartilhamentos SMB existentes.

Passos

1. Execute a ação desejada:

Se você quiser…	Digite os comandos…
Monte um volume	`volume mount -vserver svm_name -volume volume_name -junction-path junction_path`

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

2. Verifique se o volume está no estado de montagem desejado:

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

Exemplos

O exemplo a seguir monta um volume chamado "vendas" localizado na SVM "VS1" no ponto de junção ""/vendas":

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

O exemplo a seguir desmonta e fica offline um volume chamado "data" localizado na SVM ""VS1":

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

Apresentar informações sobre a montagem de volume e ponto de junção do NAS do ONTAP

Você pode exibir informações sobre volumes montados para máquinas virtuais de armazenamento (SVMs) e os pontos de junção para os quais os volumes são montados. Você também pode determinar quais volumes não estão montados em um ponto de junção. Use essas informações para entender e gerenciar seu namespace SVM.

Passo

1. Execute a ação desejada:

Se você quiser exibir…	Digite o comando…
Informações resumidas sobre volumes montados e não montados no SVM	`volume show -vserver` *`vserver_name`* `-junction`
Informações detalhadas sobre volumes montados e não montados no SVM	`volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-instance`
Informações específicas sobre volumes montados e não montados no SVM	a. Se necessário, você pode exibir campos válidos para o `-fields` parâmetro usando o seguinte comando: `volume show -fields ?` b. Apresentar a informação pretendida utilizando o `-fields` parâmetro: `volume show -vserver` *`vserver_name`* `-fields` *`fieldname`*`,…`

Exemplos

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

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

O exemplo a seguir exibe informações sobre campos especificados para volumes localizados no SVM VS2:

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

Configurar estilos de segurança

Como os estilos de segurança afetam o acesso aos dados

Saiba mais sobre os estilos de segurança do ONTAP NAS

Existem quatro estilos de segurança diferentes: UNIX, NTFS, misto e unificado. Cada estilo de segurança tem um efeito diferente sobre como as permissões são tratadas para os dados. Você deve entender os diferentes efeitos para garantir que você selecione o estilo de segurança apropriado para seus propósitos.

É importante entender que os estilos de segurança não determinam quais tipos de clientes podem ou não acessar dados. Os estilos de segurança determinam apenas o tipo de permissões que o ONTAP usa para controlar o acesso aos dados e que tipo de cliente pode modificar essas permissões.

Por exemplo, se um volume usa estilo de segurança UNIX, os clientes SMB ainda podem acessar dados (desde que autentiquem e autorizem adequadamente) devido à natureza multiprotocolo do ONTAP. No entanto, o ONTAP usa permissões UNIX que somente clientes UNIX podem modificar usando ferramentas nativas.

Estilo de segurança	Clientes que podem modificar permissões	Permissões que os clientes podem usar	Estilo de segurança eficaz resultante	Clientes que podem acessar arquivos
UNIX	NFS	NFSv3 bits de modo	UNIX	NFS e SMB
		ACLs NFSv4.x		
NTFS	SMB	ACLs NTFS	NTFS	
Misto	NFS ou SMB	NFSv3 bits de modo	UNIX	
		NFSv4.ACLs		
		ACLs NTFS	NTFS	
Unificado (somente para volumes infinitos, no ONTAP 9.4 e versões anteriores).	NFS ou SMB	NFSv3 bits de modo	UNIX	
		ACLs NFSv4,1		
		ACLs NTFS	NTFS	

Os volumes FlexVol suportam estilos de segurança UNIX, NTFS e mistos. Quando o estilo de segurança é misto ou unificado, as permissões efetivas dependem do tipo de cliente que modificou as permissões pela última vez porque os usuários definem o estilo de segurança individualmente. Se o último cliente que modificou permissões fosse um cliente NFSv3, as permissões são bits do modo UNIX NFSv3. Se o último cliente foi um cliente NFSv4, as permissões são NFSv4 ACLs. Se o último cliente foi um cliente SMB, as permissões são ACLs do Windows NTFS.

O estilo de segurança unificado só está disponível com volumes infinitos, que não são mais suportados no ONTAP 9.5 e versões posteriores. Para obter mais informações, Visão geral do gerenciamento do FlexGroup volumesconsulte .

O `show-effective-permissions` parâmetro com o `vserver security file-directory` O comando permite que você exiba permissões efetivas concedidas a um usuário do Windows ou UNIX no caminho de arquivo ou pasta especificado. Além disso, o parâmetro opcional `-share-name` permite exibir a permissão de compartilhamento efetivo. Saiba mais sobre `vserver security file-directory show-effective-permissions` o "Referência do comando ONTAP"na .

> O ONTAP define inicialmente algumas permissões de arquivo padrão. Por padrão, o estilo de segurança eficaz em todos os dados em UNIX, volumes mistos e de estilo de segurança unificado é UNIX e o tipo de permissões efetivas é bits de modo UNIX (0755 a menos que especificado de outra forma) até ser configurado por um cliente como permitido pelo estilo de segurança padrão. Por padrão, o estilo de segurança eficaz em todos os dados em volumes de estilo de segurança NTFS é NTFS e tem uma ACL que permite o controle total para todos.

Informações relacionadas

- "Referência do comando ONTAP"

Aprenda sobre estilos de segurança em volumes ONTAP NFS FlexVol

Os estilos de segurança podem ser definidos em volumes FlexVol (raiz ou volumes de dados) e qtrees. Os estilos de segurança podem ser definidos manualmente no momento da criação, herdados automaticamente ou alterados posteriormente.

Decida qual estilo de segurança usar em SVMs ONTAP NAS

Para ajudá-lo a decidir qual estilo de segurança usar em um volume, você deve considerar dois fatores. O fator principal é o tipo de administrador que gerencia o sistema de arquivos. O fator secundário é o tipo de usuário ou serviço que acessa os dados no volume.

Ao configurar o estilo de segurança em um volume, você deve considerar as necessidades do seu ambiente para garantir que você selecione o melhor estilo de segurança e evite problemas com o gerenciamento de permissões. As seguintes considerações podem ajudá-lo a decidir:

Estilo de segurança	Escolha se…
UNIX	• O sistema de arquivos é gerenciado por um administrador UNIX. • A maioria dos usuários são clientes NFS. • Um aplicativo que acessa os dados usa um usuário UNIX como a conta de serviço.
NTFS	• O sistema de arquivos é gerenciado por um administrador do Windows. • A maioria dos usuários são clientes SMB. • Um aplicativo que acessa os dados usa um usuário do Windows como a conta de serviço.
Misto	• O sistema de arquivos é gerenciado por administradores UNIX e Windows e os usuários consistem em clientes NFS e SMB.

Saiba mais sobre a herança de estilo de segurança NFS do ONTAP

Se você não especificar o estilo de segurança ao criar um novo FlexVol volume ou uma qtree, ele herdará seu estilo de segurança de maneiras diferentes.

Os estilos de segurança são herdados da seguinte maneira:

- Um FlexVol volume herda o estilo de segurança do volume raiz do SVM.
- Uma qtree herda o estilo de segurança do seu que contém FlexVol volume.
- Um arquivo ou diretório herda o estilo de segurança dele contendo FlexVol volume ou qtree.

Saiba mais sobre a preservação de permissões ONTAP NFS UNIX

Quando os arquivos em um FlexVol volume que atualmente têm permissões UNIX são editados e salvos por aplicativos do Windows, o ONTAP pode preservar as permissões UNIX.

Quando os aplicativos em clientes do Windows editam e salvam arquivos, eles leem as propriedades de segurança do arquivo, criam um novo arquivo temporário, aplicam essas propriedades ao arquivo temporário e dão ao arquivo temporário o nome do arquivo original.

Quando os clientes Windows executam uma consulta para as propriedades de segurança, eles recebem uma ACL construída que representa exatamente as permissões UNIX. O único propósito desta ACL construída é

preservar as permissões UNIX do arquivo, pois os arquivos são atualizados por aplicativos do Windows para garantir que os arquivos resultantes tenham as mesmas permissões UNIX. O ONTAP não define nenhuma ACLs NTFS usando a ACL construída.

Gerenciar permissões UNIX em SVMs ONTAP NFS usando a guia Segurança do Windows

Se você quiser manipular permissões UNIX de arquivos ou pastas em volumes mistos de estilo de segurança ou qtrees em SVMs, você pode usar a guia Segurança em clientes Windows. Como alternativa, você pode usar aplicativos que podem consultar e definir ACLs do Windows.

- Modificação de permissões UNIX

  Você pode usar a guia Segurança do Windows para exibir e alterar permissões UNIX para um volume ou qtree misto de estilo de segurança. Se você usar a guia principal de Segurança do Windows para alterar permissões UNIX, primeiro remova o ACE existente que deseja editar (isso define os bits de modo como 0) antes de fazer as alterações. Como alternativa, você pode usar o editor avançado para alterar permissões.

  Se as permissões de modo forem usadas, você pode alterar diretamente as permissões de modo para o UID listado, GID e outros (todos os outros com uma conta no computador). Por exemplo, se o UID exibido tiver permissões r-x, você pode alterar as permissões UID para rwx.

- Alterando permissões UNIX para permissões NTFS

  Você pode usar a guia Segurança do Windows para substituir objetos de segurança UNIX por objetos de segurança do Windows em um volume de estilo de segurança misto ou qtree onde os arquivos e pastas têm um estilo de segurança eficaz UNIX.

  Você deve primeiro remover todas as entradas de permissão UNIX listadas antes de poder substituí-las pelos objetos de Usuário e Grupo do Windows desejados. Em seguida, você pode configurar ACLs baseadas em NTFS nos objetos Usuário e Grupo do Windows. Removendo todos os objetos de segurança UNIX e adicionando apenas usuários e grupos do Windows a um arquivo ou pasta em um volume ou qtree misto de estilo de segurança, você altera o estilo de segurança efetivo no arquivo ou pasta de UNIX para NTFS.

  Ao alterar permissões em uma pasta, o comportamento padrão do Windows é propagar essas alterações para todas as subpastas e arquivos. Portanto, você deve alterar a opção de propagação para a configuração desejada se não quiser propagar uma alteração no estilo de segurança para todas as pastas, subpastas e arquivos filhos.

Configurar estilos de segurança em volumes raiz ONTAP NFS SVM

Você configura o estilo de segurança do volume raiz da máquina virtual de storage (SVM) para determinar o tipo de permissões usado para dados no volume raiz do SVM.

Passos

1. Use o `vserver create` comando com o `-rootvolume-security-style` parâmetro para definir o estilo de segurança.

   As opções possíveis para o estilo de segurança do volume raiz são `unix`, `ntfs` ou `mixed`.

2. Exiba e verifique a configuração, incluindo o estilo de segurança do volume raiz do SVM criado:

   `vserver show -vserver vserver_name`

Configurar estilos de segurança em volumes ONTAP NFS FlexVol

Você configura o estilo de segurança do FlexVol volume para determinar o tipo de permissões usadas para dados nos volumes do FlexVol da máquina virtual de storage (SVM).

Passos

1. Execute uma das seguintes ações:

Se o FlexVol volume…	Use o comando…
Ainda não existe	`volume create` e inclua o `-security-style` parâmetro para especificar o estilo de segurança.
Já existe	`volume modify` e inclua o `-security-style` parâmetro para especificar o estilo de segurança.

   As opções possíveis para o estilo de segurança do FlexVol volume são `unix`, `ntfs` ou `mixed`.

   Se você não especificar um estilo de segurança ao criar um FlexVol volume, o volume herdará o estilo de segurança do volume raiz.

   Para obter mais informações sobre os `volume create` comandos ou `volume modify`, "Gerenciamento de storage lógico"consulte .

2. Para exibir a configuração, incluindo o estilo de segurança do FlexVol volume criado, digite o seguinte comando:

   `volume show -volume volume_name -instance`

Configurar estilos de segurança em qtrees ONTAP NFS

Você configura o estilo de segurança do volume de qtree para determinar o tipo de permissões usadas para dados no qtrees.

Passos

1. Execute uma das seguintes ações:

Se a qtree…	Use o comando…
Ainda não existe	`volume qtree create` e inclua o `-security-style` parâmetro para especificar o estilo de segurança.

Já existe	`volume qtree modify` e inclua o `-security-style` parâmetro para especificar o estilo de segurança.

As opções possíveis para o estilo de segurança de qtree são `unix`, `ntfs`, ou `mixed`.

Se você não especificar um estilo de segurança ao criar uma qtree, o estilo de segurança padrão será `mixed`.

Para obter mais informações sobre os `volume qtree create` comandos ou `volume qtree modify`, "Gerenciamento de storage lógico"consulte .

2. Para exibir a configuração, incluindo o estilo de segurança da qtree que você criou, digite o seguinte comando: `volume qtree show -qtree qtree_name -instance`

Configurar o acesso a arquivos usando NFS

Saiba mais sobre como configurar o acesso a arquivos NFS em SVMs ONTAP

Você deve concluir várias etapas para permitir que os clientes acessem arquivos em máquinas virtuais de armazenamento (SVMs) usando NFS. Existem algumas etapas adicionais que são opcionais, dependendo da configuração atual do seu ambiente.

Para que os clientes possam acessar arquivos em SVMs usando NFS, você deve concluir as seguintes tarefas:

1. Habilite o protocolo NFS na SVM.

   Você precisa configurar o SVM para permitir acesso a dados de clientes em NFS.

2. Criar um servidor NFS no SVM.

   Um servidor NFS é uma entidade lógica no SVM que permite que o SVM forneça arquivos em NFS. Você deve criar o servidor NFS e especificar as versões do protocolo NFS que deseja permitir.

3. Configurar políticas de exportação no SVM.

   Você deve configurar políticas de exportação para tornar os volumes e qtrees disponíveis para os clientes.

4. Configure o servidor NFS com a segurança adequada e outras configurações, dependendo da rede e do ambiente de armazenamento.

   Esta etapa pode incluir a configuração Kerberos, LDAP, NIS, mapeamentos de nomes e usuários locais.

Proteja o acesso NFS usando políticas de exportação

Como as políticas de exportação controlam o acesso do cliente aos volumes ou qtrees do ONTAP NFS

As políticas de exportação contêm uma ou mais *regras de exportação* que processam cada solicitação de acesso de cliente. O resultado do processo determina se o cliente é negado ou concedido acesso e que nível de acesso. Uma política de exportação com

regras de exportação deve existir na máquina virtual de storage (SVM) para que os clientes acessem os dados.

Você associa exatamente uma política de exportação a cada volume ou qtree para configurar o acesso do cliente ao volume ou qtree. O SVM pode conter várias políticas de exportação. Isso permite que você faça o seguinte para SVMs com vários volumes ou qtrees:

- Atribua diferentes políticas de exportação a cada volume ou qtree do SVM para controle de acesso de cliente individual a cada volume ou qtree no SVM.
- Atribua a mesma política de exportação a vários volumes ou qtrees do SVM para controle de acesso de cliente idêntico sem ter que criar uma nova política de exportação para cada volume ou qtree.

Se um cliente fizer uma solicitação de acesso que não é permitida pela política de exportação aplicável, a solicitação falhará com uma mensagem de permissão negada. Se um cliente não corresponder a nenhuma regra na política de exportação, o acesso será negado. Se uma política de exportação estiver vazia, todos os acessos serão implicitamente negados.

Você pode modificar uma política de exportação dinamicamente em um sistema executando o ONTAP.

Políticas de exportação padrão para SVMs ONTAP NFS

Cada SVM tem uma política de exportação padrão que não contém regras. Uma política de exportação com regras deve existir antes que os clientes possam acessar os dados no SVM. Cada FlexVol volume contido no SVM deve estar associado a uma política de exportação.

Ao criar um SVM, o sistema de storage cria automaticamente uma política de exportação padrão chamada `default` volume raiz do SVM. Você deve criar uma ou mais regras para a política de exportação padrão antes que os clientes possam acessar os dados no SVM. Como alternativa, você pode criar uma política de exportação personalizada com regras. Você pode modificar e renomear a política de exportação padrão, mas não pode excluir a política de exportação padrão.

Quando você cria um FlexVol volume que contém o SVM, o sistema de storage cria o volume e associa o volume à política de exportação padrão para o volume raiz do SVM. Por padrão, cada volume criado no SVM está associado à política de exportação padrão do volume raiz. Você pode usar a política de exportação padrão para todos os volumes contidos no SVM ou criar uma política de exportação exclusiva para cada volume. Você pode associar vários volumes à mesma política de exportação.

Como funcionam as regras de exportação do ONTAP NFS

As regras de exportação são os elementos funcionais de uma política de exportação. As regras de exportação correspondem às solicitações de acesso do cliente a um volume em relação aos parâmetros específicos que você configura para determinar como lidar com as solicitações de acesso do cliente.

Uma política de exportação deve conter pelo menos uma regra de exportação para permitir o acesso aos clientes. Se uma política de exportação contiver mais de uma regra, as regras serão processadas na ordem em que aparecem na política de exportação. A ordem da regra é ditada pelo número do índice da regra. Se uma regra corresponder a um cliente, as permissões dessa regra serão usadas e nenhuma outra regra será processada. Se nenhuma regra corresponder, o cliente é negado o acesso.

Você pode configurar regras de exportação para determinar permissões de acesso do cliente usando os

seguintes critérios:

- O protocolo de acesso ao arquivo usado pelo cliente que envia a solicitação, por exemplo, NFSv4 ou SMB.
- Um identificador de cliente, por exemplo, nome de host ou endereço IP.

  O tamanho máximo para o `-clientmatch` campo é de 4096 carateres.

- O tipo de segurança usado pelo cliente para autenticar, por exemplo, Kerberos v5, NTLM ou AUTH_SYS.

Se uma regra especificar vários critérios, o cliente deve corresponder a todos eles para que a regra seja aplicada.

> A partir do ONTAP 9.3, você pode habilitar a verificação de configuração de política de exportação como uma tarefa em segundo plano que Registra quaisquer violações de regras em uma lista de regras de erro. Os `vserver export-policy config-checker` comandos invocam o verificador e exibem resultados, que podem ser usados para verificar sua configuração e excluir regras errôneas da política.
>
> Os comandos apenas validam a configuração de exportação para nomes de host, netgroups e usuários anônimos.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

A solicitação de acesso do cliente é enviada usando o protocolo NFSv3 e o cliente tem o endereço IP 10,1.17,37.

Mesmo que o protocolo de acesso do cliente corresponda, o endereço IP do cliente está em uma sub-rede diferente da especificada na regra de exportação. Portanto, a correspondência do cliente falha e esta regra não se aplica a este cliente.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

A solicitação de acesso do cliente é enviada usando o protocolo NFSv4 e o cliente tem o endereço IP 10,1.16,54.

O protocolo de acesso do cliente corresponde e o endereço IP do cliente está na sub-rede especificada. Portanto, a correspondência do cliente é bem-sucedida e esta regra se aplica a este cliente. O cliente obtém

acesso de leitura e gravação independentemente do seu tipo de segurança.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

O cliente nº 1 tem o endereço IP 10,1.16,207, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com Kerberos v5.

O cliente nº 2 tem o endereço IP 10,1.16,211, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com AUTH_SYS.

O protocolo de acesso do cliente e o endereço IP correspondem a ambos os clientes. O parâmetro somente leitura permite o acesso somente leitura a todos os clientes, independentemente do tipo de segurança com o qual eles autenticaram. Portanto, ambos os clientes recebem acesso somente leitura. No entanto, somente o cliente nº 1 obtém acesso de leitura e gravação porque usou o tipo de segurança aprovado Kerberos v5 para autenticar. O cliente nº 2 não obtém acesso de leitura e gravação.

Gerenciar acesso ONTAP SVM para clientes NFS com tipos de segurança não listados

Quando um cliente se apresenta com um tipo de segurança que não está listado em um parâmetro de acesso de uma regra de exportação, você tem a opção de negar acesso ao cliente ou mapeá-lo para o ID de usuário anônimo usando a opção `none` no parâmetro de acesso.

Um cliente pode apresentar-se com um tipo de segurança que não está listado em um parâmetro de acesso porque foi autenticado com um tipo de segurança diferente ou não foi autenticado de todo (tipo de segurança AUTH_NONE). Por padrão, o cliente é automaticamente negado o acesso a esse nível. No entanto, você pode adicionar a opção `none` ao parâmetro Access. Como resultado, os clientes com um estilo de segurança não listado são mapeados para o ID de usuário anônimo. O `-anon` parâmetro determina qual ID de usuário é atribuído a esses clientes. O ID de usuário especificado para o `-anon` parâmetro deve ser um usuário válido que esteja configurado com permissões que você considere apropriadas para o usuário anônimo.

Valores válidos para o `-anon` intervalo de parâmetros `0` de a `65535`.

ID de utilizador atribuída a `-anon`	**Processamento resultante de solicitações de acesso do cliente**
`0 - 65533`	A solicitação de acesso do cliente é mapeada para o ID de usuário anônimo e obtém acesso dependendo das permissões configuradas para esse usuário.
`65534`	A solicitação de acesso do cliente é mapeada para o usuário ninguém e obtém acesso dependendo das permissões configuradas para esse usuário. Este é o padrão.

ID de utilizador atribuída a `-anon`	Processamento resultante de solicitações de acesso do cliente
`65535`	A solicitação de acesso de qualquer cliente é negada quando mapeada para essa ID e o cliente se apresenta com o tipo de segurança AUTH_NONE. A solicitação de acesso de clientes com ID de usuário 0 é negada quando mapeada para essa ID e o cliente se apresenta com qualquer outro tipo de segurança.

Ao usar a opção `none`, é importante lembrar que o parâmetro somente leitura é processado primeiro. Considere as seguintes diretrizes ao configurar regras de exportação para clientes com tipos de segurança não listados:

Somente leitura inclui `none`	A leitura-gravação inclui `none`	Acesso resultante para clientes com tipos de segurança não listados
Não	Não	Negado
Não	Sim	Negado porque somente leitura é processada primeiro
Sim	Não	Somente leitura como anônima
Sim	Sim	Leia-escreva como anônimo

Exemplos

O exemplo a seguir mostra uma política de exportação com um `-rwrule any` parâmetro:

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

O cliente nº 1 tem o endereço IP 10,1.16,207, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com Kerberos v5.

O cliente nº 2 tem o endereço IP 10,1.16,211, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com AUTH_SYS.

O cliente nº 3 tem o endereço IP 10,1.16,234, envia uma solicitação de acesso usando o protocolo NFSv3 e não autenticou (ou seja, o tipo de segurança AUTH_NONE).

O protocolo de acesso do cliente e o endereço IP correspondem aos três clientes. O parâmetro somente leitura permite o acesso somente leitura a clientes com seu próprio ID de usuário autenticado com

AUTH_SYS. O parâmetro somente leitura permite o acesso somente leitura como usuário anônimo com ID de usuário 70 para clientes autenticados usando qualquer outro tipo de segurança. O parâmetro read-write permite o acesso de leitura-gravação a qualquer tipo de segurança, mas neste caso só se aplica a clientes já filtrados pela regra somente leitura.

Portanto, os clientes nº 1 e nº 3 recebem acesso de leitura e gravação apenas como usuário anônimo com ID de usuário 70. O cliente nº 2 obtém acesso de leitura e gravação com seu próprio ID de usuário.

O exemplo a seguir mostra uma política de exportação com um `-rwrule none` parâmetro:

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule none`
- `-anon 70`

O cliente nº 1 tem o endereço IP 10,1.16,207, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com Kerberos v5.

O cliente nº 2 tem o endereço IP 10,1.16,211, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com AUTH_SYS.

O cliente nº 3 tem o endereço IP 10,1.16,234, envia uma solicitação de acesso usando o protocolo NFSv3 e não autenticou (ou seja, o tipo de segurança AUTH_NONE).

O protocolo de acesso do cliente e o endereço IP correspondem aos três clientes. O parâmetro somente leitura permite o acesso somente leitura a clientes com seu próprio ID de usuário autenticado com AUTH_SYS. O parâmetro somente leitura permite o acesso somente leitura como usuário anônimo com ID de usuário 70 para clientes autenticados usando qualquer outro tipo de segurança. O parâmetro read-write permite o acesso de leitura-gravação somente como usuário anônimo.

Portanto, o cliente nº 1 e o cliente nº 3 recebem acesso de leitura e gravação somente como usuário anônimo com ID de usuário 70. O cliente nº 2 obtém acesso somente leitura com seu próprio ID de usuário, mas é negado o acesso de leitura e gravação.

Como os tipos de segurança ONTAP determinam os níveis de acesso do cliente NFS

O tipo de segurança com o qual o cliente autenticou desempenha um papel especial nas regras de exportação. Você deve entender como o tipo de segurança determina os níveis de acesso que o cliente obtém a um volume ou qtree.

Os três níveis de acesso possíveis são os seguintes:

1. Somente leitura
2. Leitura-gravação
3. Superusuário (para clientes com ID de usuário 0)

Como o nível de acesso por tipo de segurança é avaliado nesta ordem, você deve observar as seguintes regras ao construir parâmetros de nível de acesso em regras de exportação:

Para um cliente obter nível de acesso…	Esses parâmetros de acesso devem corresponder ao tipo de segurança do cliente…
Apenas de leitura normal do utilizador	Somente leitura (`-rorule`)
Leitura-escrita normal do utilizador	Somente leitura (`-rorule`) e leitura-gravação (`-rwrule`)
Somente leitura do superusuário	Apenas leitura (`-rorule`) e. `-superuser`
Leitura-gravação do superusuário	Somente leitura (`-rorule`) e leitura-gravação (`-rwrule`) e. `-superuser`

Os seguintes são tipos de segurança válidos para cada um destes três parâmetros de acesso:

- `any`
- `none`
- `never`

  Este tipo de segurança não é válido para utilização com o `-superuser` parâmetro.

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`
- `sys`

Ao combinar o tipo de segurança de um cliente com cada um dos três parâmetros de acesso, há três resultados possíveis:

Se o tipo de segurança do cliente…	Então o cliente…
Corresponde ao especificado no parâmetro Access.	Obtém acesso para esse nível com seu próprio ID de usuário.
Não corresponde ao especificado, mas o parâmetro Access inclui a opção `none`.	Obtém acesso para esse nível, mas como o usuário anônimo com o ID de usuário especificado pelo `-anon` parâmetro.
Não corresponde ao especificado e o parâmetro Access não inclui a opção `none`.	Não obtém acesso para esse nível. Isso não se aplica ao `-superuser` parâmetro porque ele sempre inclui `none` mesmo quando não especificado.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule sys,krb5`
- `-superuser krb5`

O cliente nº 1 tem o endereço IP 10,1.16,207, tem ID de usuário 0, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com Kerberos v5.

O cliente nº 2 tem o endereço IP 10,1.16,211, tem ID de usuário 0, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com AUTH_SYS.

O cliente nº 3 tem o endereço IP 10,1.16,234, tem ID de usuário 0, envia uma solicitação de acesso usando o protocolo NFSv3 e não autenticou (AUTH_NONE).

O protocolo de acesso do cliente e o endereço IP correspondem aos três clientes. O parâmetro somente leitura permite o acesso somente leitura a todos os clientes, independentemente do tipo de segurança. O parâmetro read-write permite o acesso de leitura-gravação a clientes com sua própria ID de usuário autenticado com AUTH_SYS ou Kerberos v5. O parâmetro superuser permite o acesso do superusuário a clientes com ID de usuário 0 autenticado com Kerberos v5.

Portanto, o cliente nº 1 obtém acesso de leitura e gravação do superusuário porque ele corresponde aos três parâmetros de acesso. O cliente nº 2 obtém acesso de leitura e gravação, mas não acesso ao superusuário. O cliente nº 3 obtém acesso somente leitura, mas não acesso ao superusuário.

Saiba mais sobre como gerenciar solicitações de acesso de superusuário do ONTAP NFS

Ao configurar políticas de exportação, você precisa considerar o que deseja acontecer se o sistema de armazenamento receber uma solicitação de acesso de cliente com ID de usuário 0, ou seja, como superusuário, e configurar suas regras de exportação de acordo.

No mundo UNIX, um usuário com o ID de usuário 0 é conhecido como superusuário, normalmente chamado de root, que tem direitos de acesso ilimitados em um sistema. O uso do superusuário Privileges pode ser perigoso por várias razões, incluindo a violação do sistema e da segurança de dados.

Por padrão, o ONTAP mapeia os clientes que apresentam com ID de usuário 0 para o usuário anônimo. No entanto, você pode especificar o `-superuser` parâmetro em regras de exportação para determinar como lidar com clientes que apresentam com ID de usuário 0, dependendo do seu tipo de segurança. A seguir estão as opções válidas para o `-superuser` parâmetro:

- `any`
- `none`

  Esta é a configuração padrão se você não especificar o `-superuser` parâmetro.

- `krb5`
- `ntlm`
- `sys`

Há duas maneiras diferentes de como os clientes que apresentam com ID de usuário 0 são manipulados, dependendo da `-superuser` configuração do parâmetro:

Se o `-superuser` parâmetro e o tipo de segurança do cliente…	**Então o cliente…**
Correspondência	Obtém acesso de superusuário com ID de usuário 0.
Não corresponder	Obtém acesso como usuário anônimo com o ID de usuário especificado pelo `-anon` parâmetro e suas permissões atribuídas. Isso é independentemente de o parâmetro somente leitura ou leitura-gravação especificar a opção `none`.

Se um cliente apresentar com ID de usuário 0 para acessar um volume com estilo de segurança NTFS e o `-superuser` parâmetro estiver definido como `none`, o ONTAP usará o mapeamento de nomes para o usuário anônimo obter as credenciais adequadas.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-anon 127`

O cliente nº 1 tem o endereço IP 10,1.16,207, tem ID de usuário 746, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com Kerberos v5.

O cliente nº 2 tem o endereço IP 10,1.16,211, tem ID de usuário 0, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com AUTH_SYS.

O protocolo de acesso do cliente e o endereço IP correspondem a ambos os clientes. O parâmetro somente leitura permite o acesso somente leitura a todos os clientes, independentemente do tipo de segurança com o qual eles autenticaram. No entanto, somente o cliente nº 1 obtém acesso de leitura e gravação porque usou o tipo de segurança aprovado Kerberos v5 para autenticar.

O cliente nº 2 não obtém acesso ao superusuário. Em vez disso, ele é mapeado para anônimo porque o `-superuser` parâmetro não é especificado. Isto significa que o padrão é `none` e mapeia automaticamente a ID do usuário 0 para anônimo. O cliente nº 2 também só obtém acesso somente leitura porque seu tipo de segurança não corresponde ao parâmetro de leitura-gravação.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`

- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

O cliente nº 1 tem o endereço IP 10,1.16,207, tem ID de usuário 0, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com Kerberos v5.

O cliente nº 2 tem o endereço IP 10,1.16,211, tem ID de usuário 0, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com AUTH_SYS.

O protocolo de acesso do cliente e o endereço IP correspondem a ambos os clientes. O parâmetro somente leitura permite o acesso somente leitura a todos os clientes, independentemente do tipo de segurança com o qual eles autenticaram. No entanto, somente o cliente nº 1 obtém acesso de leitura e gravação porque usou o tipo de segurança aprovado Kerberos v5 para autenticar. O cliente nº 2 não obtém acesso de leitura e gravação.

A regra de exportação permite o acesso do superusuário para clientes com ID de usuário 0. O cliente nº 1 obtém acesso ao superusuário porque corresponde ao ID do usuário e ao tipo de segurança para somente leitura e `-superuser` parâmetros. O cliente nº 2 não obtém acesso de leitura-escrita ou superusuário porque seu tipo de segurança não corresponde ao parâmetro de leitura-gravação ou ao `-superuser` parâmetro. Em vez disso, o cliente nº 2 é mapeado para o usuário anônimo, que neste caso tem o ID de usuário 0.

Saiba mais sobre caches de política de exportação ONTAP NFS

Para melhorar o desempenho do sistema, o ONTAP usa caches locais para armazenar informações como nomes de host e grupos de rede. Isso permite que o ONTAP processe regras de política de exportação mais rapidamente do que recuperar as informações de fontes externas. Entender o que são os caches e o que eles fazem pode ajudá-lo a solucionar problemas de acesso ao cliente.

Você configura políticas de exportação para controlar o acesso do cliente às exportações NFS. Cada política de exportação contém regras e cada regra contém parâmetros que correspondem à regra aos clientes que solicitam acesso. Alguns desses parâmetros exigem que o ONTAP entre em Contato com uma fonte externa, como servidores DNS ou NIS, para resolver objetos como nomes de domínio, nomes de host ou netgroups.

Essas comunicações com fontes externas levam um pouco de tempo. Para aumentar o desempenho, o ONTAP reduz o tempo necessário para resolver objetos de regra de política de exportação armazenando informações localmente em cada nó em vários caches.

Nome do cache	Tipo de informação armazenada
Acesso	Mapeamentos de clientes para políticas de exportação correspondentes
Nome	Mapeamentos de nomes de usuário UNIX para IDs de usuário UNIX correspondentes
ID	Mapeamentos de IDs de usuário UNIX para IDs de usuário UNIX correspondentes e IDs de grupo UNIX estendidos

Nome do cache	Tipo de informação armazenada
Host	Mapeamentos de nomes de host para endereços IP correspondentes
Grupo de rede	Mapeamentos de netgroups para endereços IP correspondentes de membros
Showmount	Lista de diretórios exportados do namespace SVM

Se você alterar as informações nos servidores de nomes externos em seu ambiente depois que o ONTAP as recuperou e armazenou localmente, os caches agora podem conter informações desatualizadas. Embora o ONTAP atualize caches automaticamente após determinados períodos de tempo, os caches diferentes têm tempos e algoritmos diferentes de expiração e atualização.

Outro motivo possível para que os caches contenham informações desatualizadas é quando o ONTAP tenta atualizar informações em cache, mas encontra uma falha ao tentar se comunicar com servidores de nomes. Se isso acontecer, o ONTAP continuará a usar as informações atualmente armazenadas nos caches locais para evitar a interrupção do cliente.

Como resultado, as solicitações de acesso ao cliente que devem ser bem-sucedidas podem falhar e as solicitações de acesso ao cliente que devem falhar podem ser bem-sucedidas. Você pode exibir e lavar manualmente alguns dos caches de política de exportação ao solucionar problemas de acesso ao cliente.

Saiba mais sobre caches de acesso ONTAP NFS

O ONTAP usa um cache de acesso para armazenar os resultados da avaliação de regras de política de exportação para operações de acesso do cliente para um volume ou qtree. Isso resulta em melhorias de desempenho porque as informações podem ser recuperadas muito mais rapidamente do cache de acesso do que passar pelo processo de avaliação de regras de política de exportação sempre que um cliente envia uma solicitação de e/S.

Sempre que um cliente NFS enviar uma solicitação de e/S para acessar dados em um volume ou qtree, o ONTAP deve avaliar cada solicitação de e/S para determinar se deve conceder ou negar a solicitação de e/S. Essa avaliação envolve verificar todas as regras de política de exportação da política de exportação associada ao volume ou qtree. Se o caminho para o volume ou qtree envolver cruzar um ou mais pontos de junção, isso pode exigir a realização desta verificação para várias políticas de exportação ao longo do caminho.

Observe que essa avaliação ocorre para cada solicitação de e/S enviada de um cliente NFS, como leitura, gravação, lista, cópia e outras operações, não apenas para solicitações de montagem inicial.

Depois que o ONTAP identificou as regras de política de exportação aplicáveis e decidiu se deseja permitir ou negar a solicitação, o ONTAP cria uma entrada no cache de acesso para armazenar essas informações.

Quando um cliente NFS envia uma solicitação de e/S, o ONTAP observa o endereço IP do cliente, a ID do SVM e a política de exportação associada ao volume ou qtree de destino e verifica primeiro a entrada correspondente no cache de acesso. Se existir uma entrada correspondente no cache de acesso, o ONTAP usará as informações armazenadas para permitir ou negar a solicitação de e/S. Se uma entrada correspondente não existir, o ONTAP passa pelo processo normal de avaliação de todas as regras de política aplicáveis, conforme explicado acima.

As entradas de cache de acesso que não são usadas ativamente não são atualizadas. Isso reduz a comunicação desnecessária e desperdiçada com o nome externo serve.

Recuperar as informações do cache de acesso é muito mais rápido do que passar por todo o processo de avaliação de regras de política de exportação para cada solicitação de e/S. Portanto, o uso do cache de acesso melhora significativamente o desempenho reduzindo a sobrecarga das verificações de acesso do cliente.

Saiba mais sobre os parâmetros de cache de acesso NFS do ONTAP

Vários parâmetros controlam os períodos de atualização para entradas no cache de acesso. Entender como esses parâmetros funcionam permite modificá-los para ajustar o cache de acesso e equilibrar o desempenho com o quão recente é a informação armazenada.

O cache de acesso armazena entradas que consistem em uma ou mais regras de exportação que se aplicam a clientes que tentam acessar volumes ou qtrees. Essas entradas são armazenadas por um determinado período de tempo antes de serem atualizadas. O tempo de atualização é determinado pelos parâmetros de cache de acesso e depende do tipo de entrada de cache de acesso.

Você pode especificar parâmetros de cache de acesso para SVMs individuais. Isso permite que os parâmetros sejam diferentes de acordo com os requisitos de acesso à SVM. As entradas de cache de acesso que não são usadas ativamente não são atualizadas, o que reduz a comunicação desnecessária e desperdiçada com servidores de nomes externos.

Acesse o tipo de entrada de cache	Descrição	Período de atualização em segundos
Entradas positivas	Acesse entradas de cache que não resultaram na negação de acesso aos clientes.	Mínimo: 300 Máximo: 86.400 Padrão: 3.600
Entradas negativas	Acesse entradas de cache que resultaram na negação de acesso aos clientes.	Mínimo: 60 Máximo: 86.400 Padrão: 3.600

Exemplo

Um cliente NFS tenta acessar um volume em um cluster. O ONTAP corresponde o cliente a uma regra de política de exportação e determina que o cliente obtém acesso com base na configuração da regra de política de exportação. O ONTAP armazena a regra de política de exportação no cache de acesso como uma entrada positiva. Por padrão, o ONTAP mantém a entrada positiva no cache de acesso por uma hora (3.600 segundos) e, em seguida, atualiza automaticamente a entrada para manter as informações atualizadas.

Para evitar que o cache de acesso seja preenchido desnecessariamente, há um parâmetro adicional para limpar entradas de cache de acesso existentes que não foram usadas por um determinado período de tempo para decidir o acesso do cliente. `-harvest-timeout`Este parâmetro tem um intervalo permitido de 60 a 2.592.000 segundos e uma predefinição de 86.400 segundos.

Remover políticas de exportação das qtrees do ONTAP NFS

Se você decidir que não deseja que uma política de exportação específica seja atribuída a uma qtree por mais tempo, poderá remover a política de exportação modificando a qtree para herdar a política de exportação do volume que contém. Você pode fazer isso usando o `volume qtree modify` comando com o `-export-policy` parâmetro e uma string de nome vazia ("").

Passos

1. Para remover uma política de exportação de uma qtree, digite o seguinte comando:

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy ""
   ```

2. Verifique se a qtree foi modificada em conformidade:

   ```
   volume qtree show -qtree qtree_name -fields export-policy
   ```

Validar IDs de qtree ONTAP NFS para operações de arquivo qtree

O ONTAP pode executar uma validação adicional opcional de IDs de qtree. Essa validação garante que as solicitações de operação de arquivo cliente usem um ID de qtree válido e que os clientes só possam mover arquivos dentro da mesma qtree. Pode ativar ou desativar esta validação modificando o `-validate-qtree-export` parâmetro. Este parâmetro está ativado por predefinição.

Sobre esta tarefa

Esse parâmetro só é efetivo quando você atribuiu uma política de exportação diretamente a um ou mais qtrees na máquina virtual de armazenamento (SVM).

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute uma das seguintes ações:

Se pretender que a validação da ID de qtree seja…	Digite o seguinte comando…
Ativado	`vserver nfs modify -vserver vserver_name -validate-qtree-export enabled`
Desativado	`vserver nfs modify -vserver vserver_name -validate-qtree-export disabled`

3. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Restrições de política de exportação e junções aninhadas para volumes ONTAP NFS FlexVol

Se você configurou políticas de exportação para definir uma política menos restritiva em uma junção aninhada, mas uma política mais restritiva em uma junção de nível mais alto, o acesso à junção de nível inferior pode falhar.

Você deve garantir que as junções de nível mais alto tenham políticas de exportação menos restritivas do que as junções de nível mais baixo.

Usando Kerberos com NFS para segurança forte

Suporte ONTAP NFS para Kerberos

O Kerberos fornece autenticação segura forte para aplicativos cliente/servidor. A autenticação fornece a verificação de identidades de usuário e processo para um servidor. No ambiente ONTAP, o Kerberos fornece autenticação entre máquinas virtuais de armazenamento (SVMs) e clientes NFS.

No ONTAP 9, a seguinte funcionalidade Kerberos é suportada:

- Autenticação Kerberos 5 com verificação de integridade (krb5i)

  O Krb5i usa checksums para verificar a integridade de cada mensagem NFS transferida entre cliente e servidor. Isso é útil tanto por motivos de segurança (por exemplo, para garantir que os dados não foram adulterados) quanto por motivos de integridade de dados (por exemplo, para evitar a corrupção de dados ao usar NFS em redes não confiáveis).

- Autenticação Kerberos 5 com verificação de privacidade (krb5p)

  Krb5p usa checksums para criptografar todo o tráfego entre o cliente e o servidor. Isto é mais seguro e também incorre mais carga.

- Criptografia AES de 128 bits e 256 bits

  O Advanced Encryption Standard (AES) é um algoritmo de encriptação para proteger dados eletrónicos. O ONTAP suporta AES com chaves de 128 bits (AES-128) e AES com criptografia de chaves de 256 bits (AES-256) para Kerberos para maior segurança.

- Configurações de realm Kerberos no nível da SVM

  Os administradores do SVM agora podem criar configurações do Kerberos Realm no nível SVM. Isso significa que os administradores do SVM não precisam mais confiar no administrador do cluster para a configuração do Kerberos Realm e podem criar configurações individuais do Kerberos Realm em um ambiente de alocação a vários clientes.

Requisitos para configurar o Kerberos com ONTAP NFS

Antes de configurar o Kerberos com NFS no sistema, você deve verificar se determinados itens no ambiente de rede e armazenamento estão configurados

corretamente.

> As etapas para configurar seu ambiente dependem de qual versão e tipo de sistema operacional cliente, controlador de domínio, Kerberos, DNS, etc. que você está usando. Documentar todas essas variáveis está além do escopo deste documento. Para obter mais informações, consulte a respetiva documentação para cada componente.
>
> Para um exemplo detalhado de como configurar o ONTAP e o Kerberos 5 com NFSv3 e NFSv4 em um ambiente usando o ative Directory do Windows Server 2008 R2 e hosts Linux, consulte o relatório técnico 4073.

Os seguintes itens devem ser configurados primeiro:

Requisitos de ambiente de rede

- Kerberos

  Você deve ter uma configuração Kerberos funcionando com um centro de distribuição de chaves (KDC), como Kerberos baseados no ative Directory do Windows ou MIT Kerberos.

  Os servidores NFS devem usar `nfs` como o componente principal de sua máquina principal.

- Serviço de diretório

  Você deve usar um serviço de diretório seguro em seu ambiente, como ative Directory ou OpenLDAP, que esteja configurado para usar LDAP em SSL/TLS.

- NTP

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

- Resolução de nome de domínio (DNS)

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

- Contas de utilizador

  Cada cliente deve ter uma conta de usuário no Reino Kerberos. Os servidores NFS devem usar "nfs" como o componente principal de sua máquina principal.

Requisitos do cliente NFS

- NFS

  Cada cliente deve ser configurado corretamente para se comunicar através da rede usando NFSv3 ou NFSv4.

  Os clientes devem suportar RFC1964 e RFC2203.

- Kerberos

  Cada cliente deve ser configurado corretamente para usar a autenticação Kerberos, incluindo os seguintes

detalhes:

  - A encriptação para comunicação TGS está ativada.

    AES-256 para maior segurança.

  - O tipo de encriptação mais seguro para comunicação TGT está ativado.
  - O domínio e o domínio Kerberos estão configurados corretamente.
  - O GSS está ativado.

    Ao usar credenciais de máquina:

  - Não execute `gssd` com o `-n` parâmetro.
  - Não execute `kinit` como usuário raiz.

- Cada cliente deve usar a versão mais recente e atualizada do sistema operacional.

  Isso fornece a melhor compatibilidade e confiabilidade para criptografia AES com Kerberos.

- DNS

  Cada cliente deve ser configurado corretamente para usar o DNS para a resolução correta do nome.

- NTP

  Cada cliente deve estar sincronizando com o servidor NTP.

- Informações de host e domínio

  Cada cliente `/etc/hosts` e `/etc/resolv.conf` arquivos devem conter o nome de host correto e as informações de DNS, respetivamente.

- Ficheiros keytab

  Cada cliente deve ter um arquivo keytab do KDC. O Reino deve estar em letras maiúsculas. O tipo de criptografia deve ser AES-256 para maior segurança.

- Opcional: Para obter o melhor desempenho, os clientes se beneficiam de ter pelo menos duas interfaces de rede: Uma para comunicação com a rede local e outra para comunicação com a rede de armazenamento.

Requisitos do sistema de storage

- Licença NFS

  O sistema de storage deve ter uma licença NFS válida instalada.

- Licença CIFS

  A licença CIFS é opcional. Só é necessário para verificar credenciais do Windows ao usar mapeamento de nomes multiprotocolo. Não é necessário em um ambiente restrito somente para UNIX.

- SVM

  Você precisa ter pelo menos um SVM configurado no sistema.

- DNS na SVM

  Você deve ter DNS configurado em cada SVM.

- Servidor NFS

  Você precisa ter o NFS configurado na SVM.

- Criptografia AES

  Para uma segurança mais forte, você deve configurar o servidor NFS para permitir apenas criptografia AES-256 para Kerberos.

- Servidor SMB

  Se você estiver executando um ambiente multiprotocolo, deverá ter o SMB configurado na SVM. O servidor SMB é necessário para o mapeamento de nomes multiprotocolo.

- Volumes

  Você precisa ter um volume raiz e pelo menos um volume de dados configurados para uso pelo SVM.

- Volume raiz

  O volume raiz do SVM precisa ter a seguinte configuração:

Nome	Definição
Estilo de segurança	UNIX
UID	Raiz ou ID 0
GID	Raiz ou ID 0
Permissões da UNIX	777

  Em contraste com o volume raiz, os volumes de dados podem ter um estilo de segurança.

- Grupos UNIX

  O SVM deve ter os seguintes grupos UNIX configurados:

Nome do grupo	ID do grupo
daemon	1
raiz	0
pcuser	65534 (criado automaticamente pelo ONTAP ao criar o SVM)

- Utilizadores UNIX

  O SVM deve ter os seguintes usuários UNIX configurados:

Nome de utilizador	ID de utilizador	ID do grupo principal	Comentário
nfs	500	0	Necessário para a fase INIT do GSS O primeiro componente do usuário cliente NFS SPN é usado como usuário.
pcuser	65534	65534	Necessário para uso multiprotocolo NFS e CIFS Criado e adicionado ao grupo pcuser automaticamente pelo ONTAP ao criar o SVM.
raiz	0	0	Necessário para a montagem

  O usuário nfs não é necessário se existir um mapeamento de nomes Kerberos-UNIX para o SPN do usuário cliente NFS.

- Políticas e regras de exportação

  Você deve ter configurado políticas de exportação com as regras de exportação necessárias para os volumes raiz e de dados e qtrees. Se todos os volumes da SVM forem acessados por Kerberos, você poderá definir as opções de regra de exportação `-rorule` , `-rwrule` e `-superuser` para o volume raiz como `krb5` , `krb5i` ou `krb5p`.

- Mapeamento de nomes Kerberos-UNIX

  Se você quiser que o usuário identificado pelo usuário cliente NFS SPN tenha permissões de raiz, você deve criar um mapeamento de nome para root.

Informações relacionadas

"Relatório técnico da NetApp 4073: Autenticação unificada segura"

"Ferramenta de Matriz de interoperabilidade do NetApp"

"Administração do sistema"

"Gerenciamento de storage lógico"

Especifique o domínio de ID do usuário ONTAP para NFSv4

Para especificar o domínio de ID de usuário, você pode definir a `-v4-id-domain` opção.

Sobre esta tarefa

Por padrão, o ONTAP usa o domínio NIS para o mapeamento de ID de usuário NFSv4, se um estiver definido. Se um domínio NIS não estiver definido, o domínio DNS será usado. Talvez seja necessário definir o domínio de ID de usuário se, por exemplo, você tiver vários domínios de ID de usuário. O nome de domínio deve corresponder à configuração de domínio no controlador de domínio. Não é necessário para NFSv3.

Passo

1. Introduza o seguinte comando:

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

Configurar serviços de nomes

Saiba mais sobre a configuração do switch do serviço de nomes NFS do ONTAP

O ONTAP armazena informações de configuração do serviço de nomes em uma tabela equivalente `/etc/nsswitch.conf` ao arquivo em sistemas UNIX. Você deve entender a função da tabela e como o ONTAP a usa para que você possa configurá-la adequadamente para o seu ambiente.

A tabela de switch de serviço de nome do ONTAP determina quais fontes de serviço de nome o ONTAP consulta para obter informações para um determinado tipo de informações de serviço de nome. O ONTAP mantém uma tabela de switch de serviço de nomes separada para cada SVM.

Tipos de banco de dados

A tabela armazena uma lista de serviços de nomes separada para cada um dos seguintes tipos de banco de dados:

Tipo de banco de dados	Define fontes de serviço de nome para…	Fontes válidas são…
hosts	Conversão de nomes de host para endereços IP	ficheiros, dns
grupo	Procurar informações do grupo de utilizadores	arquivos, nis, ldap
passwd	Procurar informações do utilizador	arquivos, nis, ldap
grupo de rede	Procurar informações do netgroup	arquivos, nis, ldap
namemap	Mapeando nomes de usuários	ficheiros, ldap

Tipos de origem

As fontes especificam qual fonte de serviço de nomes usar para recuperar as informações apropriadas.

Especificar tipo de origem…	Para procurar informações em…	Gerenciado pelas famílias de comando…

ficheiros	Arquivos de origem local	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	Servidores NIS externos, conforme especificado na configuração do domínio NIS da SVM	`vserver services name-service nis-domain`
ldap	Servidores LDAP externos, conforme especificado na configuração de cliente LDAP do SVM	`vserver services name-service ldap`
dns	Servidores DNS externos conforme especificado na configuração DNS do SVM	`vserver services name-service dns`

Mesmo que você Planeje usar NIS ou LDAP para acesso a dados e autenticação de administração SVM, você ainda deve incluir `files` e configurar usuários locais como um fallback caso a autenticação NIS ou LDAP falhe.

Protocolos usados para acessar fontes externas

Para acessar os servidores para fontes externas, o ONTAP usa os seguintes protocolos:

Fonte do serviço de nomes externo	Protocolo utilizado para acesso
NIS	UDP
DNS	UDP
LDAP	TCP

Exemplo

O exemplo a seguir exibe a configuração do switch do serviço de nomes para o SVM_1:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                Source
Vserver         Database        Order
--------------- ------------    ---------
svm_1           hosts           files,
                                dns
svm_1           group           files
svm_1           passwd          files
svm_1           netgroup        nis,
                                files
```

Para procurar endereços IP para hosts, o ONTAP primeiro consulta os arquivos de origem locais. Se a consulta não retornar nenhum resultado, os servidores DNS serão verificados em seguida.

Para procurar informações de usuários ou grupos, o ONTAP consulta apenas arquivos de fontes locais. Se a consulta não retornar nenhum resultado, a pesquisa falhará.

Para procurar informações de netgroup, o ONTAP primeiro consulta servidores NIS externos. Se a consulta não retornar nenhum resultado, o arquivo netgroup local será marcado em seguida.

Não há entradas de serviço de nomes para o mapeamento de nomes na tabela para o SVM.svm_1. Portanto, o ONTAP consulta apenas arquivos de origem local por padrão.

Informações relacionadas

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

Utilize LDAP

Saiba mais sobre LDAP para SVMs ONTAP NFS

Um servidor LDAP (Lightweight Directory Access Protocol) permite manter centralmente as informações do usuário. Se você armazenar seu banco de dados de usuários em um servidor LDAP em seu ambiente, poderá configurar seu sistema de storage para procurar informações de usuário em seu banco de dados LDAP existente.

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

    As seguintes opções de segurança de sessão estão disponíveis:

        - Assinatura LDAP (fornece verificação de integridade de dados) e assinatura e vedação LDAP (fornece verificação e criptografia de integridade de dados)
        - INICIE O TLS
        - LDAPS (LDAP sobre TLS ou SSL)
    - Para ativar consultas LDAP assinadas e seladas, os seguintes serviços devem ser configurados:
        - Os servidores LDAP devem suportar o mecanismo SASL GSSAPI (Kerberos).
        - Os servidores LDAP devem ter Registros DNS A/AAAA, bem como Registros PTR configurados no servidor DNS.
        - Os servidores Kerberos devem ter Registros SRV presentes no servidor DNS.
    - Para ativar o TLS ou LDAPS, os seguintes pontos devem ser considerados.
        - É uma prática recomendada do NetApp usar Iniciar TLS em vez de LDAPS.
        - Se o LDAPS for usado, o servidor LDAP deverá ser habilitado para TLS ou SSL no ONTAP 9.5 e posteriores. SSL não é suportado no ONTAP 9.4 - 9.0.
        - Um servidor de certificados já deve estar configurado no domínio.
    - Para ativar a perseguição de referência LDAP (no ONTAP 9.5 e posterior), as seguintes condições devem ser satisfeitas:
        - Ambos os domínios devem ser configurados com uma das seguintes relações de confiança:
            - Bidirecional
            - One-way, onde o primário confia no domínio de referência
            - Pai-filho
        - O DNS deve ser configurado para resolver todos os nomes de servidor referidos.
        - As senhas de domínio devem ser iguais para autenticar quando `--bind-as-cifs-server` definidas como verdadeiro.

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

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

- Começando com ONTAP 9.11,1, você pode usar "Use a vinculação rápida LDAP para autenticação nsswitch para SVMs ONTAP NFS."
- Você deve inserir um esquema LDAP ao configurar o cliente LDAP no SVM.

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

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

Para obter informações adicionais, "Relatório técnico do NetApp 4835: Como configurar o LDAP no ONTAP"consulte .

Saiba mais sobre assinatura e selagem LDAP para SVMs ONTAP NFS

A partir do ONTAP 9, você pode configurar a assinatura e a vedação para habilitar a segurança da sessão LDAP em consultas para um servidor AD (ative Directory). Você deve configurar as configurações de segurança do servidor NFS na máquina virtual de armazenamento (SVM) para corresponder às do servidor LDAP.

A assinatura confirma a integridade dos dados de carga útil LDAP usando tecnologia de chave secreta. A vedação criptografa os dados de carga útil LDAP para evitar a transmissão de informações confidenciais em texto não criptografado. Uma opção *LDAP Security Level* indica se o tráfego LDAP precisa ser assinado, assinado e selado, ou não. A predefinição é `none`. teste

A assinatura LDAP e a vedação no tráfego SMB são ativadas no SVM com a `-session-security-for-ad-ldap` opção de `vserver cifs security modify` comando.

Saiba mais sobre LDAPS para SVMs ONTAP NFS

Você deve entender certos termos e conceitos sobre como o ONTAP protege a comunicação LDAP. O ONTAP pode usar TLS ou LDAPS para configurar sessões autenticadas entre servidores LDAP integrados ao ative Directory ou servidores LDAP baseados em UNIX.

Terminologia

Existem certos termos que você deve entender sobre como o ONTAP usa o LDAPS para proteger a comunicação LDAP.

- **LDAP**

  (Lightweight Directory Access Protocol) Um protocolo para acessar e gerenciar diretórios de informações. O LDAP é usado como um diretório de informações para armazenar objetos como usuários, grupos e grupos de rede. O LDAP também fornece serviços de diretório que gerenciam esses objetos e atendem solicitações LDAP de clientes LDAP.

- **SSL**

  (Secure Sockets Layer) Um protocolo desenvolvido para enviar informações de forma segura pela Internet. O SSL é suportado pelo ONTAP 9 e posterior, mas foi obsoleto em favor do TLS.

- **TLS**

  (Transport Layer Security) um protocolo de rastreamento de padrões IETF que é baseado nas especificações SSL anteriores. É o sucessor do SSL. O TLS é compatível com o ONTAP 9.5 e posterior.

- **LDAPS (LDAP sobre SSL ou TLS)**

  Um protocolo que usa TLS ou SSL para proteger a comunicação entre clientes LDAP e servidores LDAP. Os termos *LDAP sobre SSL* e *LDAP sobre TLS* às vezes são usados de forma intercambiável. O LDAPS é suportado pelo ONTAP 9.5 e posterior.

- No ONTAP 9.8-9.5, o LDAPS só pode ser habilitado na porta 636. Para fazer isso, use o `-use-ldaps-for-ad-ldap` parâmetro com o `vserver cifs security modify` comando.
- A partir do ONTAP 9.9,1, o LDAPS pode ser ativado em qualquer porta, embora a porta 636 permaneça a predefinição. Para fazer isso, defina o `-ldaps-enabled` parâmetro `true` e especifique o parâmetro desejado `-port`. Saiba mais sobre `vserver services name-service ldap client create` o "Referência do comando ONTAP"na .

É uma prática recomendada do NetApp usar Iniciar TLS em vez de LDAPS.

- * Iniciar TLS*

  (Também conhecido como *start_tls*, *STARTTLS* e *STARTTLS*) Um mecanismo para fornecer comunicação segura usando os protocolos TLS.

  O ONTAP usa o STARTTLS para proteger a comunicação LDAP e usa a porta LDAP padrão (389) para se comunicar com o servidor LDAP. O servidor LDAP deve ser configurado para permitir conexões pela porta LDAP 389; caso contrário, as conexões LDAP TLS do SVM ao servidor LDAP falharão.

Como o ONTAP usa o LDAPS

O ONTAP oferece suporte à autenticação de servidor TLS, o que permite que o cliente LDAP SVM confirme a identidade do servidor LDAP durante a operação de vinculação. Os clientes LDAP habilitados para TLS podem usar técnicas padrão de criptografia de chave pública para verificar se o certificado e a ID pública de um servidor são válidos e foram emitidos por uma autoridade de certificação (CA) listada na lista de CAs confiáveis do cliente.

O LDAP suporta STARTTLS para criptografar comunicações usando TLS. O STARTTLS começa como uma conexão de texto simples sobre a porta LDAP padrão (389), e essa conexão é então atualizada para TLS.

O ONTAP oferece suporte ao seguinte:

- LDAPS para tráfego relacionado a SMB entre os servidores LDAP integrados ao ative Directory e o SVM
- LDAPS para tráfego LDAP para mapeamento de nomes e outras informações do UNIX

  Servidores LDAP integrados ao ative Directory ou servidores LDAP baseados em UNIX podem ser usados para armazenar informações para mapeamento de nomes LDAP e outras informações do UNIX, como usuários, grupos e netgroups.

- Certificados CA raiz autoassinados

  Ao usar um LDAP integrado do ative-Directory, o certificado raiz autoassinado é gerado quando o Serviço de certificados do Windows Server é instalado no domínio. Ao usar um servidor LDAP baseado em UNIX para mapeamento de nomes LDAP, o certificado raiz autoassinado é gerado e salvo usando meios apropriados para esse aplicativo LDAP.

Por predefinição, o LDAPS está desativado.

Habilitar suporte LDAP RFC2307bis para SVMs ONTAP NFS

Se você quiser usar o LDAP e exigir a capacidade adicional de usar associações a grupos aninhados, você pode configurar o ONTAP para habilitar o suporte ao LDAP RFC2307bis.

Antes de começar

Você deve ter criado uma cópia de um dos esquemas de cliente LDAP padrão que você deseja usar.

Sobre esta tarefa

Em esquemas de cliente LDAP, os objetos de grupo usam o atributo memberUid. Esse atributo pode conter vários valores e lista os nomes dos usuários que pertencem a esse grupo. Em esquemas de cliente LDAP habilitados para RFC2307bis, os objetos de grupo usam o atributo uniqueMember. Este atributo pode conter o nome distinto completo (DN) de outro objeto no diretório LDAP. Isso permite que você use grupos aninhados porque os grupos podem ter outros grupos como membros.

O usuário não deve ser membro de mais de 256 grupos, incluindo grupos aninhados. O ONTAP ignora quaisquer grupos acima do limite de 256 grupos.

Por padrão, o suporte a RFC2307bis está desativado.

> O suporte a RFC2307bis é ativado automaticamente no ONTAP quando um cliente LDAP é criado com o esquema MS-AD-BIS.

Para obter informações adicionais, "Relatório técnico do NetApp 4835: Como configurar o LDAP no ONTAP"consulte .

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Modifique o esquema de cliente LDAP RFC2307 copiado para ativar o suporte RFC2307bis:

   ```
   vserver services name-service ldap client schema modify -vserver vserver_name
   -schema schema-name -enable-rfc2307bis true
   ```

3. Modifique o esquema para corresponder à classe de objeto suportada no servidor LDAP:

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -group-of-unique-names-object-class object_class
   ```

4. Modifique o esquema para corresponder ao nome de atributo suportado no servidor LDAP:

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -unique-member-attribute attribute_name
   ```

5. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Opções de configuração do ONTAP NFS para pesquisas de diretório LDAP

Você pode otimizar as pesquisas de diretório LDAP, incluindo informações de usuário, grupo e netgroup, configurando o cliente LDAP do ONTAP para se conetar a servidores LDAP da maneira mais apropriada para o seu ambiente. Você precisa entender quando os valores padrão de pesquisa base LDAP e escopo são suficientes e quais parâmetros especificar quando os valores personalizados são mais apropriados.

As opções de pesquisa de cliente LDAP para informações de usuário, grupo e netgroup podem ajudar a evitar consultas LDAP com falha e, portanto, falha no acesso de cliente aos sistemas de armazenamento. Eles também ajudam a garantir que as pesquisas sejam o mais eficientes possível para evitar problemas de desempenho do cliente.

Valores de pesquisa padrão base e escopo

A base LDAP é o DN base padrão que o cliente LDAP usa para executar consultas LDAP. Todas as pesquisas, incluindo pesquisas de usuário, grupo e netgroup, são feitas usando o DN base. Essa opção é apropriada quando o diretório LDAP é relativamente pequeno e todas as entradas relevantes estão localizadas no mesmo DN.

Se você não especificar um DN base personalizado, o padrão será `root`. Isso significa que cada consulta pesquisa o diretório inteiro. Embora isso maximize as chances de sucesso da consulta LDAP, ela pode ser ineficiente e resultar em desempenho significativamente menor com grandes diretórios LDAP.

O escopo base LDAP é o escopo de pesquisa padrão que o cliente LDAP usa para executar consultas LDAP. Todas as pesquisas, incluindo pesquisas de usuário, grupo e netgroup, são feitas usando o escopo base. Ele determina se a consulta LDAP pesquisa somente a entrada nomeada, as entradas um nível abaixo do DN ou toda a subárvore abaixo do DN.

Se você não especificar um escopo base personalizado, o padrão será `subtree`. Isso significa que cada consulta pesquisa a subárvore inteira abaixo do DN. Embora isso maximize as chances de sucesso da consulta LDAP, ela pode ser ineficiente e resultar em desempenho significativamente menor com grandes diretórios LDAP.

Valores de pesquisa de base e escopo personalizados

Opcionalmente, você pode especificar valores de base e escopo separados para pesquisas de usuário, grupo e netgroup. Limitar a base de pesquisa e o escopo das consultas dessa forma pode melhorar significativamente o desempenho, pois limita a pesquisa a uma subseção menor do diretório LDAP.

Se você especificar valores de base e escopo personalizados, eles substituirão a base de pesquisa padrão geral e o escopo para pesquisas de usuário, grupo e netgroup. Os parâmetros para especificar valores de base e escopo personalizados estão disponíveis no nível de privilégio avançado.

Parâmetro cliente LDAP…	Especifica personalizado…
`-base-dn`	DN base para todas as pesquisas LDAP. Vários valores podem ser inseridos, se necessário (por exemplo, se a busca por referências LDAP estiver habilitada no ONTAP 9.5 e versões posteriores).
`-base-scope`	Escopo base para todas as pesquisas LDAP.
`-user-dn`	DNs base para todas as pesquisas de usuários LDAP. Este parâmetro também se aplica a pesquisas de mapeamento de nomes de usuários.
`-user-scope`	Escopo base para todas as pesquisas de usuários LDAP. Este parâmetro também se aplica a pesquisas de mapeamento de nomes de usuários.
`-group-dn`	DNs base para todas as pesquisas de grupos LDAP.

`-group-scope`	Escopo base para todas as pesquisas de grupo LDAP.
`-netgroup-dn`	DNs base para todas as pesquisas de grupos de rede LDAP.
`-netgroup-scope`	Escopo base para todas as pesquisas de netgroup LDAP.

Vários valores DN base personalizados

Se a estrutura de diretórios LDAP for mais complexa, poderá ser necessário especificar vários DNS base para procurar determinadas informações em várias partes do diretório LDAP. Você pode especificar vários DNS para os parâmetros DN de usuário, grupo e netgroup separando-os com um ponto e vírgula (;) e anexando toda a lista de pesquisa DN com aspas duplas ("). Se um DN contiver um ponto-e-vírgula, você deve adicionar um caractere de escape imediatamente antes do ponto-e-vírgula no DN.

Observe que o escopo se aplica a toda a lista de DNS especificada para o parâmetro correspondente. Por exemplo, se você especificar uma lista de três DNS de usuário e subárvore diferentes para o escopo do usuário, o usuário LDAP pesquisará toda a subárvore para cada um dos três DNS especificados.

A partir do ONTAP 9.5, você também pode especificar LDAP *referral chasing*, o que permite que o cliente LDAP ONTAP consulte solicitações de pesquisa para outros servidores LDAP se uma resposta de referência LDAP não for retornada pelo servidor LDAP primário. O cliente usa esses dados de referência para recuperar o objeto de destino do servidor descrito nos dados de referência. Para procurar objetos presentes nos servidores LDAP referidos, o base-DN dos objetos referidos pode ser adicionado ao base-DN como parte da configuração do cliente LDAP. No entanto, os objetos referidos só são procurados quando a busca por referência está ativada (usando a `-referral-enabled true` opção) durante a criação ou modificação do cliente LDAP.

Filtros de pesquisa LDAP personalizados

Você pode usar o parâmetro opção de configuração LDAP para criar um filtro de pesquisa personalizado. O `-group-membership-filter` parâmetro especifica o filtro de pesquisa a ser usado ao procurar associação de grupo a partir de um servidor LDAP.

Um exemplo de filtros válidos são:

```
(cn=*99), (cn=1*), (|(cn=*22)(cn=*33))
```

Saiba mais "Como configurar o LDAP no ONTAP"sobre o .

Melhorar o desempenho das pesquisas de grupo de rede por host do diretório LDAP para SVMs ONTAP NFS

Se o seu ambiente LDAP estiver configurado para permitir pesquisas netgroup-by-host, você poderá configurar o ONTAP para aproveitar isso e realizar pesquisas netgroup-by-host. Isso pode acelerar significativamente as pesquisas do netgroup e reduzir possíveis problemas de acesso ao cliente NFS devido à latência durante as pesquisas do netgroup.

Antes de começar

Seu diretório LDAP deve conter um `netgroup.byhost` mapa.

Seus servidores DNS devem conter Registros de pesquisa direta (A) e reversa (PTR) para clientes NFS.

Quando você especifica endereços IPv6 em netgroups, você deve sempre encurtar e compactar cada endereço conforme especificado no RFC 5952.

Sobre esta tarefa

Os servidores NIS armazenam informações do netgroup em três mapas separados chamados `netgroup` `netgroup.byuser` , e `netgroup.byhost`. O objetivo dos `netgroup.byuser` mapas e `netgroup.byhost` é acelerar as pesquisas de netgroup. O ONTAP pode realizar pesquisas netgroup-by-host em servidores NIS para melhorar os tempos de resposta de montagem.

Por padrão, os diretórios LDAP não têm um `netgroup.byhost` mapa como os servidores NIS. No entanto, é possível, com a ajuda de ferramentas de terceiros, importar um mapa NIS `netgroup.byhost` para diretórios LDAP para permitir pesquisas rápidas netgroup-by-host. Se você tiver configurado seu ambiente LDAP para permitir pesquisas netgroup-by-host, poderá configurar o cliente LDAP do ONTAP com o `netgroup.byhost` nome do mapa, DN e o escopo de pesquisa para pesquisas mais rápidas netgroup-by-host.

Receber os resultados das pesquisas netgroup-by-host com mais rapidez permite que o ONTAP processe regras de exportação com mais rapidez quando os clientes NFS solicitam acesso às exportações. Isso reduz a chance de atraso no acesso devido a problemas de latência de pesquisa do netgroup.

Passos

1. Obtenha o nome distinto completo exato do mapa NIS `netgroup.byhost` importado para o diretório LDAP.

   O DN do mapa pode variar dependendo da ferramenta de terceiros usada para importação. Para obter o melhor desempenho, você deve especificar o DN exato do mapa.

2. Defina o nível de privilégio como avançado: `set -privilege advanced`
3. Ative as pesquisas netgroup-by-host na configuração de cliente LDAP da máquina virtual de armazenamento (SVM): `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost-dn netgroup-by-host_map_distinguished_name -netgroup-byhost -scope netgroup-by-host_search_scope`

   `-is-netgroup-byhost-enabled {true false`Ativar ou desativar a pesquisa netgroup-by-host para diretórios LDAP. A predefinição é `false.

   `-netgroup-byhost-dn netgroup-by-host_map_distinguished_name` Especifica o nome distinto do `netgroup.byhost` mapa no diretório LDAP. Ele substitui o DN base para pesquisas netgroup-by-host. Se você não especificar esse parâmetro, o ONTAP usará o DN base.

   `-netgroup-byhost-scope {base|onelevel subtree`especifica o escopo de pesquisa para pesquisas netgroup-by-host. Se não especificar este parâmetro, a predefinição é `subtree.

   Se a configuração do cliente LDAP ainda não existir, você pode habilitar pesquisas netgroup-by-host especificando esses parâmetros ao criar uma nova configuração de cliente LDAP usando o `vserver services name-service ldap client create` comando.

O `-ldap-servers` campo substitui o `-servers` campo. Você pode usar o `-ldap -servers` campo para especificar um nome de host ou um endereço IP para o servidor LDAP.

4. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exemplo

O comando a seguir modifica a configuração de cliente LDAP existente chamada "ldap_corp" para habilitar pesquisas netgroup-by-host usando o mapa chamado netgroup `netgroup.byhost`.byhost", dc `subtree`

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

Depois de terminar

Os `netgroup.byhost` mapas e `netgroup` no diretório devem ser mantidos sempre sincronizados para evitar problemas de acesso do cliente.

Informações relacionadas

"IETF RFC 5952: Uma recomendação para representação de texto de endereço IPv6"

Use a vinculação rápida LDAP para autenticação nsswitch para SVMs ONTAP NFS

A partir do ONTAP 9.11,1, você pode aproveitar a funcionalidade LDAP *fast bind* (também conhecida como *concurrent bind*) para solicitações de autenticação de cliente mais rápidas e simples. Para utilizar esta funcionalidade, o servidor LDAP tem de suportar a funcionalidade de ligação rápida.

Sobre esta tarefa

Sem vinculação rápida, o ONTAP usa o LDAP Simple BIND para autenticar usuários administrativos com o servidor LDAP. Com esse método de autenticação, o ONTAP envia um nome de usuário ou grupo para o servidor LDAP, recebe a senha de hash armazenada e compara o código de hash do servidor com o código de hash gerado localmente a partir da senha do usuário. Se forem idênticos, o ONTAP concede permissão de login.

Com a funcionalidade de vinculação rápida, o ONTAP envia apenas credenciais de usuário (nome de usuário e senha) para o servidor LDAP por meio de uma conexão segura. Em seguida, o servidor LDAP valida essas credenciais e instrui o ONTAP a conceder permissões de login.

Uma vantagem do fast bind é que não há necessidade de o ONTAP suportar cada novo algoritmo de hash suportado por servidores LDAP, porque o hash de senha é executado pelo servidor LDAP.

"Saiba mais sobre como usar o fast bind."

Você pode usar configurações de cliente LDAP existentes para o LDAP fast bind. No entanto, é altamente recomendável que o cliente LDAP seja configurado para TLS ou LDAPS; caso contrário, a senha é enviada por fio em texto simples.

Para ativar o LDAP fast bind em um ambiente ONTAP, você precisa atender a estes requisitos:

- Os usuários de administração do ONTAP devem ser configurados em um servidor LDAP que suporte a vinculação rápida.
- O SVM do ONTAP deve ser configurado para LDAP no banco de dados de switch de serviços de nome (nsswitch).
- As contas de usuário e grupo de administrador do ONTAP devem ser configuradas para autenticação nsswitch usando vinculação rápida.

Passos

1. Confirme com o administrador LDAP que o LDAP FAST BIND é suportado no servidor LDAP.
2. Certifique-se de que as credenciais de utilizador admin do ONTAP estão configuradas no servidor LDAP.
3. Verifique se o administrador ou SVM de dados está configurado corretamente para o LDAP fast bind.

   a. Para confirmar se o servidor LDAP FAST BIND está listado na configuração do cliente LDAP, introduza:

      `vserver services name-service ldap client show`

      "Saiba mais sobre a configuração do cliente LDAP."

   b. Para confirmar `ldap` que é uma das fontes configuradas para o banco de dados nsswitch `passwd`, digite:

      `vserver services name-service ns-switch show`

   "Saiba mais sobre a configuração do nsswitch."

4. Certifique-se de que os usuários de administração estejam autenticando com o nsswitch e que a autenticação LDAP de vinculação rápida esteja habilitada em suas contas.

   ◦ Para usuários existentes, insira `security login modify` e verifique as seguintes configurações de parâmetro:

      `-authentication-method nsswitch`

      `-is-ldap-fastbind true`

   Saiba mais sobre `security login modify` o "Referência do comando ONTAP"na .

   ◦ Para novos usuários de administração, "Ative o acesso à conta LDAP ou NIS ONTAP"consulte .

Exibir estatísticas LDAP para SVMs ONTAP NFS

Você pode exibir estatísticas LDAP para máquinas virtuais de armazenamento (SVMs) em um sistema de armazenamento para monitorar o desempenho e diagnosticar problemas.

Antes de começar

- Você deve ter configurado um cliente LDAP no SVM.
- Você deve ter objetos LDAP identificados a partir dos quais você pode exibir dados.

Passo

1. Veja os dados de desempenho para objetos de contador:

```
statistics show
```

Exemplos

O exemplo a seguir exibe estatísticas para a amostra chamada **smpl_1** para contadores: avg_processor_busy e CPU_busy

```
cluster1::*> statistics start -object system -counter
avg_processor_busy|cpu_busy -sample-id smpl_1
Statistics collection is being started for Sample-id: smpl_1

cluster1::*> statistics stop -sample-id smpl_1
Statistics collection is being stopped for Sample-id: smpl_1

cluster1::*> statistics show -sample-id smpl_1
Object: system
Instance: cluster
Start-time: 8/2/2012 18:27:53
End-time: 8/2/2012 18:27:56
Cluster: cluster1
   Counter                                                     Value
   -------------------------------- --------------------------------
   avg_processor_busy                                             6%
   cpu_busy
```

Informações relacionadas

- "estatísticas mostram"
- "início das estatísticas"
- "estatísticas param"

Configurar mapeamentos de nomes

Saiba mais sobre a configuração de mapeamento de nomes para SVMs ONTAP NAS

O ONTAP usa mapeamento de nomes para mapear identidades SMB para identidades UNIX, identidades Kerberos para identidades UNIX e identidades UNIX para identidades SMB. Ele precisa dessas informações para obter credenciais de usuário e fornecer acesso adequado aos arquivos, independentemente de estarem se conetando a partir de um cliente NFS ou de um cliente SMB.

Há duas exceções em que você não precisa usar o mapeamento de nomes:

- Você configura um ambiente UNIX puro e não planeja usar o acesso SMB ou o estilo de segurança NTFS em volumes.
- Em vez disso, você configura o usuário padrão a ser usado.

Nesse cenário, o mapeamento de nomes não é necessário porque, em vez de mapear cada credencial de cliente individual, todas as credenciais de cliente são mapeadas para o mesmo usuário padrão.

Observe que você pode usar o mapeamento de nomes somente para usuários, não para grupos.

No entanto, você pode mapear um grupo de usuários individuais para um usuário específico. Por exemplo, você pode mapear todos os usuários do AD que começam ou terminam com a palavra VENDAS para um usuário UNIX específico e para o UID do usuário.

Saiba mais sobre mapeamentos de nomes para SVMs ONTAP NAS

Quando o ONTAP tem que mapear credenciais para um usuário, ele primeiro verifica o banco de dados de mapeamento de nomes local e o servidor LDAP para um mapeamento existente. Verifique uma ou ambas e em que ordem é determinada pela configuração do serviço de nomes do SVM.

- Para mapeamento do Windows para UNIX

  Se nenhum mapeamento for encontrado, o ONTAP verifica se o nome de usuário do Windows em minúsculas é um nome de usuário válido no domínio UNIX. Se isso não funcionar, ele usará o usuário UNIX padrão desde que esteja configurado. Se o usuário UNIX padrão não estiver configurado e o ONTAP também não puder obter um mapeamento dessa maneira, o mapeamento falhará e um erro será retornado.

- Para mapeamento UNIX para Windows

  Se nenhum mapeamento for encontrado, o ONTAP tentará encontrar uma conta do Windows que corresponda ao nome UNIX no domínio SMB. Se isso não funcionar, ele usará o usuário SMB padrão, desde que esteja configurado. Se o usuário SMB padrão não estiver configurado e o ONTAP não puder obter um mapeamento dessa maneira, o mapeamento falhará e um erro será retornado.

As contas de máquina são mapeadas para o usuário UNIX padrão especificado por padrão. Se nenhum usuário UNIX padrão for especificado, mapeamentos de contas de máquina falharão.

- A partir do ONTAP 9.5, você pode mapear contas de máquina para usuários que não sejam o usuário UNIX padrão.
- No ONTAP 9.4 e anteriores, você não pode mapear contas de máquina para outros usuários.

  Mesmo que os mapeamentos de nomes para contas de máquinas sejam definidos, os mapeamentos serão ignorados.

Pesquisas multidomínio para mapeamentos de nomes de usuários do UNIX para o Windows em SVMs NAS ONTAP

O ONTAP oferece suporte a pesquisas de vários domínios ao mapear usuários UNIX para usuários do Windows. Todos os domínios confiáveis descobertos são pesquisados por correspondências ao padrão de substituição até que um resultado correspondente seja retornado. Como alternativa, você pode configurar uma lista de domínios confiáveis preferenciais, que é usada em vez da lista de domínios confiáveis descobertos e é pesquisada em ordem até que um resultado correspondente seja retornado.

Como as relações de confiança de domínio afetam as pesquisas de mapeamento de nomes de usuário do Windows

Para entender como o mapeamento de nomes de usuário de vários domínios funciona, você deve entender como as relações de confiança de domínio funcionam com o ONTAP. As relações de confiança do ative Directory com o domínio home do servidor SMB podem ser uma confiança bidirecional ou podem ser um dos dois tipos de confiança unidirecionais, uma confiança de entrada ou uma confiança de saída. O domínio inicial é o domínio ao qual pertence o servidor SMB no SVM.

- *Confiança bidirecional*

  Com trusts bidirecionais, ambos os domínios confiam uns nos outros. Se o domínio home do servidor SMB tiver uma confiança bidirecional com outro domínio, o domínio home pode autenticar e autorizar um usuário pertencente ao domínio confiável e vice-versa.

  As pesquisas de mapeamento de nome de usuário do UNIX para o Windows podem ser realizadas apenas em domínios com confiança bidirecional entre o domínio inicial e o outro domínio.

- *Outbound Trust*

  Com uma confiança de saída, o domínio home confia no outro domínio. Nesse caso, o domínio home pode autenticar e autorizar um usuário pertencente ao domínio confiável de saída.

  Um domínio com uma confiança de saída com o domínio inicial é *not* pesquisado ao executar pesquisas de mapeamento de nomes de usuário do UNIX para o Windows.

- *Confiança inbound*

  Com uma confiança de entrada, o outro domínio confia no domínio home do servidor SMB. Neste caso, o domínio inicial não pode autenticar ou autorizar um usuário pertencente ao domínio confiável de entrada.

  Um domínio com uma confiança de entrada com o domínio inicial é *not* pesquisado ao executar pesquisas de mapeamento de nomes de usuário do UNIX para o Windows.

Como os curingas (*) são usados para configurar pesquisas de vários domínios para mapeamento de nomes

As pesquisas de mapeamento de nomes de vários domínios são facilitadas pelo uso de curingas na seção domínio do nome de usuário do Windows. A tabela a seguir ilustra como usar curingas na parte de domínio de uma entrada de mapeamento de nomes para habilitar pesquisas de vários domínios:

Padrão	Substituição	Resultado
raiz	o administrador do servidor não está habilitado a usar a barra de ferramentas	O usuário UNIX "'root'" é mapeado para o usuário chamado "'administrador'". Todos os domínios confiáveis são pesquisados em ordem até que o primeiro usuário correspondente chamado "administrador" seja encontrado.

Padrão	Substituição	Resultado
*	clique no botão "ok"	Os usuários UNIX válidos são mapeados para os usuários do Windows correspondentes. Todos os domínios confiáveis são pesquisados em ordem até que o primeiro usuário correspondente com esse nome seja encontrado. O asterisco é válido apenas para o mapeamento de nomes de UNIX para Windows, e não para o contrário.

Como as pesquisas de nomes de vários domínios são realizadas

Você pode escolher um dos dois métodos para determinar a lista de domínios confiáveis usados para pesquisas de nomes de vários domínios:

- Use a lista de confiança bidirecional descoberta automaticamente compilada pelo ONTAP
- Use a lista de domínio confiável preferida que você compila

Se um usuário UNIX for mapeado para um usuário do Windows com um curinga usado para a seção de domínio do nome de usuário, o usuário do Windows será pesquisado em todos os domínios confiáveis da seguinte forma:

- Se uma lista de domínio confiável preferencial estiver configurada, o usuário mapeado do Windows será pesquisado somente nesta lista de pesquisa, em ordem.
- Se uma lista preferencial de domínios confiáveis não estiver configurada, o usuário do Windows será pesquisado em todos os domínios confiáveis bidirecionais do domínio doméstico.
- Se não houver domínios bidirecionalmente confiáveis para o domínio home, o usuário será pesquisado no domínio home.

Se um usuário UNIX for mapeado para um usuário do Windows sem uma seção de domínio no nome de usuário, o usuário do Windows será pesquisado no domínio inicial.

Regras de conversão de mapeamento de nomes para SVMs ONTAP NAS

Um sistema ONTAP mantém um conjunto de regras de conversão para cada SVM. Cada regra consiste em duas partes: Um *pattern* e um *replacement*. As conversões começam no início da lista apropriada e executam uma substituição com base na primeira regra de correspondência. O padrão é uma expressão regular estilo UNIX. A substituição é uma cadeia de carateres contendo sequências de escape que representam subexpressões do padrão, como no programa UNIX `sed`.

Crie mapeamentos de nomes para SVMs ONTAP NAS

Você pode usar o `vserver name-mapping create` comando para criar um mapeamento de nomes. Use mapeamentos de nomes para permitir que os usuários do Windows acessem volumes de estilo de segurança UNIX e o inverso.

Sobre esta tarefa

Para cada SVM, o ONTAP oferece suporte a até 12.500 mapeamentos de nomes para cada direção.

Passo

1. Criar um mapeamento de nomes:

```
vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-
unix|unix-win} -position integer -pattern text -replacement text
```

> As `-pattern` declarações e `-replacement` podem ser formuladas como expressões regulares. Você também pode usar a `-replacement` instrução para negar explicitamente um mapeamento para o usuário usando a cadeia de substituição nula `" "` (o caractere de espaço). Saiba mais sobre `vserver name-mapping create` o "Referência do comando ONTAP"na .

Quando os mapeamentos do Windows para UNIX são criados, todos os clientes SMB que tenham conexões abertas ao sistema ONTAP no momento em que os novos mapeamentos são criados devem fazer logout e fazer login novamente para ver os novos mapeamentos.

Exemplos

O comando a seguir cria um mapeamento de nomes no SVM chamado VS1. O mapeamento é um mapeamento do UNIX para o Windows na posição 1 na lista de prioridades. O mapeamento mapeia o usuário UNIX johnd para o usuário do Windows Eng.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

O comando a seguir cria outro mapeamento de nomes no SVM chamado VS1. O mapeamento é um mapeamento do Windows para o UNIX na posição 1 na lista de prioridades. Aqui o padrão e a substituição incluem expressões regulares. O mapeamento mapeia cada usuário CIFS no domínio ENG para usuários no domínio LDAP associado ao SVM.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

O comando a seguir cria outro mapeamento de nomes no SVM chamado VS1. Aqui, o padrão inclui "" como um elemento no nome de usuário do Windows que deve ser escapado. O mapeamento mapeia as operações do usuário do Windows para o usuário do UNIX John_OPS.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

Configurar o usuário padrão para SVMs ONTAP NAS

Você pode configurar um usuário padrão para usar se todas as outras tentativas de mapeamento falharem para um usuário ou se não quiser mapear usuários individuais entre UNIX e Windows. Alternativamente, se você quiser que a autenticação de usuários não mapeados falhe, você não deve configurar um usuário padrão.

Sobre esta tarefa

Para autenticação CIFS, se você não quiser mapear cada usuário do Windows para um usuário UNIX individual, você pode especificar um usuário UNIX padrão.

Para autenticação NFS, se você não quiser mapear cada usuário UNIX para um usuário individual do Windows, você pode especificar um usuário padrão do Windows.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Digite o seguinte comando…
Configure o usuário UNIX padrão	`vserver cifs options modify -default-unix-user user_name`
Configure o usuário padrão do Windows	`vserver nfs modify -default-win-user user_name`

Comandos ONTAP para gerenciar mapeamentos de nomes NFS

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`

Saiba mais sobre `vserver name-mapping` o "Referência do comando ONTAP"na .

Habilitar acesso para clientes NFS do Windows para SVMs ONTAP

O ONTAP suporta acesso a arquivos de clientes Windows NFSv3. Isso significa que os clientes que executam sistemas operacionais Windows com suporte a NFSv3 podem acessar arquivos em exportações NFSv3 no cluster. Para usar essa funcionalidade com êxito, você deve configurar corretamente a máquina virtual de storage (SVM) e estar ciente de certos requisitos e limitações.

Sobre esta tarefa

Por padrão, o suporte ao cliente do Windows NFSv3 está desativado.

Antes de começar

O NFSv3 precisa estar habilitado no SVM.

Passos

1. Ativar o suporte ao cliente do Windows NFSv3:

   ```
   vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly disabled
   ```

2. Em todos os SVMs que suportam clientes Windows NFSv3, desative os `-enable-ejukebox` parâmetros e `-v3-connection-drop`:

   ```
   vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection -drop disabled
   ```

   Os clientes do Windows NFSv3 agora podem montar exportações no sistema de armazenamento.

3. Certifique-se de que cada cliente do Windows NFSv3 utiliza suportes rígidos especificando a `-o mtype=hard` opção.

   Isso é necessário para garantir montagens confiáveis.

```
mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
```

Habilitar a exibição de exportações em clientes NFS para SVMs ONTAP

Os clientes NFS podem usar o `showmount -e` comando para ver uma lista de exportações disponíveis a partir de um servidor ONTAP NFS. Isso pode ajudar os usuários a identificar o sistema de arquivos que eles querem montar.

O ONTAP permite que clientes NFS visualizem a lista de exportação por padrão. Em versões anteriores, a `showmount` opção `vserver nfs modify` do comando deve ser ativada explicitamente. Para visualizar a lista de exportação, o NFSv3 deve estar habilitado no SVM.

Exemplo

O comando a seguir mostra o recurso showmount no SVM chamado VS1:

```
clusterl : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
------- ---------
vs1    enabled
```

O comando a seguir executado em um cliente NFS exibe a lista de exportações em um servidor NFS com o endereço IP 10.63.21.9:

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix        (everyone)
/unix/unixl  (everyone)
/unix/unix2  (everyone)
/            (everyone)
```

Gerenciar o acesso a arquivos usando NFS

Habilitar ou desabilitar NFSv3 para SVMs ONTAP

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`

Habilitar ou desabilitar NFSv4.0 para SVMs ONTAP

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`

Habilitar ou desabilitar NFSv4.1 para SVMs ONTAP

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 limites do pool de armazenamento ONTAP NFSv4

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`

Se você quiser…	Digite o seguinte comando…
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.
```

Habilitar ou desabilitar pNFS para SVMs ONTAP

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

Antes de começar

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 via TCP e UDP para SVMs ONTAP

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 para SVMs ONTAP

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 acesso NFS a volumes NTFS ONTAP 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.

Antes de começar

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 ONTAP NFS em portas não reservadas

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 para SVMs ONTAP NFS

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`

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

3. Defina o nível de privilégio como admin:

   `set -privilege admin`

Modificar portas usadas para serviços NFSv3 para SVMs ONTAP

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.

Antes de começar

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

Parâmetro da porta NFS	Descrição	Porta predefinida
`-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.

   Saiba mais sobre `network connections listening show` o "Referência do comando ONTAP"na .

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 ONTAP 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

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

Solucionar problemas de serviço de nomes para SVMs ONTAP NAS

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"

Verificar conexões de serviço de nomes para SVMs ONTAP NAS

Você pode verificar os servidores de nomes DNS e Lightweight Directory Access Protocol (LDAP) para verificar se eles estão conectados 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 ONTAP para gerenciar entradas de switch de serviço de nomes NAS

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`

Saiba mais sobre `vserver services name-service ns-switch` o "Referência do comando ONTAP"na .

Informações relacionadas

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

Comandos ONTAP para gerenciar o cache do serviço de nomes NAS

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 ONTAP para gerenciar mapeamentos de nomes NFS

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`

Saiba mais sobre `vserver name-mapping` o "Referência do comando ONTAP"na .

Comandos ONTAP para gerenciar usuários UNIX locais do NAS

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`

Saiba mais sobre `vserver services name-service unix-user` o "Referência do comando ONTAP"na .

Comandos ONTAP para gerenciar grupos UNIX locais NAS

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`

Saiba mais sobre `vserver services name-service unix-group` o "Referência do comando ONTAP"na .

Limites para usuários, grupos e membros de grupo UNIX locais para SVMs ONTAP NFS

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 para SVMs ONTAP NFS

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`

Se você quiser…	Use o comando…
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`

Saiba mais sobre `vserver services unix` o "Referência do comando ONTAP"na .

Comandos ONTAP para gerenciar grupos de rede locais NFS

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`

Saiba mais sobre `vserver services name-service netgroup file` o "Referência do comando ONTAP"na .

Comandos ONTAP para gerenciar configurações de domínio NFS 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.

Saiba mais sobre `vserver services name-service nis-domain` o "Referência do comando ONTAP"na .

Comandos ONTAP para gerenciar configurações de cliente NFS 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`

Saiba mais sobre `vserver services name-service ldap client` o "Referência do comando ONTAP"na .

Comandos ONTAP para gerenciar configurações NFS 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`

Saiba mais sobre `vserver services name-service ldap` o "Referência do comando ONTAP"na .

Comandos ONTAP para gerenciar modelos de esquema de cliente NFS 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.

Saiba mais sobre `vserver services name-service ldap client schema` o "Referência do comando ONTAP"na .

Comandos ONTAP 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`

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

Comandos ONTAP para gerenciar configurações de domínio NFS Kerberos

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`

Saiba mais sobre `vserver nfs kerberos realm` o "Referência do comando ONTAP"na .

Comandos ONTAP para gerenciamento de 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`

Saiba mais sobre `vserver export-policy` o "Referência do comando ONTAP"na .

Comandos ONTAP 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.

Saiba mais sobre `vserver export-policy` o "Referência do comando ONTAP"na .

Configurar o cache de credenciais NFS

Motivos para modificar o tempo de vida do cache de credenciais NFS para SVMs ONTAP

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.

Problema	Medidas corretivas
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.
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.

Configurar o tempo de vida para credenciais de usuário NFS armazenadas em cache para SVMs ONTAP

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

Liberar caches de política de exportação para SVMs ONTAP NAS

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.
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.

Se você quiser flush…	Digite o comando…
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`

Exibir a fila e o cache do netgroup de política de exportação para SVMs ONTAP NFS

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`

Saiba mais sobre `vserver export-policy netgroup` o "Referência do comando ONTAP"na .

Verifique se um endereço IP do cliente é membro de um grupo de rede ONTAP NFS

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 para SVMs ONTAP NFS

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

Aprenda sobre bloqueio de arquivos entre protocolos para SVMs ONTAP NFS

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.

Saiba mais sobre bits somente leitura para SVMs ONTAP NFS

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.

O bit somente leitura interage com os bits ACL e do modo Unix das seguintes maneiras:

Quando o bit somente leitura é definido em um arquivo:

- Nenhuma alteração será feita na ACL desse arquivo. Os clientes NFS verão a mesma ACL de antes da

definição do bit somente leitura.

- Todos os bits do modo Unix que permitem acesso de gravação ao arquivo são ignorados.
- Clientes NFS e SMB podem ler o arquivo, mas não podem modificá-lo.
- ACLs e bits do modo UNIX são ignorados em favor do bit somente leitura. Isso significa que, mesmo que a ACL permita acesso de gravação, o bit somente leitura impede modificações.

Quando o bit somente leitura não está definido em um arquivo:

- O ONTAP determina o acesso com base nos bits do ACL e do modo UNIX.
  - Se os bits da ACL ou do modo UNIX negarem acesso de gravação, os clientes NFS e SMB não poderão modificar o arquivo.
  - Se nem os bits do ACL nem do modo UNIX negarem acesso de gravação, os clientes NFS e SMB poderão modificar o arquivo.

> 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.

Aprenda como o ONTAP NFS e o Windows diferem no tratamento de 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 .

Exibir informações sobre bloqueios para SVMs ONTAP NFS

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. Saiba mais sobre `vserver locks show` o "Referência do comando ONTAP"na .

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
```

Quebrando bloqueios de arquivo para SVMs ONTAP NFS

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. Saiba mais sobre `vserver locks break` o "Referência do comando ONTAP"na .

Passos

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

   Saiba mais sobre `vserver locks show` o "Referência do comando ONTAP"na .

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
   ```

Aprenda como os filtros de primeira leitura e primeira gravação do ONTAP 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
```

Modificar o ID de implementação do servidor NFSv4.1 para SVMs ONTAP

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

Saiba mais sobre os benefícios de habilitar ACLs NFSv4 para SVMs ONTAP

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

Saiba mais sobre ACLs NFSv4 para SVMs ONTAP

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. Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

Habilitar ou desabilitar a modificação da ACL do NFSv4 para SVMs ONTAP

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
   ```

Aprenda como o ONTAP usa ACLs NFSv4 para determinar se ele pode excluir arquivos

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.

Habilitar ou desabilitar ACLs NFSv4 para SVMs ONTAP

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`

Modificar o limite máximo de ACE para ACLs NFSv4 para SVMs ONTAP

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

Habilitar ou desabilitar delegações de arquivos de leitura NFSv4 para SVMs ONTAP

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.

Habilitar ou desabilitar delegações de arquivos de gravação NFSv4 para SVMs ONTAP

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`
Desativar as delegações de ficheiros de gravação NFSv4	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled`

Se você quiser…	Então…
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

Saiba mais sobre bloqueio de arquivos e registros NFSv4 para SVMs ONTAP

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 concessão de bloqueio NFSv4 para SVMs ONTAP

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 carência de bloqueio NFSv4 para SVMs ONTAP

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
   ```

Saiba mais sobre referências NFSv4 para SVMs ONTAP

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.

Habilitar ou desabilitar referências NFSv4 para SVMs ONTAP

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.

Antes de começar

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 para SVMs ONTAP 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"
- "exibição de objeto de catálogo de estatísticas"
- "estatísticas mostram"
- "início das estatísticas"
- "estatísticas param"

Exibir estatísticas de DNS para SVMs ONTAP NFS

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"
- "exibição de objeto de catálogo de estatísticas"
- "estatísticas mostram"
- "início das estatísticas"
- "estatísticas param"

Exibir estatísticas NIS para SVMs ONTAP NFS

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"
- "exibição de objeto de catálogo de estatísticas"
- "estatísticas mostram"
- "início das estatísticas"
- "estatísticas param"

Saiba mais sobre o suporte para VMware vStorage sobre ONTAP 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?"

Habilitar ou desabilitar VMware vStorage sobre ONTAP 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"

Habilitar ou desabilitar o suporte a rquota em SVMs ONTAP NFS

O protocolo de cota remota (rquota) permite que os clientes NFS obtenham informações de cota para usuários de uma máquina remota. O suporte para versões rquota varia de acordo com a sua versão do ONTAP.

- O rquota v1 é suportado no ONTAP 9 e posterior.
- O rquota v2 é suportado no ONTAP 9.12.1 e posterior.

  Se você atualizar do rquota v1 para o rquota v2, poderá notar uma alteração inesperada no limite de cota do usuário. Essa alteração se deve à diferença na maneira como a cota é calculada entre rquota v1 e rquota v2. Para mais informações, consulte o"Base de conhecimento da NetApp : Por que o limite de cota do usuário mudou inesperadamente" .

Sobre esta tarefa

Por padrão, rquota está desativada.

Passo

1. Ativar ou desativar rquota:

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 .

Saiba mais sobre melhorias de desempenho do NFSv3 e NFSv4 e tamanho de transferência TCP para SVMs ONTAP

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.

Modificar o tamanho máximo de transferência TCP NFSv3 e NFSv4 para SVMs ONTAP

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
```

Configurar o número de IDs de grupo permitidos para usuários NFS para SVMs ONTAP

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 habilitar grupos estendidos(`-auth-sys-extended-groups`) que usam IDs de grupo além do máximo padrão de 16, consulte o"Base de conhecimento da NetApp : Quais são os pré-requisitos para habilitar auth-sys-extended-groups?"

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
```

Informações relacionadas

- "Base de conhecimento da NetApp : alterações nos grupos estendidos AUTH_SYS para autenticação NFS para ONTAP 9"

Controlar o acesso do usuário root aos dados de segurança NTFS para SVMs ONTAP

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
```

Versões e clientes de NFS compatíveis

Saiba mais sobre as versões e clientes ONTAP NFS suportados

Antes de poder usar o NFS na rede, você precisa saber quais versões e clientes do ONTAP são compatíveis.

Esta tabela observa quando versões maiores e menores do protocolo NFS são suportadas por padrão no ONTAP. O suporte por padrão não indica que esta é a versão mais antiga do ONTAP que suporta esse protocolo NFS.

Versão	Suportado	Introduzido
NFSv3	Sim	Todos os lançamentos do ONTAP
NFSv4.0	Sim	ONTAP 8
NFSv4.1	Sim	ONTAP 8,1
NFSv4.2	Sim	ONTAP 9,8
PNFS	Sim	ONTAP 8,1

Para obter as informações mais recentes sobre quais clientes NFS ONTAP suportam, consulte a Matriz de interoperabilidade.

"Ferramenta de Matriz de interoperabilidade do NetApp"

Saiba mais sobre o suporte ONTAP para a funcionalidade NFSv4.0

O ONTAP suporta todas as funcionalidades obrigatórias no NFSv4,0, exceto os mecanismos de segurança SPKM3 e LIPKEY.

A seguinte funcionalidade NFSv4 é suportada:

- **COMPOSTO**

  Permite que um cliente solicite várias operações de arquivo em uma única solicitação RPC (chamada de procedimento remoto).

- * Delegação de arquivos*

  Permite que o servidor delege o controle de arquivos a alguns tipos de clientes para acesso de leitura e gravação.

- **Pseudo-fs**

  Usado por servidores NFSv4 para determinar pontos de montagem no sistema de armazenamento. Não existe nenhum protocolo de montagem no NFSv4.

- **Bloqueio**

  Baseado em leasing. Não existem protocolos NLM (Network Lock Manager) ou NSM (Network Status Monitor) separados no NFSv4.

Para obter mais informações sobre o protocolo NFSv4,0, consulte RFC 3530.

Saiba mais sobre as limitações de suporte ONTAP para NFSv4

Você deve estar ciente de várias limitações do suporte do ONTAP para NFSv4.

- O recurso de delegação não é suportado por todos os tipos de cliente.
- No ONTAP 9.4 e versões anteriores, nomes com carateres não-ASCII em volumes diferentes de UTF8 volumes são rejeitados pelo sistema de armazenamento.

  No ONTAP 9.5 e versões posteriores, os volumes criados com a configuração de linguagem utf8mb4 e montados usando NFS v4 não estão mais sujeitos a essa restrição.

- Todos os identificadores de arquivo são persistentes; o servidor não fornece alças de arquivo voláteis.
- Migração e replicação não são compatíveis.
- Os clientes NFSv4 não são suportados com espelhos de compartilhamento de carga somente leitura.

  O ONTAP encaminha clientes NFSv4 para a fonte do espelho de compartilhamento de carga para acesso direto de leitura e gravação.

- Atributos nomeados não são suportados.
- Todos os atributos recomendados são suportados, exceto para o seguinte:
  - `archive`
  - `hidden`
  - `homogeneous`
  - `mimetype`
  - `quota_avail_hard`

- quota_avail_soft
- quota_used
- system
- time_backup

> Embora não ofereça suporte aos `quota*` atributos, o ONTAP oferece suporte a cotas de usuário e grupo por meio do protocolo RQUOTA de banda lateral.

Saiba mais sobre o suporte ONTAP para NFSv4.1

A partir do ONTAP 9.8, a funcionalidade nconnect está disponível por predefinição quando o NFSv4,1 está ativado.

Implementações anteriores de clientes NFS usam apenas uma única conexão TCP com uma montagem. No ONTAP, uma única conexão TCP pode se tornar um gargalo com o aumento de IOPS.

O nconnect melhora o desempenho do cliente NFS ao permitir múltiplas conexões TCP (até 16) para uma única montagem, ajudando a superar o gargalo de desempenho que pode ocorrer com uma única conexão TCP à medida que o IOPS aumenta.

NFSv4,1 é ativado por padrão no ONTAP 9.9,1 e posterior. Em versões anteriores, você pode habilitá-la especificando a `-v4.1` opção e definindo-a para `enabled` quando criar um servidor NFS na máquina virtual de armazenamento (SVM).

O ONTAP não suporta delegações de nível de diretório e arquivo NFSv4,1.

Informações relacionadas

"Saiba mais sobre o nconnect para otimizar o desempenho do NFS.".

Saiba mais sobre o suporte ONTAP para NFSv4.2

A partir do ONTAP 9.8, o ONTAP suporta o protocolo NFSv4,2 para permitir acesso a clientes habilitados para NFSv4,2.

O NFSv4.2 está habilitado por padrão no ONTAP 9.9.1 e versões posteriores. No ONTAP 9.8, é necessário habilitar manualmente a versão 4.2 especificando o `-v4.2` opção e definindo-a para `enabled` ao criar um servidor NFS na máquina virtual de armazenamento (SVM). Habilitar o NFSv4.1 também permite que os clientes usem os recursos do NFSv4.1 enquanto estiverem montados como v4.2.

Versões sucessivas do ONTAP expandem o suporte para NFSv4,2 recursos opcionais.

Começando com…	NFSv4,2 recursos opcionais incluem …
ONTAP 9.12,1	• Atributos estendidos do NFS • Ficheiros esparsos • Reservas de espaço
ONTAP 9.9,1	Controlo de Acesso obrigatório (MAC) identificado como NFS

Etiquetas de segurança NFS v4,2

A partir do ONTAP 9.9,1, os rótulos de segurança NFS podem ser ativados. Eles são desativados por padrão.

Com os rótulos de segurança NFS v4,2, os servidores ONTAP NFS são cientes do Controle de Acesso obrigatório (MAC), armazenando e recuperando atributos SEC_label enviados pelos clientes.

Para obter mais informações, "RFC 7240"consulte .

A partir do ONTAP 9.12,1, as etiquetas de segurança NFS v4,2 são compatíveis com operações de despejo NDMP. Se rótulos de segurança forem encontrados em arquivos ou diretórios em versões anteriores, o despejo falhará.

Passos

1. Altere a configuração de privilégios para avançado:

```
set -privilege advanced
```

2. Ativar etiquetas de segurança:

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel enabled
```

Atributos estendidos do NFS

A partir do ONTAP 9.12,1, os atributos estendidos NFS (xattrs) são ativados por padrão.

Atributos estendidos são atributos NFS padrão definidos "RFC 8276" e habilitados em clientes NFS modernos. Eles podem ser usados para anexar metadados definidos pelo usuário a objetos do sistema de arquivos, e são de interesse em implantações de segurança avançadas.

Atributos estendidos NFS não são atualmente suportados para operações de despejo NDMP. Se atributos estendidos forem encontrados em arquivos ou diretórios, o despejo prossegue, mas não faz backup dos atributos estendidos nesses arquivos ou diretórios.

Se você precisar desativar atributos estendidos, use o `vserver nfs modify -v4.2-xattrs disabled` comando.

Saiba mais sobre o nconnect para otimizar o desempenho do NFS.

A partir do ONTAP 9.8, a funcionalidade nconnect está disponível por padrão quando o NFSv4.1 está habilitado. O nconnect melhora o desempenho do cliente NFS, permitindo múltiplas conexões TCP para uma única montagem.

Como funciona o nconnect

Implementações anteriores de clientes NFS usam apenas uma única conexão TCP com uma montagem. No ONTAP, uma única conexão TCP pode se tornar um gargalo com o aumento de IOPS.

Um cliente com nconnect habilitado pode ter várias conexões TCP (até 16) associadas a uma única montagem NFS. O nconnect usa apenas um endereço IP e estabelece várias conexões TCP sobre esse único

IP para montar a exportação NFS. O cliente NFS distribui as operações de arquivo em várias conexões TCP em um esquema de rodízio, obtendo maior taxa de transferência da largura de banda de rede disponível.

Versões NFS suportadas

- O nconnect é recomendado para montagens NFSv3, NFSv4.2 e NFSv4.1.
- O nconnect *não* é recomendado para montagens NFSv4.0.

> Para obter o melhor desempenho, a NetApp recomenda o uso do NFSv4.1 com o nconnect em vez do NFSv4.0. Embora o NFSv4.0 suporte múltiplas conexões, o NFSv4.1 com nconnect proporciona melhor distribuição de carga e maior taxa de transferência.

Suporte ao cliente

Consulte a documentação do cliente NFS para confirmar se o nconnect é suportado na versão do cliente.

Informações relacionadas

- "Saiba mais sobre o suporte ONTAP para NFSv4.1"
- "Saiba mais sobre o suporte ONTAP para NFSv4.2"

Saiba mais sobre o suporte ONTAP para NFS paralelo

O ONTAP dá suporte a NFS paralelo (pNFS). O protocolo pNFS oferece melhorias de desempenho ao proporcionar aos clientes acesso direto aos dados de um conjunto de arquivos distribuídos por vários nós de um cluster. Ele ajuda os clientes a localizar o caminho ideal para um volume.

Saiba mais sobre montagens rígidas ONTAP NFS

Ao solucionar problemas de montagem, você precisa ter certeza de que está usando o tipo de montagem correto. O NFS suporta dois tipos de montagem: Suportes macios e suportes rígidos. Você deve usar apenas suportes rígidos por razões de confiabilidade.

Você não deve usar montagens virtuais, especialmente quando houver possibilidade de tempos limite frequentes de NFS. As condições de corrida podem ocorrer como resultado desses tempos limite, o que pode levar à corrupção de dados.

NFS paralelo

Introdução

Saiba mais sobre NFS paralelo (pNFS) no ONTAP.

O NFS paralelo foi introduzido como um padrão RFC em janeiro de 2010, sob o RFC-5661, para permitir que os clientes acessem diretamente os dados de arquivos em servidores NFSv4.1, separando os caminhos de metadados e de dados. Esse acesso direto oferece benefícios de desempenho por meio da localização de dados, eficiência

da CPU e paralelização de operações. Uma RFC posterior foi elaborada em 2018, abrangendo os tipos de layout pNFS (RFC-8434), que define padrões para layouts de arquivos, blocos e objetos. O ONTAP utiliza o tipo de layout de arquivo para operações pNFS.

> A partir de julho de 2024, o conteúdo de relatórios técnicos publicados anteriormente como PDFs foi integrado à documentação do produto ONTAP . A documentação de gerenciamento de armazenamento NFS do ONTAP agora inclui conteúdo do *TR-4063: Sistema de Arquivos de Rede Paralelo (pNFS) no NetApp ONTAP*.

Durante anos, o NFSv3 foi a versão padrão do protocolo NFS, utilizada em praticamente todos os casos de uso. No entanto, o protocolo apresentava limitações, como a falta de capacidade de manter estado, um modelo de permissões rudimentar e recursos básicos de bloqueio. O NFSv4.0 (RFC 7530) introduziu uma série de melhorias em relação ao NFSv3 e foi ainda mais aprimorado com as versões subsequentes NFSv4.1 (RFC 5661) e NFSv4.2 (RFC 7862), que adicionaram recursos como o NFS paralelo (pNFS).

Benefícios do NFSv4.x

O NFSv4.x oferece as seguintes vantagens em relação ao NFSv3:

- Compatível com firewalls, pois o NFSv4 utiliza apenas uma única porta (2049) para suas operações.
- Gerenciamento de cache avançado e agressivo, como delegações no NFSv4.x
- Opções robustas de segurança RPC que empregam criptografia
- Internacionalização de caracteres
- Operações compostas
- Funciona apenas com TCP
- Protocolo com estado (não sem estado como o NFSv3)
- Integração completa do Kerberos para mecanismos de autenticação eficientes
- Encaminhamentos NFS
- Suporte para controle de acesso compatível com UNIX e Windows.
- Identificadores de usuário e grupo baseados em strings
- pNFS (NFSv4.1)
- Atributos estendidos (NFSv4.2)
- Etiquetas de segurança (NFSv4.2)
- Operações de arquivo esparsas (FALLOCATE) (NFSv4.2)

Para obter mais informações sobre o NFSv4.x em geral, incluindo as melhores práticas e detalhes sobre os recursos, consulte "Relatório técnico da NetApp 4067: Guia de práticas recomendadas e implementação de NFS".

Informações relacionadas

- "Visão geral da configuração NFS"
- "Visão geral do gerenciamento do NFS"
- "Gerenciamento de volumes do FlexGroup"
- "Visão geral do trunking NFS"

- https://www.netapp.com/pdf.html?item=/media/19370-tr-4523.pdf
- "Relatório técnico do NetApp 4616: Kerberos NFS no ONTAP com o Microsoft ative Directory"

Aprenda sobre a arquitetura pNFS no ONTAP.

A arquitetura pNFS é composta por três componentes principais: um cliente NFS que suporta pNFS, um servidor de metadados que fornece um caminho dedicado para operações de metadados e um servidor de dados que fornece caminhos localizados para arquivos.

O acesso do cliente ao pNFS requer conectividade de rede aos caminhos de dados e metadados disponíveis no servidor NFS. Se o servidor NFS contiver interfaces de rede inacessíveis aos clientes, ele poderá anunciar caminhos de dados inacessíveis, o que pode causar interrupções.

Servidor de metadados

O servidor de metadados no pNFS é estabelecido quando um cliente inicia uma montagem usando NFSv4.1 ou posterior, com o pNFS habilitado no servidor NFS. Quando isso é feito, todo o tráfego de metadados é enviado por meio dessa conexão e permanece nela durante todo o período de montagem, mesmo que a interface seja migrada para outro nó.

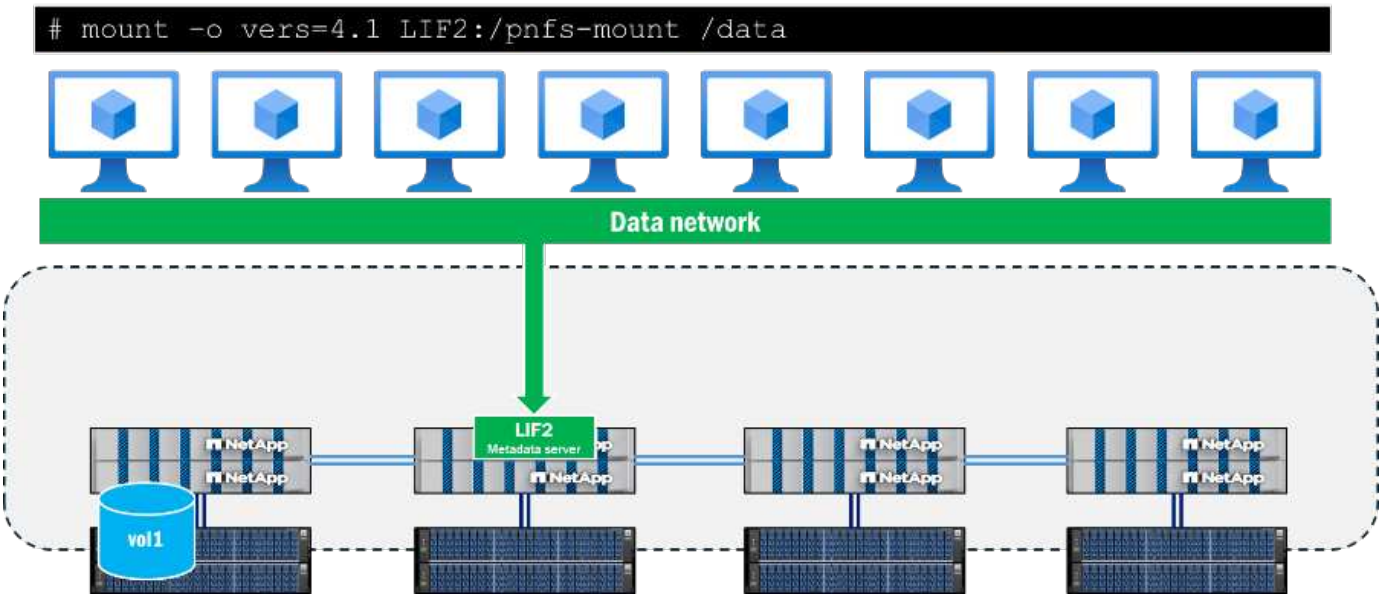


Figura 1. Estabeleça o servidor de metadados em pNFS no ONTAP.

O suporte a pNFS é determinado durante a chamada de montagem, especificamente nas chamadas EXCHANGE_ID. Isso pode ser visto em uma captura de pacotes abaixo das operações NFS como um indicador. Quando os sinalizadores pNFS `EXCHGID4_FLAG_USE_PNFS_DS` e `EXCHGID4_FLAG_USE_PNFS_MDS` Se o parâmetro estiver definido como 1, a interface estará apta para operações de dados e metadados no pNFS.

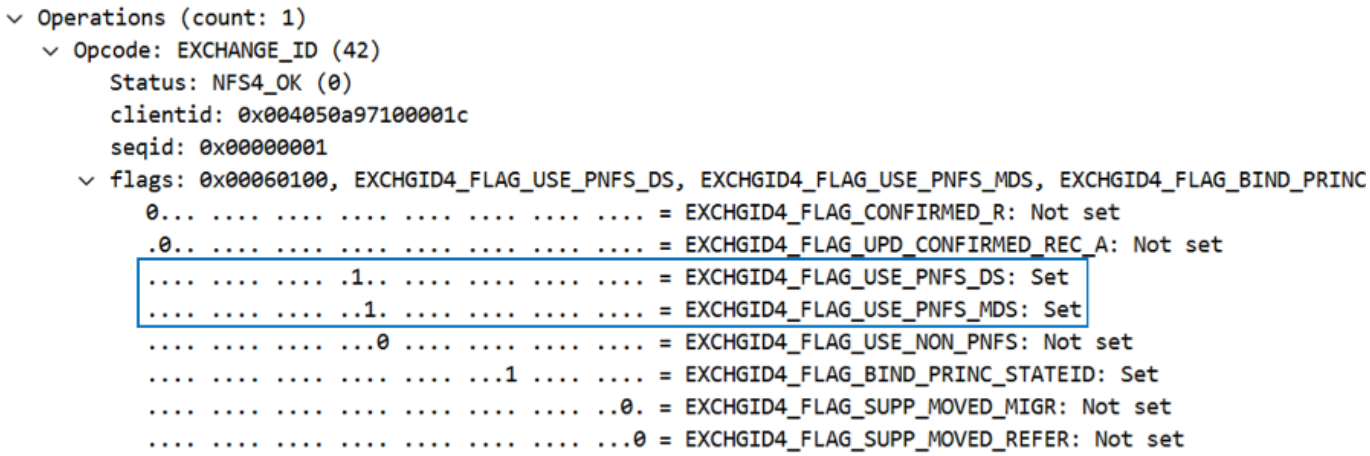


Figura 2. Captura de pacotes para montagem pNFS

Os metadados no NFS geralmente consistem em atributos de arquivos e pastas, como identificadores de arquivos, permissões, horários de acesso e modificação e informações de propriedade. Os metadados também podem incluir a criação e exclusão de chamadas, a vinculação e desvinculação de chamadas e renomeações.

Em pNFS, existe também um subconjunto de chamadas de metadados específicas para o recurso pNFS, que são abordadas com mais detalhes em "RFC 5661". Essas chamadas são usadas para ajudar a determinar dispositivos elegíveis para pNFS, mapeamentos de dispositivos para conjuntos de dados e outras informações necessárias. A tabela a seguir mostra uma lista dessas operações de metadados específicas do pNFS.

Operação	Descrição
LAYOUTGET	Obtém o mapa do servidor de dados a partir do servidor de metadados.
LAYOUTCOMMIT	Os servidores confirmam o layout e atualizam os mapas de metadados.
LAYOUTRETURN	Retorna o layout original ou o novo layout caso os dados tenham sido modificados.
OBTER INFORMAÇÕES DO DISPOSITIVO	O cliente recebe informações atualizadas sobre um servidor de dados no cluster de armazenamento.
OBTER LISTA DE DISPOSITIVOS	O cliente solicita a lista de todos os servidores de dados que participam do cluster de armazenamento.
CB_LAYOUTRECALL	O servidor recupera o layout dos dados do cliente caso sejam detectados conflitos.
CB_RECALL_ANY	Retorna todos os layouts para o servidor de metadados.
CB_NOTIFY_DEVICEID	Notifica sobre quaisquer alterações no ID do dispositivo.

Informações sobre o caminho dos dados

Após o servidor de metadados ser estabelecido e as operações de dados começarem, o ONTAP inicia o rastreamento dos IDs de dispositivo elegíveis para operações de leitura e gravação pNFS, bem como os mapeamentos de dispositivo, que associam os volumes no cluster às interfaces de rede locais. Esse processo ocorre quando uma operação de leitura ou gravação é realizada no ponto de montagem. Chamadas de metadados, como `GETATTR`. não acionará esses mapeamentos de dispositivos. Assim sendo, executar um `ls` O comando executado dentro do ponto de montagem não atualizará os mapeamentos.

Os dispositivos e mapeamentos podem ser visualizados usando a CLI do ONTAP com privilégios avançados,

conforme mostrado abaixo.

```
::*> pnfs devices show -vserver DEMO
  (vserver nfs pnfs devices show)
Vserver Name     Mapping ID      Volume MSID     Mapping Status
Generation
---------------  --------------- --------------- ---------------
-------------
DEMO             16              2157024470      available       1

::*> pnfs devices mappings show -vserver SVM
  (vserver nfs pnfs devices mappings show)
Vserver Name    Mapping ID      Dsid            LIF IP
--------------  --------------- --------------- --------------------
DEMO            16              2488            10.193.67.211
```

Nesses comandos, os nomes dos volumes não estão presentes. Em vez disso, são utilizados os IDs numéricos associados a esses volumes: o ID do conjunto mestre (MSID) e o ID do conjunto de dados (DSID). Para encontrar os volumes associados aos mapeamentos, você pode usar `volume show -dsid [dsid_numeric]` ou `volume show -msid [msid_numeric]` com privilégios avançados da CLI do ONTAP .

Quando um cliente tenta ler ou gravar em um arquivo localizado em um nó remoto em relação à conexão com o servidor de metadados, o pNFS negocia os caminhos de acesso apropriados para garantir a localidade dos dados nessas operações, e o cliente é redirecionado para o dispositivo pNFS anunciado, em vez de tentar percorrer a rede do cluster para acessar o arquivo. Isso ajuda a reduzir a sobrecarga da CPU e a latência da rede.

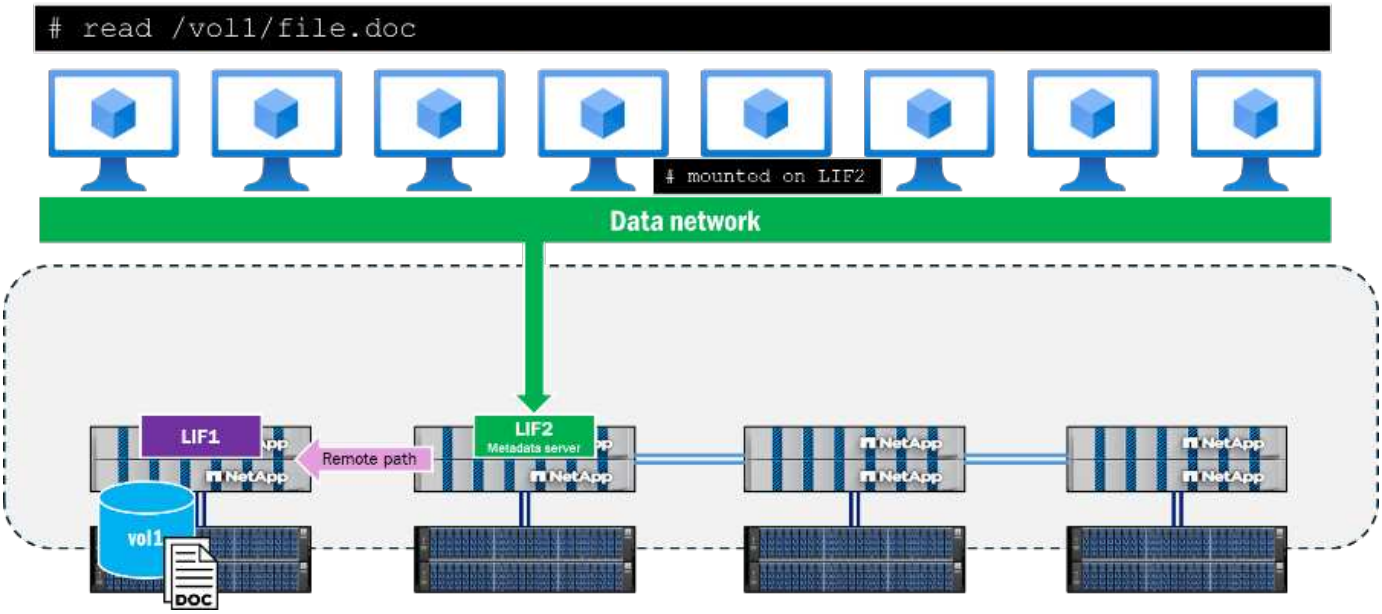


Figura 3. Caminho de leitura remota usando NFSv4.1 sem pNFS

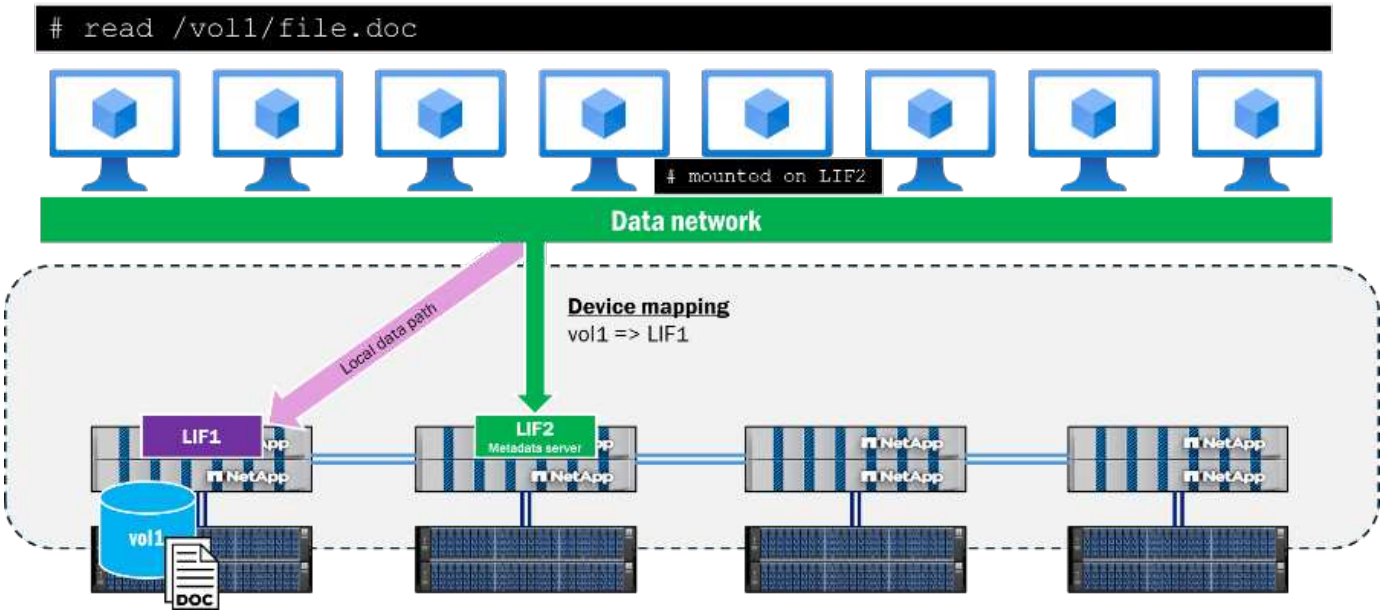


Figura 4. Caminho de leitura localizado usando pNFS

caminho de controle pNFS

Além dos metadados e dos dados presentes no pNFS, existe também um caminho de controle do pNFS. O caminho de controle é usado pelo servidor NFS para sincronizar as informações do sistema de arquivos. Em um cluster ONTAP , a rede de backend do cluster replica periodicamente para garantir que todos os dispositivos pNFS e seus mapeamentos estejam sincronizados.

fluxo de trabalho de população de dispositivos pNFS

A seguir, descrevemos como um dispositivo pNFS é populado no ONTAP depois que um cliente faz uma solicitação para ler ou gravar um arquivo em um volume.

1. O cliente solicita leitura ou gravação; uma operação OPEN é realizada e o identificador do arquivo é obtido.
2. Após a operação OPEN ser executada, o cliente envia o identificador do arquivo para o armazenamento em uma chamada LAYOUTGET através da conexão com o servidor de metadados.
3. LAYOUTGET retorna ao cliente informações sobre o layout do arquivo, como o ID do estado, o tamanho da faixa, o segmento do arquivo e o ID do dispositivo.
4. Em seguida, o cliente obtém o ID do dispositivo e envia uma chamada GETDEVINFO ao servidor para recuperar o endereço IP associado ao dispositivo.
5. O armazenamento envia uma resposta com a lista de endereços IP associados para acesso local ao dispositivo.
6. O cliente continua a conversa NFS através do endereço IP local enviado de volta pelo armazenamento.

Interação do pNFS com os volumes do FlexGroup

Os volumes FlexGroup no ONTAP apresentam o armazenamento como componentes de FlexVol volume que abrangem vários nós em um cluster, o que permite que uma carga de trabalho aproveite vários recursos de hardware, mantendo um único ponto de montagem. Como vários nós com múltiplas interfaces de rede interagem com a carga de trabalho, é natural que o tráfego remoto atravesse a rede do cluster de backend no ONTAP.

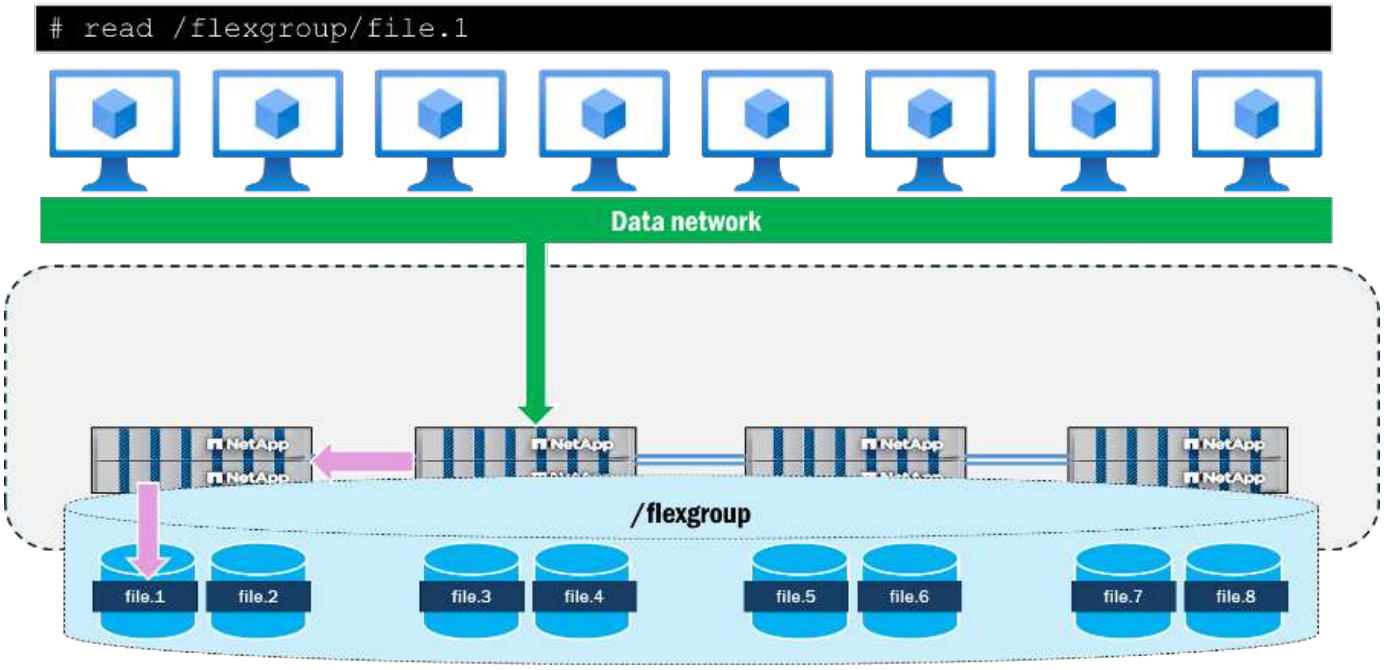


Figura 5. Acesso a um único arquivo em um volume FlexGroup sem pNFS

Ao utilizar o pNFS, o ONTAP rastreia os layouts de arquivo e volume do volume FlexGroup e os mapeia para as interfaces de dados locais no cluster. Por exemplo, se um volume constituinte que contém um arquivo sendo acessado reside no nó 1, o ONTAP notificará o cliente para redirecionar o tráfego de dados para a interface de dados no nó 1.

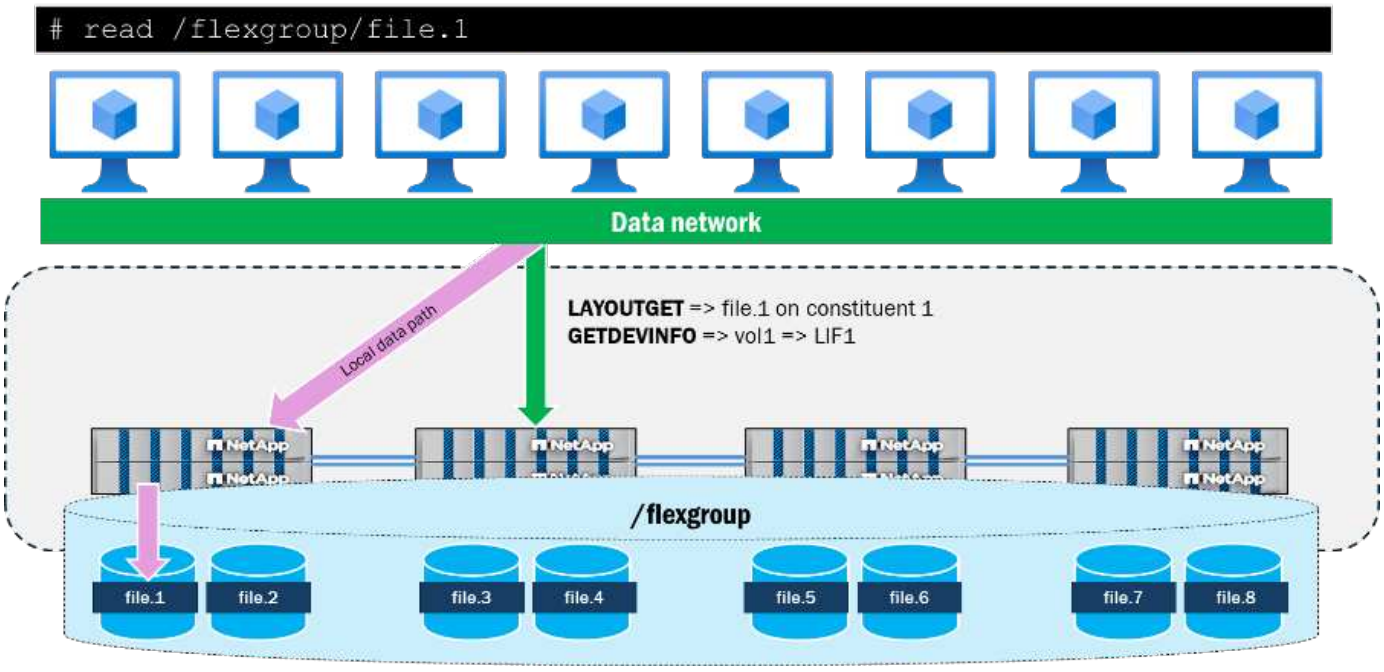


Figura 6. Acesso a um único arquivo em um volume FlexGroup com pNFS

O pNFS também permite a apresentação de caminhos de rede paralelos para arquivos a partir de um único cliente, algo que o NFSv4.1 sem pNFS não oferece. Por exemplo, se um cliente quiser acessar quatro arquivos simultaneamente a partir do mesmo ponto de montagem usando NFSv4.1 sem pNFS, o mesmo caminho de rede será utilizado para todos os arquivos e o cluster ONTAP enviará solicitações remotas para esses arquivos. O caminho de montagem pode se tornar um gargalo para as operações, já que todas seguem um único caminho e chegam a um único nó, além de também atender operações de metadados juntamente com as operações de dados.

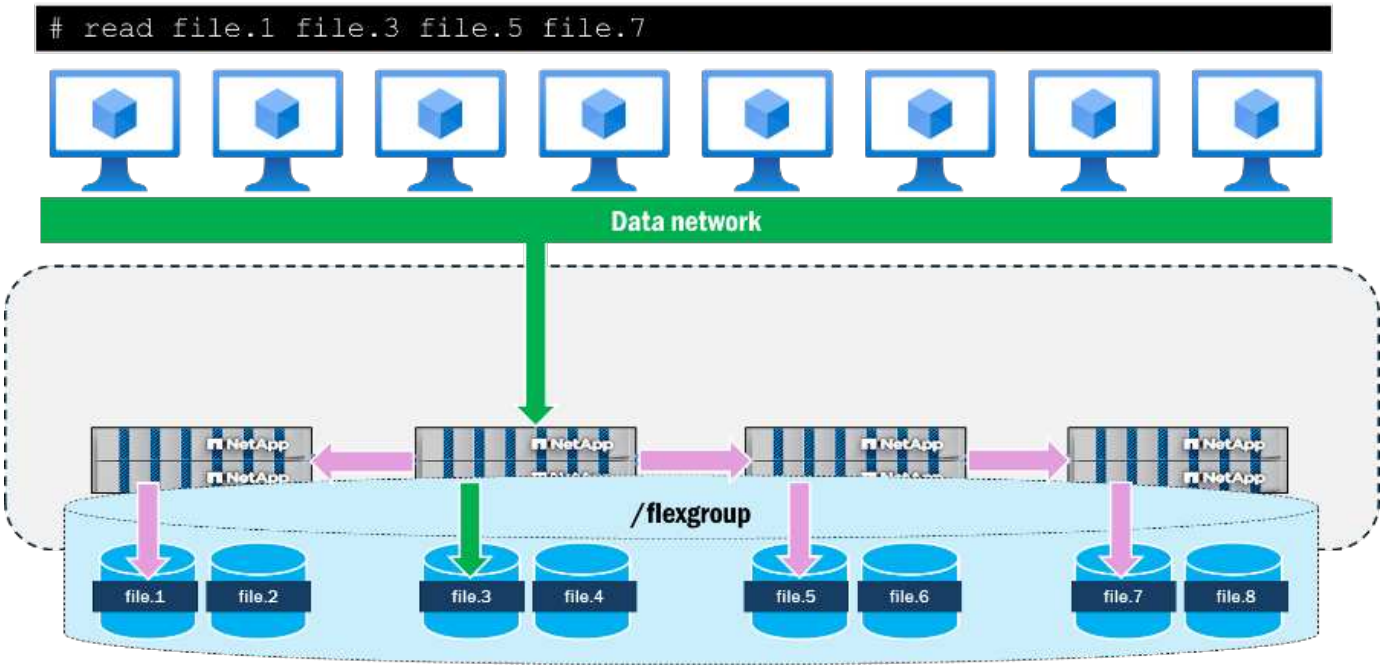


Figura 7. Acesso simultâneo a múltiplos arquivos em um volume FlexGroup sem pNFS

Quando o pNFS é usado para acessar simultaneamente os mesmos quatro arquivos a partir de um único cliente, o cliente e o servidor negociam caminhos locais para cada nó com os arquivos e usam múltiplas conexões TCP para as operações de dados, enquanto o caminho de montagem atua como o local para todas as operações de metadados. Isso proporciona benefícios em termos de latência, utilizando caminhos locais para os arquivos, mas também pode adicionar benefícios de taxa de transferência por meio do uso de múltiplas interfaces de rede, desde que os clientes possam enviar dados suficientes para saturar a rede.

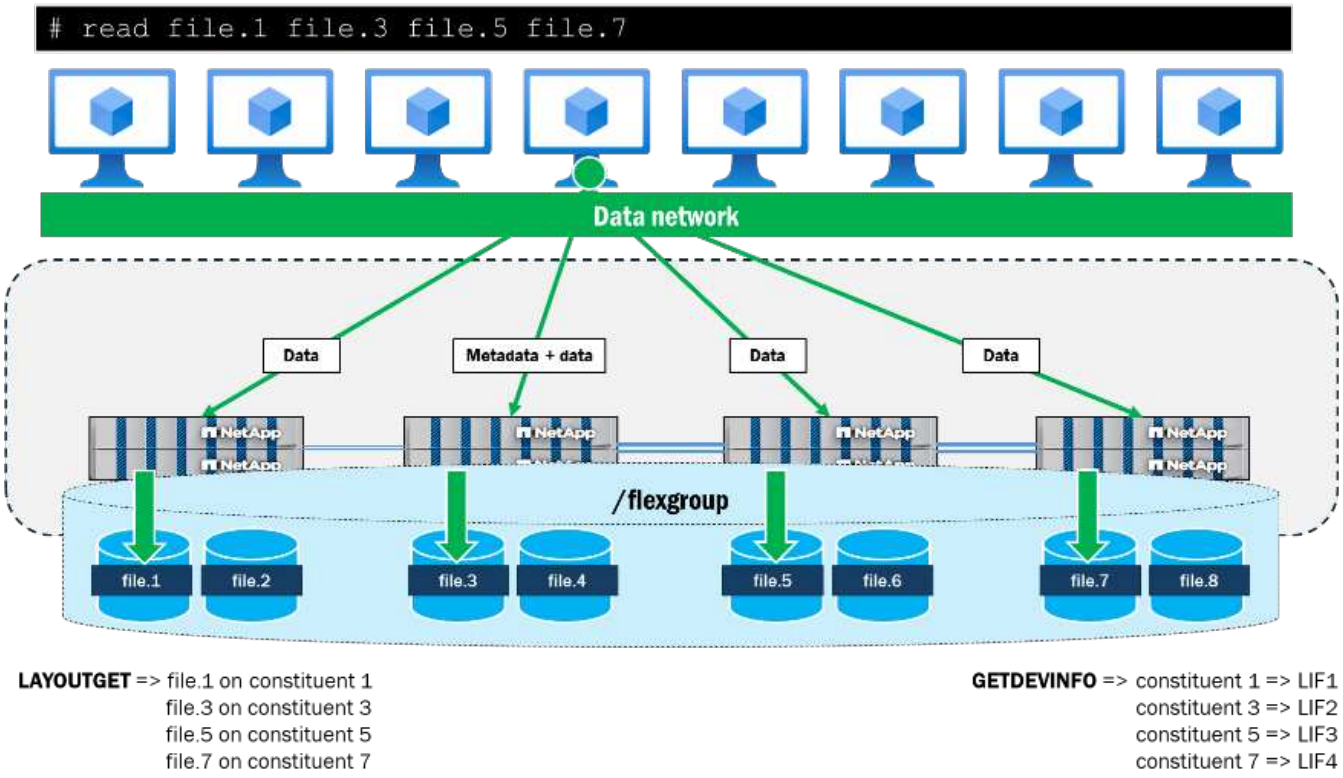


Figura 8. Acesso simultâneo a múltiplos arquivos em um volume FlexGroup com pNFS.

A seguir, são apresentados os resultados de um teste simples executado em um único cliente RHEL 9.5, onde

quatro arquivos de 10 GB (todos residentes em volumes constituintes diferentes em dois nós de cluster ONTAP) são lidos em paralelo usando o comando dd. Para cada arquivo, o rendimento geral e o tempo de conclusão foram melhorados ao usar o pNFS. Ao usar o NFSv4.1 sem pNFS, a diferença de desempenho entre arquivos locais no ponto de montagem e arquivos remotos foi maior do que com pNFS.

Teste	Taxa de transferência por arquivo (MB/s)	Tempo de conclusão por arquivo
NFSv4.1: sem pNFS	• Arquivo 1–228 (local) • Arquivo 2–227 (local) • Arquivo.3–192 (remoto) • Arquivo 4–192 (remoto)	• Arquivo 1–46 (local) • Arquivo.2–46.1 (local) • Arquivo.3–54.5 (remoto) • Arquivo.4–54.5 (remoto)
NFSv4.1: com pNFS	• Arquivo 1–248 (local) • Arquivo 2–246 (local) • Arquivo 3–244 (local via pNFS) • Arquivo 4–244 (local via pNFS)	• Arquivo.1–42.3 (local) • Arquivo.2–42.6 (local) • Arquivo 3–43 (local via pNFS) • Arquivo 4–43 (local via pNFS)

Informações relacionadas

- "Gerenciamento de volumes do FlexGroup"
- "Relatório Técnico 4571 da NetApp : Melhores Práticas do FlexGroup"

Casos de uso de pNFS no ONTAP

O pNFS pode ser usado com vários recursos do ONTAP para melhorar o desempenho e fornecer flexibilidade adicional para cargas de trabalho NFS.

pNFS com nconnect

O NFS introduziu uma nova opção de montagem em alguns clientes e servidores mais recentes, que permite estabelecer múltiplas conexões TCP ao mesmo tempo que se utiliza um único endereço IP. Isso proporciona um mecanismo para melhor paralelizar operações, contornar limitações do servidor e do cliente NFS e, potencialmente, oferecer maior desempenho geral a determinadas cargas de trabalho. O nconnect é compatível com o ONTAP 9.8 e versões posteriores, desde que o cliente também o suporte.

Ao usar o nconnect com o pNFS, as conexões serão paralelizadas usando a opção nconnect em cada dispositivo pNFS anunciado pelo servidor NFS. Por exemplo, se o nconnect estiver definido como quatro e houver quatro interfaces elegíveis para pNFS, o número total de conexões criadas será de até 16 por ponto de montagem (4 nconnect x 4 endereços IP).

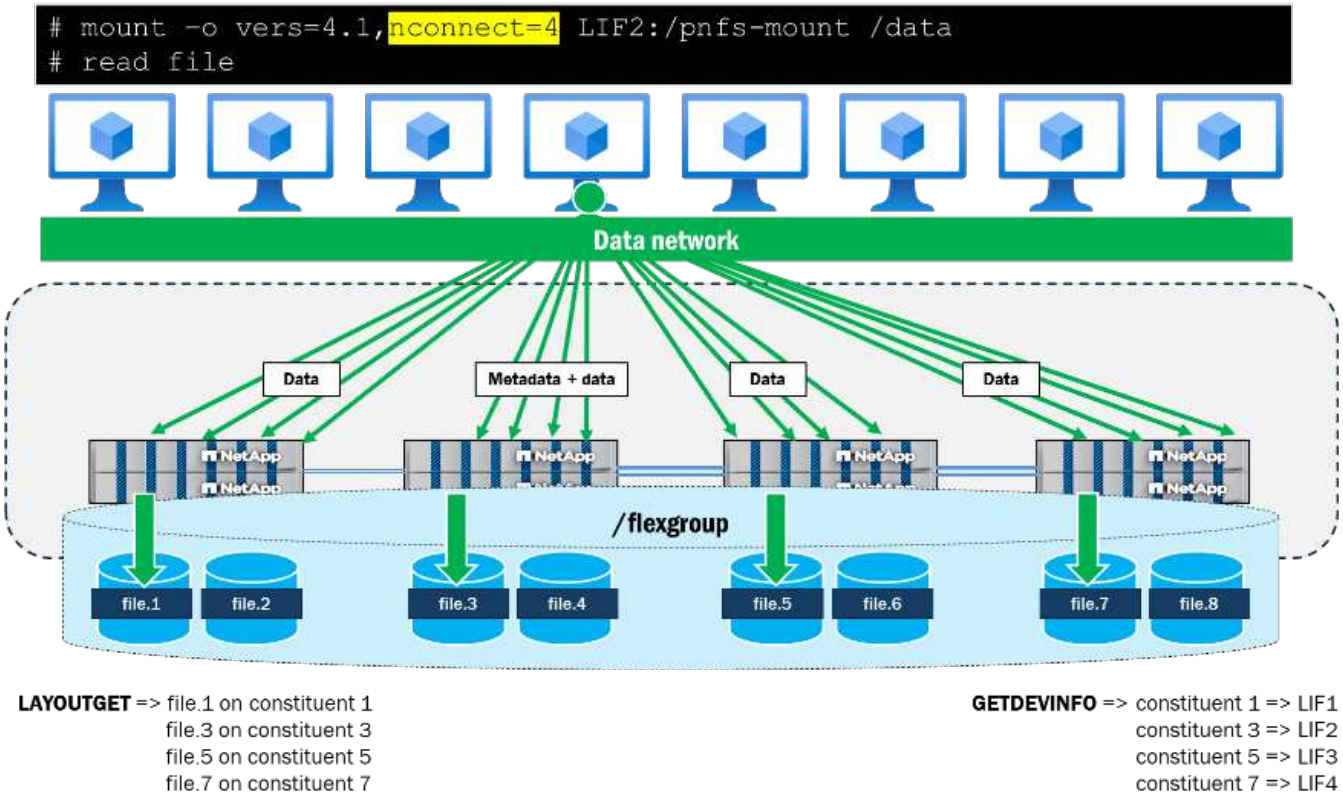


Figura 9. pNFS com nconnect definido para 4

"Saiba mais sobre o suporte do ONTAP para NFSv4.1"

pNFS com trunking de sessão NFSv4.1

Tronco de sessão NFSv4.1 ("RFC 5661, seção 2.10.5") é o uso de múltiplas conexões TCP entre um cliente e um servidor para aumentar a velocidade de transferência de dados. O suporte para trunking de sessão NFSv4.1 foi adicionado ao ONTAP 9.14.1 e deve ser usado com clientes que também suportam trunking de sessão.

No ONTAP, o trunking de sessão pode ser usado em vários nós de um cluster para fornecer maior taxa de transferência e redundância nas conexões.

O trunking de sessão pode ser estabelecido de diversas maneiras:

- **Descobrir automaticamente através de opções de montagem:** O trunking de sessão na maioria dos clientes NFS modernos pode ser estabelecido através de opções de montagem (consulte a documentação do fornecedor do seu sistema operacional) que sinalizam ao servidor NFS para enviar informações de volta ao cliente sobre os trunks de sessão. Esta informação aparece através de um pacote NFS como um `fs_location4` chamar.

  A opção de montagem utilizada depende da versão do sistema operacional do cliente. Por exemplo, as distribuições Linux do Ubuntu geralmente usam `max_connect=n` Para sinalizar que um tronco de sessão deve ser usado. Nas distribuições Linux RHEL, o `trunkdiscovery` A opção de montagem foi utilizada.

  Exemplo do Ubuntu

  ```
  mount -o vers=4.1,max_connect=8 10.10.10.10:/pNFS /mnt/pNFS
  ```

Exemplo de RHEL

```
mount -o vers=4.1,trunkdiscovery 10.10.10.10:/pNFS /mnt/pNFS
```

Se você tentar usar `max_connect` Em distribuições RHEL, será tratado como nconnect e o trunking de sessão não funcionará como esperado.

- **Configuração manual:** Você pode configurar o trunking de sessão manualmente, montando cada endereço IP individual no mesmo caminho de exportação e ponto de montagem. Por exemplo, se você tiver dois endereços IP no mesmo nó (10.10.10.10 e 10.10.10.11) para um caminho de exportação de `/pNFS`Você executa o comando mount duas vezes:

```
mount -o vers=4.1 10.10.10.10:/pNFS /mnt/pNFS
mount -o vers=4.1 10.10.10.11:/pNFS /mnt/pNFS
```

Repita esse processo em todas as interfaces que você deseja que participem do tronco.

Cada nó recebe seu próprio tronco de sessão. Os troncos não atravessam nós.

Ao usar pNFS, utilize apenas o trunking de sessão *ou* nconnect. Utilizar ambos resultará em comportamentos indesejáveis, como apenas a conexão com o servidor de metadados se beneficiar do nConnect, enquanto os servidores de dados utilizam uma única conexão.

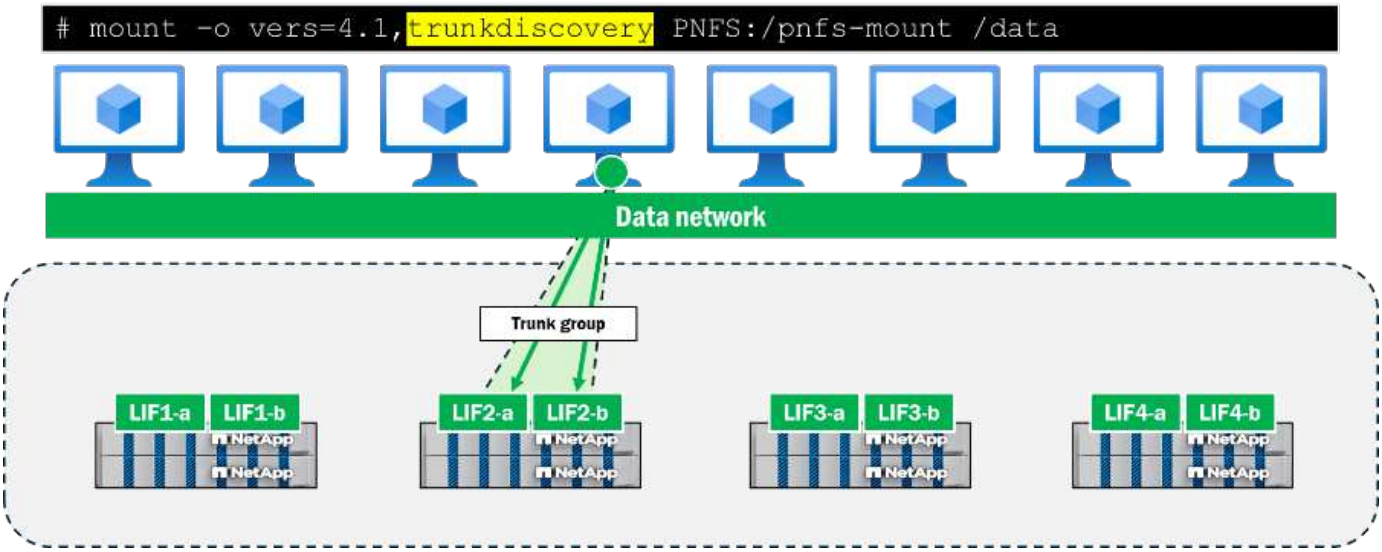
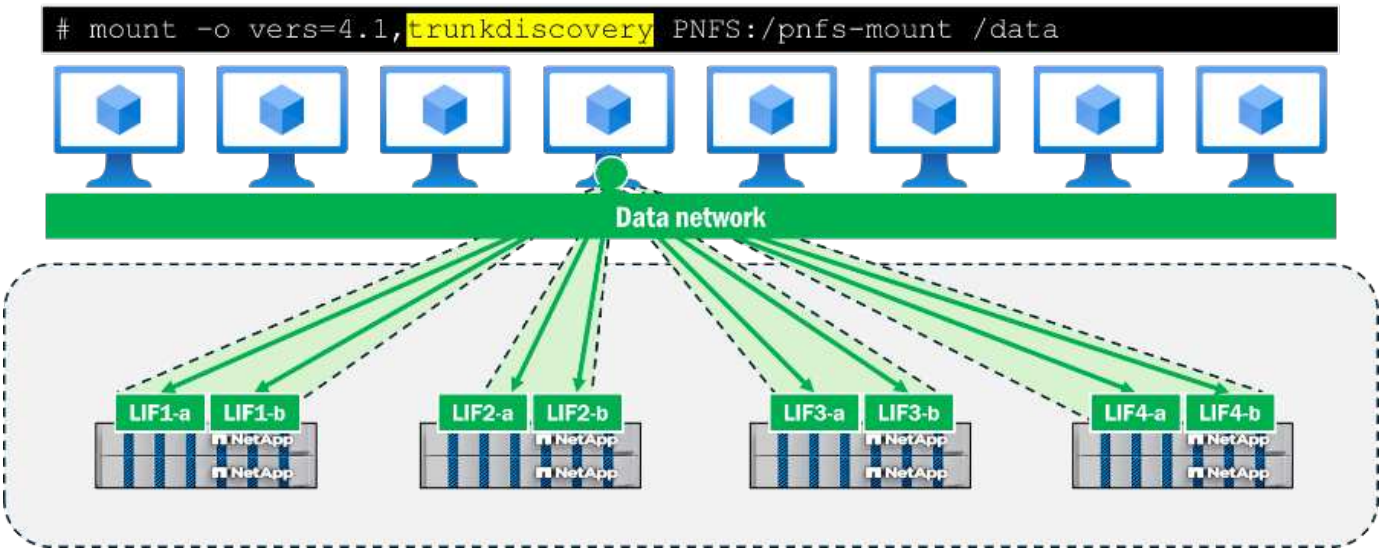


Figura 10. Tronco de sessão NFSv4.1 no ONTAP

O pNFS pode fornecer um caminho local para cada nó participante em um cluster e, quando usado com o trunk de sessão, pode aproveitar um trunk de sessão por nó para maximizar a taxa de transferência de todo o cluster.



Quando `trunkdiscovery` Se utilizado, uma chamada GETATTR adicional (FS_Locations) é aproveitada para as interfaces de tronco de sessão listadas no nó do servidor NFS onde a interface de montagem está localizada. Assim que esses endereços forem devolvidos, as montagens subsequentes serão feitas nos endereços retornados. Isso pode ser observado em uma captura de pacotes durante a montagem.

```
198 1.219372   [redacted]   [redacted]   NFS   246 V4 Call (Reply In 199) GETATTR FH: 0x787f5cf1
199 1.219579   [redacted]   [redacted]   NFS   238 V4 Reply (Call In 198) GETATTR

  Opcode: SEQUENCE (53)
      Status: NFS4_OK (0)
      sessionid: 7100001e004090a90000000000000409
      seqid: 0x00000009
      slot id: 0
      high slot id: 63
      target high slot id: 63
    > status flags: 0x00000000
  Opcode: PUTFH (22)
      Status: NFS4_OK (0)
  Opcode: GETATTR (9)
      Status: NFS4_OK (0)
    Attr mask: 0x01000100 (FSID, FS_Locations)
      reqd_attr: FSID (8)
        > fattr4_fsid
      reco_attr: FS_Locations (24)
        fattr4_fs_locations
            pathname components: 0
          fs_location4
              num: 1
            fs_location4
              servers
                  num: 1
                server: [redacted]
                    length: 14
                    contents: [redacted]
                    fill bytes: opaque data
                pathname components: 0
```

Figura 11. Descoberta do tronco de sessão NFS durante a montagem: captura de pacotes

"Saiba mais sobre o trunking NFS."

Encaminhamentos pNFS versus NFSv4.1

O recurso de encaminhamento NFSv4.1 oferece um modo de redirecionamento inicial do caminho de montagem, direcionando o cliente para a localização dos volumes mediante uma solicitação de montagem. Os encaminhamentos NFSv4.1 funcionam dentro de uma única SVM. Essa funcionalidade tenta localizar a montagem NFS em uma interface de rede que reside no mesmo nó que o volume de dados. Se essa interface ou volume for movido para outro nó enquanto estiver montado em um cliente, o caminho dos dados deixará de ser localizado até que uma nova montagem seja estabelecida.

O pNFS não tenta localizar um caminho de montagem. Em vez disso, ele estabelece um servidor de metadados usando um caminho de montagem e, em seguida, localiza o caminho dos dados dinamicamente, conforme necessário.

É possível usar referências NFSv4.1 com pNFS, mas essa funcionalidade é desnecessária. Habilitar encaminhamentos com pNFS não apresentará resultados perceptíveis.

"Ativar ou desativar encaminhamentos NFSv4"

Interação do pNFS com balanceamento de capacidade avançado

"Balanceamento de capacidade avançado" No ONTAP, partes dos dados do arquivo são gravadas em volumes constituintes de um volume FlexGroup (não é compatível com volumes FlexVol únicos). À medida que um arquivo cresce, o ONTAP decide começar a gravar dados em um novo inode multipart em um volume constituinte diferente, que pode estar no mesmo nó ou em um nó diferente. As operações de escrita, leitura e metadados nesses arquivos multi-inode são transparentes e não interferem no funcionamento dos clientes. O balanceamento avançado de capacidade melhora a gestão do espaço entre os volumes que compõem o FlexGroup , proporcionando um desempenho mais consistente.

O pNFS pode redirecionar a entrada/saída de dados para um caminho de rede localizado, dependendo das informações de layout do arquivo armazenadas no servidor NFS. Quando um único arquivo grande é criado em partes distribuídas por vários volumes constituintes que podem potencialmente abranger vários nós no cluster, o pNFS no ONTAP ainda consegue fornecer tráfego localizado para cada parte do arquivo, pois o ONTAP mantém as informações de layout de todas as partes do arquivo. Ao ler um arquivo, a localidade do caminho de dados será alterada conforme necessário.

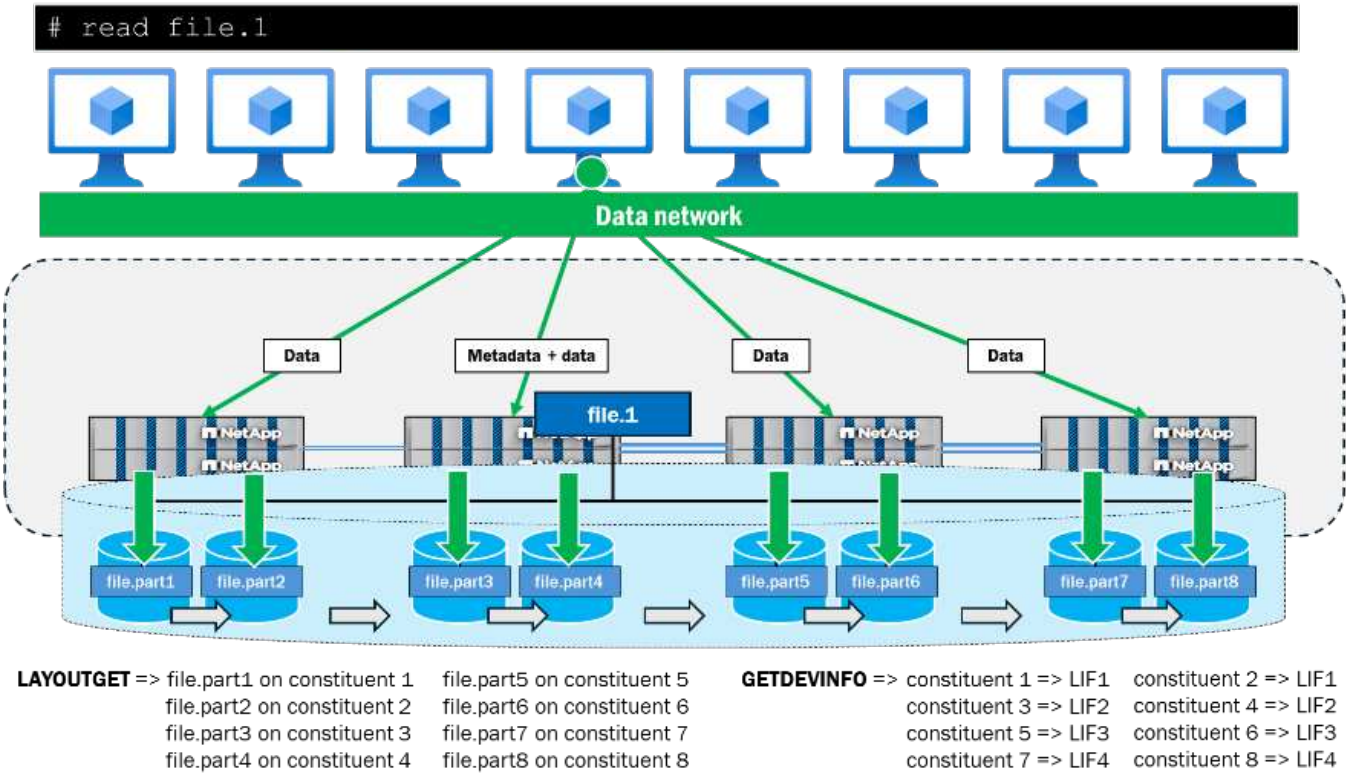


Figura 12. Balanceamento de capacidade avançado com pNFS

Informações relacionadas

- "Configuração de volume FlexGroup"

Estratégia de implantação do pNFS no ONTAP

O pNFS foi introduzido para aprimorar o NFS tradicional, separando os caminhos de metadados e dados, fornecendo localização de dados e permitindo operações paralelas.

Desafios do NFS tradicional e benefícios do pNFS

A tabela a seguir mostra os desafios do NFS tradicional e explica como o pNFS no ONTAP os resolve.

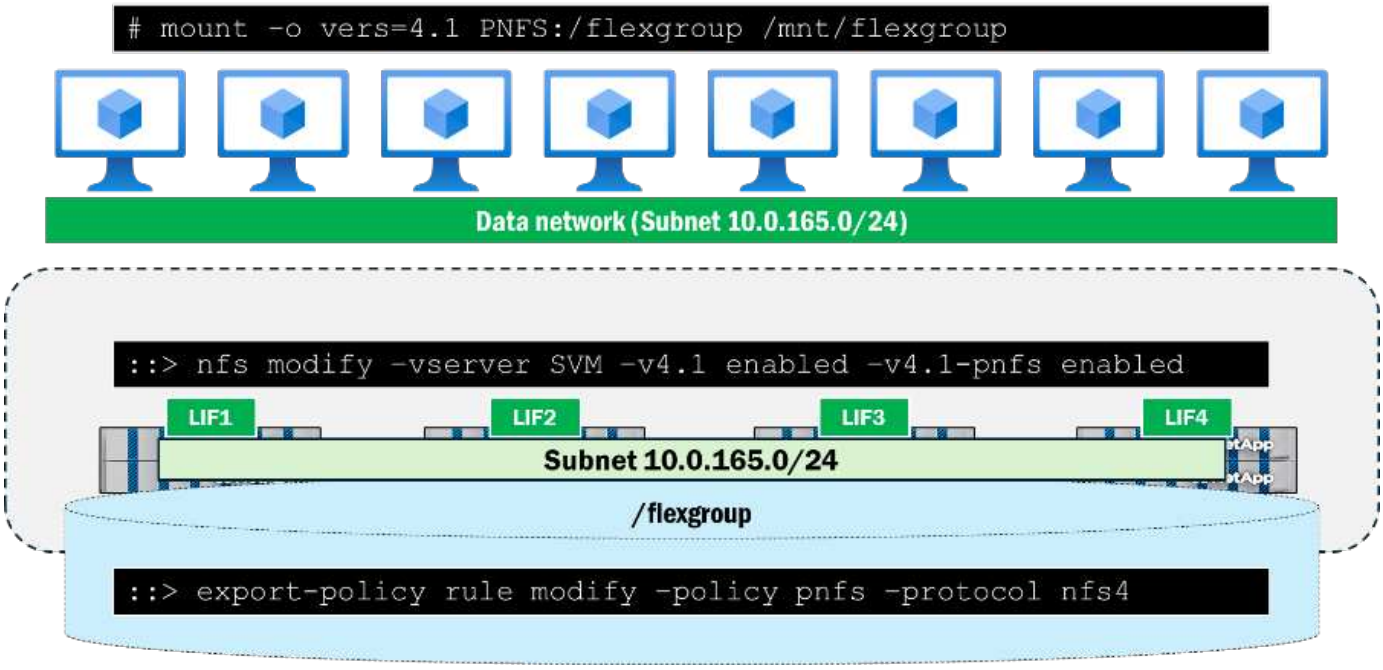
Desafio	benefício pNFS
Mesmo caminho para metadados e dados No NFS tradicional, metadados e dados percorrem o mesmo caminho, o que pode saturar tanto a rede quanto a CPU, já que um único caminho se conecta a um único nó de hardware no cluster. Essa situação se agrava quando muitos usuários tentam acessar a mesma exportação NFS.	**Os caminhos de metadados e de dados são separados, e os caminhos de dados são paralelizados.** Ao separar os caminhos de metadados e de dados para o tráfego NFS e fornecer vários caminhos de rede para os caminhos de dados, os recursos de CPU e de rede são maximizados em um cluster ONTAP , proporcionando assim maior escalabilidade para as cargas de trabalho.

Desafio	benefício pNFS
Desafios de distribuição de carga de trabalho Em um cluster ONTAP NAS, você pode ter até 24 nós, cada um com seu próprio conjunto de volumes de dados e interfaces de rede. Cada volume pode hospedar sua própria carga de trabalho ou um subconjunto dela, e com um volume FlexGroup essa carga de trabalho pode existir em vários nós que acessam um único namespace para maior simplicidade. Quando um cliente monta uma exportação NFS, o tráfego de rede será estabelecido em um único nó. Quando os dados acessados residem em um nó separado no cluster, ocorrerá tráfego remoto, o que pode adicionar latência à carga de trabalho e complexidade à administração.	**Caminhos locais e paralelos para estruturas de dados** Como o pNFS separa os caminhos de dados dos metadados e fornece vários caminhos de dados paralelos dependendo da localidade do volume no cluster, a latência pode ser reduzida diminuindo a distância do tráfego de rede no cluster, bem como aproveitando vários recursos de hardware em um cluster. Além disso, como o pNFS no ONTAP redireciona o tráfego de dados automaticamente, os administradores têm menos necessidade de gerenciar vários caminhos e locais de exportação.
Realocação de pontos de montagem NFS Depois que um ponto de montagem é estabelecido, desmontar e remontar o volume seria problemático. O ONTAP oferece a capacidade de migrar interfaces de rede entre nós, mas isso adiciona sobrecarga de gerenciamento e é disruptivo para conexões NFS com estado usando NFSv4.x. Algumas das razões para a mudança de localização de um ponto de montagem estão relacionadas aos desafios de localização dos dados.	**Realocação automática de caminhos** Com o pNFS, o servidor NFS mantém uma tabela com a localização das interfaces de rede e dos volumes. Quando uma estrutura de dados é solicitada por um cliente através do caminho de metadados no pNFS, o servidor entrega um caminho de rede otimizado ao cliente, que então utiliza esse caminho para operações de dados. Isso reduz drasticamente a sobrecarga de gerenciamento das cargas de trabalho e pode melhorar o desempenho em alguns casos.

Requisitos de configuração

A configuração do pNFS no NetApp ONTAP requer o seguinte:

- Um cliente NFS que suporte pNFS e esteja montado com NFSv4.1 ou posterior.
- NFSv4.1 habilitado no servidor NFS no ONTAP (`nfs modify -v4.1 enabled`(Desativado por padrão)
- pNFS habilitado no servidor NFS no ONTAP (`nfs modify -v4.1-pnfs enabled`(Desativado por padrão)
- Pelo menos uma interface de rede por nó, roteável para os clientes NFS.
- Volumes de dados no SVM que possuem políticas e regras de exportação que permitem NFSv4



Após os requisitos de configuração acima serem atendidos, o pNFS funcionará automaticamente.

Informações relacionadas

- "Configuração NFS"
- "Suporte ONTAP para NFSv4.1"
- "Conectividade da interface de rede para pNFS"

Plano

Plano para implantação do pNFS

Antes de implementar o pNFS em seu ambiente, certifique-se de atender aos pré-requisitos e de compreender os requisitos de interoperabilidade e os limites de configuração.

Pré-requisitos

Antes de habilitar e usar o pNFS no ONTAP, certifique-se de que os seguintes requisitos sejam atendidos:

- O NFSv4.1 ou posterior está habilitado no servidor NFS.
- Pelo menos um "Os dados LIF existem por nó." no cluster para a SVM que hospeda o servidor NFS
- Todos "Os LIFs de dados no SVM são roteáveis." para clientes NFS
- Os clientes NFS suportam pNFS (a maioria das distribuições Linux modernas de 2014 em diante).
- A conectividade de rede entre os clientes e todos os LIFs de dados no SVM está funcional.
- A resolução de DNS (caso utilize nomes de host) está configurada corretamente para todas as LIFs de dados.
- "Volumes FlexGroup" estão configurados (recomendado para melhores resultados)
- "Os domínios de ID do NFSv4.x correspondem" entre clientes e ONTAP

- "NFS Kerberos" (se utilizado) está habilitado em todos os LIFs de dados no SVM.

Resumo das melhores práticas

Ao implementar o pNFS em seu ambiente, siga estas boas práticas:

- Usar "Volumes FlexGroup" para melhor desempenho e escalabilidade de capacidade
- Garanta que todos "As interfaces de rede na SVM são roteáveis." para clientes
- "Desativar NFSv4,0" para garantir que os clientes usem NFSv4.1 ou posterior.
- Distribua os pontos de montagem por várias interfaces e nós de rede.
- Use DNS round robin para "servidores de metadados de balanceamento de carga"
- Verificar "Os domínios de ID do NFSv4.x correspondem" em clientes e servidores
- Conduta "migrações de interface de rede" e "failover de armazenamento" durante os períodos de manutenção
- Habilitar "NFS Kerberos" em todos os LIFs de dados se estiver usando segurança Kerberos
- Evite usar "Encaminhamentos NFSv4.1" ao usar pNFS
- Teste "configurações do nconnect" tenha cuidado para evitar sobrecarregar os limites de conexão TCP.
- Considerar "entroncamento de sessão" como uma alternativa a "nligar" (não use ambos juntos)
- Verificar "suporte do fornecedor do sistema operacional do cliente" para pNFS antes da implantação

Interoperabilidade

O pNFS no ONTAP foi projetado para funcionar com clientes NFS compatíveis com RFC. Aplicam-se as seguintes considerações:

- Mais moderno "Distribuições Linux de 2014 em diante" Suporte a pNFS (RHEL 6.4, Fedora 17 e versões posteriores)
- Verifique com o fornecedor do seu sistema operacional cliente se o pNFS é compatível.
- O pNFS funciona tanto com FlexVol quanto com "Volumes FlexGroup"
- O pNFS é compatível com NFSv4.1 e "NFSv4.2"
- O pNFS pode ser usado com "NFS Kerberos" (krb5, krb5i, krb5p), mas o desempenho pode ser afetado
- O pNFS pode ser usado em conjunto com "nligar" ou "entroncamento de sessão" (mas não ambos simultaneamente)
- pNFS não funciona sobre "NFSv4.0"

Limites

Os seguintes limites se aplicam ao pNFS no ONTAP:

- "limites de conexão TCP" O preço por nó varia conforme a plataforma (consulte o NetApp Hardware Universe para obter os limites específicos).
- Tamanho máximo do arquivo: Depende do tipo de volume e da versão do ONTAP.
- Número máximo de arquivos: até 200 bilhões de arquivos. "Volumes FlexGroup"
- Capacidade máxima: até 60 PB com "Volumes FlexGroup"
- "contagem de interfaces de rede"É necessário pelo menos um LIF de dados por nó; mais podem ser

necessários para balanceamento de carga.

Ao usar "nconnect com pNFS"Esteja ciente de que o número de conexões TCP se multiplica rapidamente:

- Cada cliente montado com nconnect cria múltiplas conexões TCP por LIF de dados.
- Com muitos clientes usando valores altos de nconnect, "limites de conexão TCP" pode ser excedido
- Exceder os limites de conexão TCP impede novas conexões até que as conexões existentes sejam liberadas.

Informações relacionadas

- "Conectividade da interface de rede para pNFS"
- "Habilitar ou desabilitar o NFSv4.1"
- "Suporte ONTAP para NFSv4.1"
- "Suporte ONTAP para NFSv4.2"
- "NetApp Hardware Universe"

Ajuste e melhores práticas de desempenho do pNFS

Ao usar o pNFS no ONTAP, leve em consideração os seguintes pontos e siga as melhores práticas para obter os melhores resultados.

Recomendações de tipo de volume

O pNFS no ONTAP funciona tanto com volumes FlexVol quanto com volumes FlexGroup , mas para obter os melhores resultados gerais, utilize volumes FlexGroup .

Os volumes FlexGroup oferecem:

- Um único ponto de montagem que pode abranger vários recursos de hardware em um cluster, permitindo que o pNFS localize o tráfego de dados.
- Possibilidades de capacidade massivas (até 60 PB) e grande quantidade de arquivos (até 200 bilhões de arquivos).
- Suporte para arquivos multipartes para balanceamento de capacidade e potenciais benefícios de desempenho.
- Acesso paralelo a volumes e hardware que suportam uma única carga de trabalho.

"Saiba mais sobre o gerenciamento de volumes do FlexGroup."

Recomendações de clientes

Nem todos os clientes NFS suportam pNFS, mas a maioria dos clientes modernos sim. O RHEL 6.4 e o Fedora 17 foram os primeiros clientes com suporte a pNFS (aproximadamente em 2014), portanto, é razoável supor que as versões de clientes lançadas nos últimos anos ofereçam suporte completo ao recurso. A posição do ONTAP em relação ao suporte a NFS é a seguinte: "se o cliente suporta o recurso e está em conformidade com o RFC, e nós também suportamos o recurso, então a combinação é suportada." No entanto, é uma boa prática garantir que o pNFS seja suportado pelo fornecedor do sistema operacional do cliente.

Movimentos de volume

O ONTAP oferece a capacidade de mover volumes entre nós ou agregados no mesmo cluster sem

interrupções, proporcionando flexibilidade no equilíbrio entre capacidade e desempenho. Quando ocorre uma movimentação de volume no ONTAP, os mapeamentos de dispositivos pNFS são atualizados automaticamente para informar os clientes a utilizarem a nova relação volume-interface, se necessário.

"Aprenda sobre como mover um volume"

Migração de interface de rede

O ONTAP oferece a capacidade de mover interfaces de rede entre nós no mesmo cluster para proporcionar equilíbrio de desempenho e flexibilidade de manutenção. Assim como ocorre com as movimentações de volume, quando uma migração de interface de rede acontece no ONTAP, os mapeamentos de dispositivos pNFS são atualizados automaticamente para informar os clientes a utilizarem a nova relação volume-interface, se necessário.

No entanto, como o NFSv4.1 é um protocolo com estado, uma migração de interface de rede pode ser disruptiva para clientes que estejam usando ativamente a montagem NFS. É uma boa prática realizar migrações de interfaces de rede durante uma janela de manutenção e notificar os clientes sobre possíveis interrupções na rede.

Falhas/devoluções de armazenamento

O pNFS segue as mesmas considerações de failover de armazenamento que o NFSv4.1. Esses tópicos são abordados em detalhes em "Relatório técnico da NetApp 4067: Guia de práticas recomendadas e implementação de NFS"Em geral, qualquer failover/devolução de armazenamento envolvendo pNFS deve ser feito em uma janela de manutenção, com possíveis interrupções de armazenamento esperadas devido à natureza de estado do protocolo.

Cargas de trabalho de metadados

As operações de metadados são pequenas em tamanho e podem ser grandes em número, dependendo da carga de trabalho (Você está criando um grande número de arquivos? Você está executando comandos "find"?) e contagem total de arquivos. Consequentemente, cargas de trabalho com grande número de chamadas de metadados podem sobrecarregar a CPU do servidor NFS e potencialmente causar gargalos em uma única conexão. O pNFS (e o NFSv4.x em geral) não é adequado para cargas de trabalho com alto volume de metadados que exigem alto desempenho, pois a natureza stateful, os mecanismos de bloqueio e alguns dos recursos de segurança dessa versão do protocolo podem impactar negativamente a utilização da CPU e a latência. Esses tipos de carga de trabalho (como GETATTR ou SETATTR de alta frequência) geralmente têm um desempenho melhor com NFSv3.

Servidor de metadados

O servidor de metadados no pNFS é estabelecido na montagem inicial de uma exportação NFS. Uma vez estabelecido o ponto de montagem, ele permanece no local até ser remontado ou a interface de dados ser movida. Por isso, é uma boa prática garantir que vários clientes que acessam o mesmo volume o montem em nós e interfaces de dados diferentes na SVM. Essa abordagem proporciona balanceamento de carga dos servidores de metadados entre os nós e os recursos de CPU, ao mesmo tempo que maximiza as interfaces de rede no cluster. Uma maneira de fazer isso é estabelecer uma configuração de DNS round robin, que é abordada em [referência omitida]. "Relatório Técnico 4523 da NetApp : Balanceamento de Carga de DNS no ONTAP".

Domínios de ID NFSv4.x

O NFSv4.x oferece funcionalidades de segurança de diversas maneiras (abordadas em detalhes em "Relatório técnico da NetApp 4067: Guia de práticas recomendadas e implementação de NFS"). Os domínios de ID do NFSv4.x são uma dessas maneiras, em que um cliente e um servidor devem concordar com os

domínios de ID ao tentar autenticar usuários e grupos em uma exportação NFS. Um dos efeitos colaterais de uma incompatibilidade de domínio de ID seria o usuário ou grupo aparecer como um usuário anonimizado (essencialmente suprimido) para evitar acesso indesejado. Com o NFSv4.x (e também com o pNFS), é uma boa prática garantir que os domínios de ID do NFSv4.x correspondam no cliente e no servidor.

nligar

Conforme mencionado anteriormente, o nconnect no ONTAP pode ajudar a melhorar o desempenho em algumas cargas de trabalho. Com o pNFS, é importante entender que, embora o nconnect possa melhorar o desempenho aumentando consideravelmente o número total de conexões TCP com o sistema de armazenamento, ele também pode criar problemas quando muitos clientes utilizam a opção de montagem, sobrecarregando as conexões TCP no armazenamento. O NetApp Hardware Universe aborda os limites de conexão TCP por nó.

Quando os limites de conexão TCP de um nó são excedidos, nenhuma nova conexão TCP é permitida até que as conexões existentes sejam liberadas. Isso pode criar complicações em ambientes que podem sofrer tempestades de montanha.

A tabela a seguir mostra como o pNFS com nconnect pode sobrecarregar os limites de conexão TCP:

Contagem de clientes	valor nconnect	Total de conexões TCP potenciais por montagem, por nó.
1	4	4
100	4	400
1000	8	8000
10000	8	80000
10000	16	160000 [1]

[1] Excede a maioria dos limites de conexão TCP de nó único do ONTAP

Entroncamento de sessão NFSv4,1

O trunking de sessão no ONTAP pode ser usado para aumentar a taxa de transferência e a resiliência do caminho para montagens NFSv4.x. Quando usado com pNFS, cada nó em um cluster pode estabelecer um tronco de sessão. No entanto, os troncos de sessão exigem pelo menos duas interfaces por nó, e o pNFS exige pelo menos uma interface por nó para funcionar conforme o esperado. Além disso, todas as interfaces na SVM devem ser roteáveis para os clientes NFS. O trunking de sessão e o pNFS não funcionam corretamente quando se utiliza também o nconnect. Considere o nConnect e o trunking de sessão como funcionalidades mutuamente exclusivas.

"Aprenda sobre trunking NFS"

Conectividade da interface de rede

Para funcionar corretamente, o pNFS requer uma interface de rede roteável em cada nó do cluster. Se existirem outras interfaces de rede que não sejam roteáveis para clientes NFS na mesma SVM que o servidor NFS que hospeda o pNFS, o ONTAP ainda anunciará essas interfaces no mapeamento de dispositivos para os clientes. Quando o cliente NFS tenta acessar dados por meio de interfaces em uma sub-rede diferente, ele não conseguirá se conectar, o que causará uma interrupção. É uma boa prática permitir em uma SVM apenas as interfaces de rede que podem ser acessadas pelos clientes ao usar pNFS.

Por padrão, o pNFS exige que qualquer LIF de dados na SVM seja roteável para interfaces nos clientes NFS, pois as listas de dispositivos pNFS serão preenchidas com qualquer LIF de dados na SVM. Como resultado, podem ser selecionadas LIFs de dados não roteáveis, o que pode gerar cenários de interrupção. Como prática recomendada, configure LIFs de dados roteáveis somente ao usar pNFS.

A partir do ONTAP 9.18.1 RC1 e versões posteriores, é possível especificar quais interfaces são elegíveis para tráfego pNFS por sub-rede, permitindo a combinação de interfaces roteáveis e não roteáveis. Para obter informações sobre os comandos, entre em contato com o suporte da NetApp .

NFSv4.0

O NFSv4.0 é uma opção que pode ser habilitada em um servidor ONTAP NFS juntamente com o NFSv4.1. No entanto, o pNFS não funciona com NFSv4.0. Se o NFSv4.0 estiver habilitado no servidor NFS, os clientes podem, potencialmente, montar essa versão do protocolo sem saber e não poderão aproveitar o pNFS. Consequentemente, a melhor prática é desativar explicitamente o NFSv4.0 ao usar o pNFS. O NFSv4.1 ainda precisa estar habilitado e pode funcionar independentemente do NFSv4.0.

Encaminhamentos NFSv4.1

O NFSv4.1 encaminha o caminho de montagem de um cliente para a interface de rede no nó que possui um volume. O pNFS localiza o caminho de dados, e o caminho de montagem se torna um servidor de metadados.

Embora seja possível usar os dois recursos em conjunto, o uso de referências NFSv4.1 com pNFS pode resultar no efeito indesejado de empilhar vários servidores de metadados no mesmo nó e reduzir a capacidade de distribuir os servidores de metadados por vários nós do cluster. Se os servidores de metadados não estiverem distribuídos uniformemente em um cluster ao usar o pNFS, a CPU de um único nó pode ficar sobrecarregada com solicitações de metadados, criando um gargalo de desempenho.

Sendo assim, é uma boa prática evitar o uso de referências NFSv4.1 ao usar pNFS. Em vez disso, distribua os pontos de montagem por várias interfaces de rede e nós no cluster.

"Saiba mais sobre como ativar ou desativar encaminhamentos NFSv4."

NFS Kerberos

Com o NFS Kerberos, é possível criptografar a autenticação com krb5 e criptografar ainda mais os pacotes de dados com krb5i e krb5p. Isso é habilitado por interface de rede em uma SVM e é abordado em detalhes em "Relatório técnico do NetApp 4616: Kerberos NFS no ONTAP com o Microsoft ative Directory".

Como o pNFS pode redirecionar o tráfego de dados entre nós e interfaces de rede na SVM, o NFS Kerberos deve estar habilitado e funcionando em cada interface de rede da SVM. Se alguma interface de rede na SVM não estiver habilitada para Kerberos, o pNFS não funcionará corretamente ao tentar acessar volumes de dados nessas interfaces.

Por exemplo, ao executar um teste de leitura usando o comando dd paralelo em uma SVM com pNFS habilitado e duas interfaces de rede (apenas uma habilitada para Kerberos), os arquivos localizados na interface com Kerberos habilitado apresentaram bom desempenho, enquanto os arquivos no nó com a interface sem Kerberos habilitado nunca conseguiram concluir suas leituras. Com o Kerberos ativado em ambas as interfaces, todos os arquivos funcionaram conforme o esperado.

O NFS Kerberos pode ser usado com o pNFS, desde que o NFS Kerberos esteja habilitado em todas as interfaces de rede da SVM. Lembre-se de que o NFS Kerberos pode acarretar uma perda de desempenho devido à criptografia/descriptografia dos pacotes. Portanto, é uma boa prática testar o pNFS com NFS

Kerberos minuciosamente com suas cargas de trabalho para garantir que qualquer impacto no desempenho não seja excessivo.

Abaixo, segue um exemplo do desempenho de leitura paralela ao usar krb5 (autenticação) e krb5p (criptografia de ponta a ponta) com pNFS em um cliente RHEL 9.5. Neste teste, o Krb5p apresentou uma degradação de desempenho de 70%.

Sabor Kerberos	MB/s	Tempo de conclusão
krb5	• File1-243 • File2-243 • File3-238 • File4-238	• File1-43 • File2-43,1 • File3-44 • File4-44,1
krb5p	• File1-72,9 • File2-72,8 • File3-71,4 • File4-71,2	• File1-143,9 • File2-144,1 • File3-146,9 • File4-147,3

"Aprenda sobre Kerberos com NFS para uma segurança robusta."

NFSv4.2

O NFSv4.2 foi adicionado ao ONTAP 9.8 e é a versão mais recente do NFSv4.x disponível (RFC-7862). O NFSv4.2 não possui uma opção explícita para habilitá-lo/desabilitá-lo. Em vez disso, ele é ativado/desativado juntamente com o NFSv4.1. (`-4.1 enabled`). Se um cliente suporta NFSv4.2, ele negociará a versão mais recente do NFS suportada durante o comando de montagem, a menos que seja especificado o contrário. `minorversion=2` opção de montagem.

O NFSv4.2 no ONTAP suporta as seguintes funcionalidades:

- Etiquetas de segurança (etiquetas MAC)
- Atributos estendidos
- Operações de arquivo esparsas (FALLOCATE)

O pNFS foi introduzido com o NFSv4.1, mas também é compatível com o NFSv4.2, assim como com seus recursos complementares.

"Saiba mais sobre o suporte ONTAP para NFSv4.2"

Comandos pNFS, estatísticas e registros de eventos

Esses comandos da CLI do ONTAP referem-se especificamente ao pNFS. Você pode usá-los para configurar, solucionar problemas e coletar estatísticas.

Ativar NFSv4.1

```
nfs modify -vserver SVM -v4.1 enabled
```

Ativar pNFS

```
nfs modify -vserver SVM -v4.1-pnfs enabled
```

Exibir dispositivos pNFS (privilégios avançados)

```
pnfs devices show -vserver SVM
```

```
Vserver Name     Mapping ID      Volume MSID     Mapping Status
Generation
---------------  --------------- --------------- ---------------
-------------
SVM              17              2157024470      notavailable    2
SVM              18              2157024463      notavailable    2
SVM              19              2157024469      available       3
SVM              20              2157024465      available       4
SVM              21              2157024467      available       3
SVM              22              2157024462      available       1
```

Exibir mapeamentos de dispositivos pNFS (privilégios avançados)

```
pnfs devices mappings show -vserver SVM
```

```
Vserver Name    Mapping ID      Dsid            LIF IP
--------------  --------------- --------------- --------------------
SVM             19              2449            10.x.x.x
SVM             20              2512            10.x.x.y
SVM             21              2447            10.x.x.x
SVM             22              2442            10.x.x.y
```

Capturar contadores de desempenho específicos do pNFS (privilégios avançados)

```
statistics start -object nfsv4_1 -vserver SVM -sample-id [optional-name]
```

Visualizar contadores de desempenho específicos do pNFS (privilégios avançados)

```
statistics show -object nfsv4_1 -vserver SVM
```

Veja a lista de contadores específicos do pNFS (privilégios avançados)

```
statistics catalog counter show -object nfsv4_1 -counter *layout*|*device*
```

```
Object: nfsv4_1

Counter                     Description
--------------------------- ----------------------------------------------
getdeviceinfo_avg_latency   Average latency of NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_error         The number of failed NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_percent       Percentage of NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_success       The number of successful NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_total         Total number of NFSv4.1 GETDEVICEINFO
operations.
getdevicelist_avg_latency   Average latency of NFSv4.1 GETDEVICELIST
operations.
getdevicelist_error         The number of failed NFSv4.1 GETDEVICELIST
operations.
getdevicelist_percent       Percentage of NFSv4.1 GETDEVICELIST
operations.
getdevicelist_success       The number of successful NFSv4.1 GETDEVICELIST
operations.
getdevicelist_total         Total number of NFSv4.1 GETDEVICELIST
operations.
layoutcommit_avg_latency    Average latency of NFSv4.1 LAYOUTCOMMIT
operations.
layoutcommit_error          The number of failed NFSv4.1 LAYOUTCOMMIT
operations.
layoutcommit_percent        Percentage of NFSv4.1 LAYOUTCOMMIT operations.
layoutcommit_success        The number of successful NFSv4.1 LAYOUTCOMMIT
operations.
layoutcommit_total          Total number of NFSv4.1 LAYOUTCOMMIT
operations.
layoutget_avg_latency       Average latency of NFSv4.1 LAYOUTGET
operations.
layoutget_error             The number of failed NFSv4.1 LAYOUTGET
operations.
layoutget_percent           Percentage of NFSv4.1 LAYOUTGET operations.
layoutget_success           The number of successful NFSv4.1 LAYOUTGET
operations.
layoutget_total             Total number of NFSv4.1 LAYOUTGET operations.
```

```
layoutreturn_avg_latency    Average latency of NFSv4.1 LAYOUTRETURN
operations.
layoutreturn_error          The number of failed NFSv4.1 LAYOUTRETURN
operations.
layoutreturn_percent        Percentage of NFSv4.1 LAYOUTRETURN operations.
layoutreturn_success        The number of successful NFSv4.1 LAYOUTRETURN
operations.
layoutreturn_total          Total number of NFSv4.1 LAYOUTRETURN
operations.
```

Visualizar conexões de rede ativas para NFS

Você pode verificar se várias conexões TCP estão sendo feitas com a SVM usando o `network connections active show` comando.

Por exemplo, se você quiser visualizar os troncos de sessão NFS, procure por conexões dos mesmos clientes em diferentes interfaces por nó:

```
cluster::*> network connections active show -node cluster-0* -vserver PNFS
              Vserver   Interface         Remote
      CID Ctx Name      Name:Local Port   Host:Port
Protocol/Service
--------- --- --------- ----------------- --------------------
----------------
Node: node-01
2304333128 14 PNFS      data1:2049        ubuntu22-224:740     TCP/nfs
2304333144 10 PNFS      data3:2049        ubuntu22-224:864     TCP/nfs
2304333151  5 PNFS      data1:2049        ubuntu22-226:848     TCP/nfs
2304333167 15 PNFS      data3:2049        ubuntu22-226:684     TCP/nfs
Node: node-02
2497668321 12 PNFS      data2:2049        ubuntu22-224:963     TCP/nfs
2497668337 18 PNFS      data4:2049        ubuntu22-224:859     TCP/nfs
2497668344 14 PNFS      data2:2049        ubuntu22-226:675     TCP/nfs
2497668360  7 PNFS      data4:2049        ubuntu22-226:903     TCP/nfs
```

Exibir informações da versão NFS para clientes conectados

Você também pode visualizar conexões NFS com o `nfs connected-clients show` comando. Lembre-se de que a lista de clientes exibida inclui aqueles que tiveram tráfego NFS ativo nas últimas 48 horas. Clientes NFS ociosos (mesmo que ainda estejam montados) podem não aparecer até que o ponto de montagem seja acessado. Você pode filtrar esses resultados para exibir apenas os clientes acessados mais recentemente, especificando o `-idle-time` recurso.

Por exemplo, para visualizar os clientes com atividade nos últimos 10 minutos para o pNFS SVM:

```
cluster::*> nfs connected-clients show -vserver PNFS -idle-time <10m>

 Node: node-01

Vserver: PNFS Data-Ip: 10.x.x.x Local Remote Client-Ip Protocol Volume
Policy Idle-Time Reqs Reqs Trunking

10.x.x.a nfs4.2 PNFS_root default 9m 10s 0 149 false 10.x.x.a nfs4.2
FG_0001 default 9m 10s 135847 0 false 10.x.x.b nfs4.2 PNFS_root default 8m
12s 0 157 false 10.x.x.b nfs4.2 FG_0001 default 8m 12s 52111 0 false
```

Informações relacionadas

- "Saiba mais sobre NFS paralelo (pNFS) no ONTAP."

Dependências de nomes de arquivos e diretórios NFS e SMB

Aprenda sobre dependências de nomenclatura de arquivos e diretórios ONTAP NFS e SMB

As convenções de nomenclatura de arquivos e diretórios dependem tanto dos sistemas operacionais dos clientes de rede quanto dos protocolos de compartilhamento de arquivos, além das configurações de idioma do cluster e dos clientes do ONTAP.

O sistema operacional e os protocolos de compartilhamento de arquivos determinam o seguinte:

- Carateres que um nome de arquivo pode usar
- Sensibilidade em caso de um nome de ficheiro

O ONTAP suporta carateres multibyte em nomes de arquivo, diretório e qtree, dependendo da versão do ONTAP.

Aprenda sobre caracteres válidos em diferentes sistemas operacionais para SVMs ONTAP NFS

Se você estiver acessando um arquivo ou diretório de clientes com sistemas operacionais diferentes, use carateres válidos em ambos os sistemas operacionais.

Por exemplo, se você usar UNIX para criar um arquivo ou diretório, não use dois pontos (:) no nome porque os dois pontos não são permitidos em nomes de arquivo ou diretório MS-dos. Como as restrições em carateres válidos variam de um sistema operacional para outro, consulte a documentação do sistema operacional cliente para obter mais informações sobre carateres proibidos.

Aprenda sobre a diferenciação entre maiúsculas e minúsculas de nomes de arquivos e diretórios em um ambiente multiprotocolo ONTAP NFS

Os nomes de arquivos e diretórios são sensíveis a maiúsculas e minúsculas para

clientes NFS, mas que preservam casos para clientes SMB. Você deve entender quais são as implicações em um ambiente multiprotocolo e as ações que pode precisar tomar ao especificar o caminho ao criar compartilhamentos SMB e ao acessar dados nos compartilhamentos.

Se um cliente SMB criar um diretório `testdir` chamado , os clientes SMB e NFS exibirão o nome do arquivo como `testdir`. No entanto, se um usuário SMB tentar criar um nome de diretório mais tarde `TESTDIR` , o nome não será permitido porque, para o cliente SMB, esse nome existe atualmente. Se um usuário NFS criar posteriormente um diretório `TESTDIR` chamado , clientes NFS e SMB exibirão o nome do diretório de maneira diferente, da seguinte forma:

- Em clientes NFS, você verá ambos os nomes de diretório à medida que foram criados, por `testdir` exemplo e `TESTDIR`, porque os nomes de diretório são sensíveis a maiúsculas e minúsculas.
- Os clientes SMB usam os nomes 8,3 para distinguir entre os dois diretórios. Um diretório tem o nome do arquivo base. Os diretórios adicionais recebem um nome de arquivo 8,3.
  - Em clientes SMB, você verá `testdir` e `TESTDI~1`.
  - O ONTAP cria o `TESTDI~1` nome do diretório para diferenciar os dois diretórios.

    Nesse caso, você deve usar o nome 8,3 ao especificar um caminho de compartilhamento ao criar ou modificar um compartilhamento em uma máquina virtual de storage (SVM).

Da mesma forma para arquivos, se um cliente SMB criar `test.txt`, os clientes SMB e NFS exibirão o nome do arquivo como `text.txt`. No entanto, se um usuário SMB tentar criar mais tarde `Test.txt` , o nome não será permitido porque, para o cliente SMB, esse nome existe atualmente. Se um usuário NFS criar mais tarde um arquivo `Test.txt` chamado , clientes NFS e SMB exibirão o nome do arquivo de forma diferente, da seguinte forma:

- Em clientes NFS, você verá ambos os nomes de arquivos à medida que foram criados e `test.txt` `Test.txt` , porque os nomes de arquivos são sensíveis a maiúsculas e minúsculas.
- Os clientes SMB usam os nomes 8,3 para distinguir entre os dois arquivos. Um arquivo tem o nome do arquivo base. Os ficheiros adicionais recebem um nome de ficheiro 8,3.
  - Em clientes SMB, você verá `test.txt` e `TEST~1.TXT`.
  - O ONTAP cria o `TEST~1.TXT` nome do arquivo para diferenciar os dois arquivos.

> Se um mapeamento de carateres tiver sido criado usando os comandos SVM CIFS de mapeamento de carateres, uma pesquisa do Windows que normalmente seria insensível a maiúsculas e minúsculas pode se tornar sensível a maiúsculas e minúsculas. Isso significa que as pesquisas de nome de arquivo só serão sensíveis a maiúsculas e minúsculas se o mapeamento de carateres tiver sido criado e o nome de arquivo estiver usando esse mapeamento de carateres.

Aprenda sobre como criar nomes de arquivos e diretórios NFS do ONTAP

O ONTAP cria e mantém dois nomes para arquivos ou diretórios em qualquer diretório que tenha acesso de um cliente SMB: O nome longo original e um nome no formato 8,3.

Para nomes de arquivo ou diretório que excedam o nome de oito carateres ou o limite de extensão de três carateres (para arquivos), o ONTAP gera um nome de formato 8,3 da seguinte forma:

- Ele trunca o nome do arquivo ou diretório original para seis carateres, se o nome exceder seis carateres.
- Ele adiciona um til (…) e um número, um a cinco, aos nomes de arquivo ou diretório que não são mais exclusivos depois de serem truncados.

  Se ele ficar sem números porque há mais de cinco nomes semelhantes, ele cria um nome exclusivo que não tem relação com o nome original.

- No caso dos arquivos, ele trunca a extensão do nome do arquivo para três carateres.

Por exemplo, se um cliente NFS criar um arquivo chamado `specifications.html`, o nome do arquivo de formato 8,3 criado pelo ONTAP será `specif~1.htm`. Se esse nome já existir, o ONTAP usará um número diferente no final do nome do arquivo. Por exemplo, se um cliente NFS criar outro arquivo chamado `specifications_new.html`, o formato 8,3 do `specifications_new.html` é `specif~2.htm`.

Aprenda sobre o tratamento de nomes de arquivos, diretórios e qtrees multibyte do ONTAP NFS

Começando com ONTAP 9.5, o suporte para nomes codificados UTF-8 de 4 bytes permite a criação e exibição de nomes de arquivos, diretórios e árvores que incluem carateres suplementares Unicode fora do plano multilíngue básico (BMP). Em versões anteriores, esses carateres suplementares não foram exibidos corretamente em ambientes multiprotocolo.

Para ativar o suporte para nomes codificados UTF-8 de 4 bytes, um novo código de linguagem *utf8mb4* está disponível para as `vserver` famílias de comandos e `volume` .

- Você deve criar um novo volume de uma das seguintes maneiras:
- Definir a opção de volume `-language` explicitamente:

  ```
  volume create -language utf8mb4 {…}
  ```

- Herdando a opção de volume `-language` de uma SVM que foi criada ou modificada para a opção:

  ```
  vserver [create|modify] -language utf8mb4 {…}``volume create {…}
  ```

- Se você estiver usando o ONTAP 9.6 e anteriores, não será possível modificar volumes existentes para suporte a utf8mb4; você deve criar um novo volume pronto para utf8mb4 e migrar os dados usando ferramentas de cópia baseadas em cliente.

  Se você estiver usando o ONTAP 9.7P1 ou posterior, poderá modificar volumes existentes para o utf8mb4 com uma solicitação de suporte. Para obter mais informações, "O idioma do volume pode ser alterado após a criação no ONTAP?"consulte .

Você pode atualizar SVMs para suporte a utf8mb4, mas os volumes existentes mantêm seus códigos de idioma originais.

E

Nomes LUN com carateres UTF-8 de 4 bytes não são suportados atualmente.

- Os dados de carateres Unicode são normalmente representados em aplicações de sistemas de ficheiros

Windows utilizando o formato de transformação Unicode de 16 bits (UTF-16) e em sistemas de ficheiros NFS utilizando o formato de transformação Unicode de 8 bits (UTF-8).

Em versões anteriores ao ONTAP 9.5, nomes incluindo carateres suplementares UTF-16 que foram criados por clientes Windows foram exibidos corretamente para outros clientes Windows, mas não foram traduzidos corretamente para UTF-8 para clientes NFS. Da mesma forma, nomes com carateres suplementares UTF-8 por clientes NFS criados não foram traduzidos corretamente para UTF-16 para clientes Windows.

- Quando você cria nomes de arquivo em sistemas que executam o ONTAP 9.4 ou anteriores que contêm carateres suplementares válidos ou inválidos, o ONTAP rejeita o nome do arquivo e retorna um erro de nome de arquivo inválido.

  Para evitar esse problema, use apenas carateres BMP em nomes de arquivo e evite usar carateres suplementares ou atualize para o ONTAP 9.5 ou posterior.

Carateres Unicode são permitidos em nomes de qtree.

- Você pode usar a `volume qtree` família de comandos ou o System Manager para definir ou modificar nomes de qtree.
- Os nomes de qtree podem incluir carateres de vários bytes no formato Unicode, como carateres japoneses e chineses.
- Em versões anteriores ao ONTAP 9.5, apenas os carateres BMP (ou seja, aqueles que poderiam ser representados em 3 bytes) foram suportados.

  Em versões anteriores ao ONTAP 9.5, o caminho de junção do volume pai da qtree pode conter nomes de qtree e diretório com carateres Unicode. O `volume show` comando exibe esses nomes corretamente quando o volume pai tem uma configuração de idioma UTF-8. No entanto, se o idioma do volume pai não for uma das configurações de idioma UTF-8, algumas partes do caminho de junção serão exibidas usando um nome alternativo NFS numérico.

- Em versões 9,5 e posteriores, os carateres de 4 bytes são suportados em nomes de qtree, desde que a qtree esteja em um volume habilitado para utf8mb4.

Configurar mapeamento de caracteres para tradução de nome de arquivo SMB em volumes ONTAP NFS

Os clientes NFS podem criar nomes de arquivos que contêm carateres que não são válidos para clientes SMB e determinados aplicativos do Windows. Você pode configurar o mapeamento de carateres para a tradução de nome de arquivo em volumes para permitir que clientes SMB acessem arquivos com nomes NFS que, de outra forma, não seriam válidos.

Sobre esta tarefa

Quando os arquivos criados por clientes NFS são acessados por clientes SMB, o ONTAP examina o nome do arquivo. Se o nome não for um nome de arquivo SMB válido (por exemplo, se ele tiver um caractere de dois pontos "':'" incorporado), o ONTAP retornará o nome de arquivo 8,3 que é mantido para cada arquivo. No entanto, isso causa problemas para aplicativos que codificam informações importantes em nomes de arquivos longos.

Portanto, se você estiver compartilhando um arquivo entre clientes em sistemas operacionais diferentes, você deve usar carateres nos nomes de arquivo que são válidos em ambos os sistemas operacionais.

No entanto, se você tiver clientes NFS que criam nomes de arquivo contendo carateres que não são nomes de arquivo válidos para clientes SMB, você poderá definir um mapa que converte os carateres NFS inválidos em carateres Unicode que tanto SMB quanto determinados aplicativos do Windows aceitam. Por exemplo, essa funcionalidade suporta os aplicativos CATIA MCAD e Mathematica, bem como outros aplicativos que têm esse requisito.

Você pode configurar o mapeamento de carateres em uma base volume por volume.

Você deve ter em mente o seguinte ao configurar o mapeamento de carateres em um volume:

- O mapeamento de carateres não é aplicado em pontos de junção.

  Você deve configurar explicitamente o mapeamento de carateres para cada volume de junção.

- Você deve certificar-se de que os carateres Unicode que são usados para representar carateres inválidos ou ilegais são carateres que normalmente não aparecem em nomes de arquivos; caso contrário, mapeamentos indesejados ocorrem.

  Por exemplo, se você tentar mapear dois pontos (:) para um hífen (-), mas o hífen (-) foi usado no nome do arquivo corretamente, um cliente Windows tentando acessar um arquivo chamado "'a-b'" teria sua solicitação mapeada para o nome NFS de "'a:b'" (não o resultado desejado).

- Depois de aplicar o mapeamento de carateres, se o mapeamento ainda contiver um caractere Windows inválido, o ONTAP volta para os nomes de arquivos do Windows 8,3.
- Em notificações FPolicy, logs de auditoria nas e mensagens de rastreamento de segurança, os nomes de arquivo mapeados são exibidos.
- Quando uma relação SnapMirror do tipo DP é criada, o mapeamento de carateres do volume de origem não é replicado no volume DP de destino.
- Sensibilidade do caso: Como os nomes mapeados do Windows se transformam em nomes NFS, a pesquisa dos nomes segue semântica de NFS. Isso inclui o fato de que pesquisas NFS são sensíveis a maiúsculas e minúsculas. Isso significa que os aplicativos que acessam compartilhamentos mapeados não devem depender de comportamento insensível a maiúsculas e minúsculas do Windows. No entanto, o nome 8,3 está disponível, e isso é insensível a maiúsculas e minúsculas.
- Mapeamentos parciais ou inválidos: Depois de mapear um nome para retornar aos clientes fazendo enumeração de diretórios ("dir"), o nome Unicode resultante é verificado para a validade do Windows. Se esse nome ainda tiver carateres inválidos nele, ou se for inválido para o Windows (por exemplo, termina em "." ou em branco), o nome 8,3 será retornado em vez do nome inválido.

Passo

1. Configurar mapeamento de carateres:

   ```
   vserver cifs character-mapping create -vserver vserver_name -volume
   volume_name -mapping mapping_text, ...
   ```

   O mapeamento consiste em uma lista de pares de carateres fonte-alvo separados por "':'". Os carateres são carateres Unicode inseridos usando dígitos hexadecimais. Por exemplo: 3c:E03C.

   O primeiro valor de cada `mapping_text` par que é separado por dois pontos é o valor hexadecimal do caractere NFS que você deseja traduzir, e o segundo valor é o valor Unicode que SMB usa. Os pares de mapeamento devem ser únicos (deve existir um mapeamento um-para-um).

◦ Mapeamento de origem

A tabela a seguir mostra o conjunto de carateres Unicode permissível para mapeamento de fontes:

Caractere Unicode	Caráter impresso	Descrição
0x01-0x19	Não aplicável	Caracteres de controle não-impressão
0x5C	*	Barra invertida
0x3A	:	Cólon
0x2A	*	Asterisco
0x3F	?	Ponto de interrogação
0x22	"	Marca de cotação
0x3C	*	Menos de
0x3E	>	Superior a.
0x7C		
Linha vertical	0xB1	±

◦ Mapeamento de alvos

Você pode especificar carateres de destino na ""Área de uso privado"" do Unicode no seguinte intervalo: U-E0000…U-F8FF.

Exemplo

O comando a seguir cria um mapeamento de carateres para um volume chamado "data" na máquina virtual de armazenamento (SVM) VS1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  ------------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

Comandos ONTAP NFS para gerenciar mapeamentos de caracteres para tradução de nomes de arquivos SMB

É possível gerenciar o mapeamento de carateres criando, modificando, exibindo informações ou excluindo mapeamentos de carateres de arquivo usados para a tradução de nomes de arquivo SMB em volumes FlexVol.

Se você quiser…	Use este comando…
Criar novos mapeamentos de carateres de arquivo	`vserver cifs character-mapping create`
Exibir informações sobre mapeamentos de carateres de arquivo	`vserver cifs character-mapping show`
Modificar mapeamentos de carateres de arquivo existentes	`vserver cifs character-mapping modify`
Excluir mapeamentos de carateres de arquivo	`vserver cifs character-mapping delete`

Saiba mais sobre `vserver cifs character-mapping` o "Referência do comando ONTAP"na .

Informações sobre direitos autorais

Informações sobre marcas comerciais