Proteja o acesso NFS usando políticas de exportação

ONTAP 9

NetApp
January 17, 2025

Índice

Proteja o acesso NFS usando políticas de exportação

Como as políticas de exportação controlam o acesso do cliente a volumes ou qtrees

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.

Política de exportação padrão para SVMs

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

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.

Gerencie clientes com um tipo de segurança não listado

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.
`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

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 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.

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 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 determinam os níveis de acesso do cliente

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.

Se o tipo de segurança do cliente…	Então o cliente…
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.

Gerenciar solicitações de acesso de superusuário

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.

Como o ONTAP usa caches de política de exportação

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
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.

Como o cache de acesso funciona

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.

Como funcionam os parâmetros de cache de acesso

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.

Remova uma política de exportação de uma qtree

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
```

Valide as IDs de qtree para operações de arquivos de 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 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.

Informações sobre direitos autorais

Informações sobre marcas comerciais