



# Configurar o acesso a arquivos usando NFS

ONTAP 9

NetApp  
January 17, 2025

# Índice

Configurar o acesso a arquivos usando NFS .....	1
Configure o acesso a arquivos usando a visão geral do NFS .....	1
Proteja o acesso NFS usando políticas de exportação .....	1
Usando Kerberos com NFS para segurança forte .....	13
Uso do TLS com NFS para uma segurança forte .....	19
Configurar serviços de nomes .....	22
Configurar mapeamentos de nomes .....	34
Ative o acesso para clientes Windows NFS .....	40
Ative a exibição de exportações NFS em clientes NFS .....	41

# Configurar o acesso a arquivos usando NFS

## Configure o acesso a arquivos usando a visão geral do NFS

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, "NFS em TLS", 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 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 caracteres.

- 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 <code>-anon</code>	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:

<b>Somente leitura inclui</b> <code>none</code>	<b>A leitura-gravação inclui</b> <code>none</code>	<b>Acesso resultante para clientes com tipos de segurança não listados</b>
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 <code>Access</code> .	Obtém acesso para esse nível com seu próprio ID de usuário.
Não corresponde ao especificado, mas o parâmetro <code>Access</code> inclui a opção <code>none</code> .	Obtém acesso para esse nível, mas como o usuário anônimo com o ID de usuário especificado pelo <code>-anon</code> parâmetro.
Não corresponde ao especificado e o parâmetro <code>Access</code> não inclui a opção <code>none</code> .	Não obtém acesso para esse nível. Isso não se aplica ao <code>-superuser</code> parâmetro porque ele sempre inclui <code>none</code> 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 <code>-superuser</code> 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 <code>-anon</code> parâmetro e suas permissões atribuídas. Isso é independentemente de o parâmetro somente leitura ou leitura-gravação especificar a opção <code>none</code> .

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-qtrees-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	<pre>vserver nfs modify -vserver vserver_name -validate-qtrees-export enabled</pre>
Desativado	<pre>vserver nfs modify -vserver vserver_name -validate-qtrees-export disabled</pre>

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.

## Usando Kerberos com NFS para segurança forte

### Suporte ONTAP 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 eletrônicos. 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 Kerberos com 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 respectiva 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 Active 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 Active 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 Active 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.

Nome de utilizador	ID de utilizador	ID do grupo principal	Comentário
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 de usuário 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
```

## Uso do TLS com NFS para uma segurança forte

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

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



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

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

### Requisitos

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

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

### Ativar ou desativar TLS para clientes NFS no ONTAP

Você pode melhorar a segurança das conexões NFS configurando o NFS em TLS para criptografar todos os dados enviados pela rede entre o cliente NFS e o ONTAP. Isso aumenta a segurança das conexões NFS. Você pode configurar isso em uma VM de storage existente habilitada para NFS.



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

### Ativar TLS

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

#### Antes de começar

- Consulte "[requisitos](#)" para NFS sobre TLS antes de começar.
- Consulte as páginas do manual do ONTAP para obter mais informações sobre o comando neste

procedimento.

- Saiba mais sobre `vserver nfs tls interface show` o ["Referência do comando ONTAP"](#) na .

### Passos

1. Escolha uma VM de armazenamento e uma interface lógica (LIF) na qual ativar o TLS.
2. Habilite o TLS para conexões NFS nessa VM e interface de storage.

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

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

```
vserver nfs tls interface show
```

### Exemplo

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

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

```
vserver nfs tls interface show
```

Vserver Name	Logical Interface	Address	TLS Status	TLS Certificate
vs1	data1	10.0.1.1	enabled	cert_vs1
vs2	data2	10.0.1.2	disabled	-

2 entries were displayed.

### Desativar TLS

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

### Antes de começar

Saiba mais sobre `vserver nfs tls interface disable` o ["Referência do comando ONTAP"](#) na .

### Passos

1. Escolha uma VM de armazenamento e uma interface lógica (LIF) para desativar o TLS.

2. Desative TLS para conexões NFS nessa VM e interface de storage.

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

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

```
vserver nfs tls interface show
```

### Exemplo

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

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

```
vserver nfs tls interface show
```

```

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

### Editar uma configuração TLS

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

#### Antes de começar

Saiba mais sobre `vserver nfs tls interface modify` o ["Referência do comando ONTAP"](#) na .

#### Passos

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

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

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

```
vserver nfs tls interface show
```

### Exemplo

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

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

```
vserver nfs tls interface show
```

Vserver Name	Logical Interface	Address	TLS Status	TLS Certificate
vs1	data1	10.0.1.1	disabled	-
vs2	data2	10.0.1.2	enabled	new_cert

2 entries were displayed.

### Informações relacionadas

["Ative o storage nas para servidores Linux usando NFS"](#).

## Configurar serviços de nomes

### Como funciona a configuração do switch do serviço de nomes 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	<pre>vserver services name- service unix-user vserver services name-service unix-group  vserver services name- service netgroup  vserver services name- service dns hosts</pre>
nis	Servidores NIS externos, conforme especificado na configuração do domínio NIS da SVM	<pre>vserver services name- service nis-domain</pre>
ldap	Servidores LDAP externos, conforme especificado na configuração de cliente LDAP do SVM	<pre>vserver services name- service ldap</pre>

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

Vserver	Database	Source	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

### Visão geral do LDAP

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 deve estar habilitado para TLS ou SSL no ONTAP 9.5 e posterior. O SSL não é suportado no ONTAP 9.0-9,4.
  - Um servidor de certificados já deve estar configurado no domínio.
- Para ativar a perseguição de referência LDAP (no ONTAP 9.5 e posterior), as seguintes condições devem ser satisfeitas:
  - Ambos os domínios devem ser configurados com uma das seguintes relações de confiança:
    - Bidirecional

- One-way, onde o primário confia no domínio de referência
- Pai-filho
- O DNS deve ser configurado para resolver todos os nomes de servidor referidos.
- As senhas de domínio devem ser 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 "[Ligação rápida LDAP para autenticação nsswitch.](#)"
- 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 .

### Conceitos de assinatura e vedação LDAP

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.

### Conceitos LDAPS

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 active 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 9.5-9,8, o LDAPS só pode ser ativado 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`. Para obter mais informações, consulte a `vserver services name-service ldap client create` página de manual



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 Active Directory e o SVM
- LDAPS para tráfego LDAP para mapeamento de nomes e outras informações do UNIX

Servidores LDAP integrados ao Active 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 Active 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.

### Ative o suporte ao LDAP RFC2307bis

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.

#### O que você vai precisar

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 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 conectar 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 os valores múltiplos podem ser inseridos se necessário (por exemplo, se a busca por referência LDAP estiver ativada 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 usuário LDAP este parâmetro também se aplica a pesquisas de mapeamento de nome de usuário.
-user-scope	Escopo base para todas as pesquisas de usuário LDAP este parâmetro também se aplica a pesquisas de mapeamento de nome de usuário.
-group-dn	DNS base para todas as pesquisas de grupo LDAP
-group-scope	Escopo base para todas as pesquisas de grupo LDAP
-netgroup-dn	DNS base para todas as pesquisas de netgroup 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.

## Melhore o desempenho das pesquisas de diretório LDAP `netgroup-by-host`

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`.

### O que você vai precisar

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.



A partir de ONTAP 9.2, o campo `-ldap-servers` substitui o `-servers` campo. Este novo campo pode ter 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 LDAP fast bind para autenticação nsswitch

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
```

- Para novos utilizadores de administração, consulte ["Ative o acesso a contas LDAP ou NIS."](#)

## Apresentar estatísticas LDAP

A partir do ONTAP 9.2, você pode exibir estatísticas LDAP para máquinas virtuais de armazenamento (SVMs) em um sistema de armazenamento para monitorar o desempenho e diagnosticar problemas.

### O que você vai precisar

- 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
```

## Configurar mapeamentos de nomes

### Configure a visão geral dos mapeamentos de nomes

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 conectando 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.

## Como o mapeamento de nomes funciona

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.

## Procura multidomínio para mapeamentos de nome de usuário do UNIX para o Windows

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.
*	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.  <div style="border: 1px solid gray; padding: 5px; display: inline-block;">  O asterisco é válido apenas para o mapeamento de nomes de UNIX para Windows, e não para o contrário. </div>

### 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

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 caracteres contendo sequências de escape que representam subexpressões do padrão, como no programa UNIX `sed`.

## Crie um mapeamento de nomes

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). Consulte a `vserver name-mapping create` página de manual para obter detalhes.

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
```

## Configure o usuário padrão

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	<code>vserver cifs options modify -default-unix-user user_name</code>
Configure o usuário padrão do Windows	<code>vserver nfs modify -default-win-user user_name</code>

## Comandos para gerenciar mapeamentos de nomes

Existem comandos ONTAP específicos para gerenciar mapeamentos de nomes.

Se você quiser...	Use este comando...
Crie um mapeamento de nomes	<code>vserver name-mapping create</code>

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

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

## Ative o acesso para clientes Windows NFS

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:\
```

## Ative a exibição de exportações NFS em clientes NFS

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.

A partir do ONTAP 9.2, o ONTAP permite que os 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:

```
cluster1 : : > 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/unix1 (everyone)
/unix/unix2 (everyone)
/          (everyone)
```

## Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

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

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

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

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

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

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

## Informações sobre marcas comerciais

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