



Gerenciar ACLs NFSv4

ONTAP 9

NetApp
January 17, 2025

Índice

- Gerenciar ACLs NFSv4 1
 - Benefícios de habilitar ACLs NFSv4 1
 - Como as ACLs NFSv4 funcionam 1
 - Ativar ou desativar a modificação das ACLs NFSv4 1
 - Como o ONTAP usa ACLs NFSv4 para determinar se ele pode excluir um arquivo 2
 - Ativar ou desativar ACLs NFSv4 2
 - Modifique o limite máximo de ACE para ACLs NFSv4 3

Gerenciar ACLs NFSv4

Benefícios de habilitar ACLs NFSv4

Há muitos benefícios em habilitar ACLs NFSv4.

Os benefícios de habilitar ACLs NFSv4 incluem o seguinte:

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

Como as ACLs NFSv4 funcionam

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

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

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



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

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



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

Ativar ou desativar a modificação das ACLs NFSv4

Quando o ONTAP recebe um `chmod` comando para um arquivo ou diretório com uma ACL, por padrão a ACL é mantida e modificada para refletir a alteração de bit de modo.

Você pode desativar o `-v4-acl-preserve` parâmetro para alterar o comportamento se quiser que a ACL seja descartada.

Sobre esta tarefa

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

A predefinição para este parâmetro está ativada.

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Execute uma das seguintes ações:

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

3. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

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

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

Ativar ou desativar ACLs NFSv4

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

Sobre esta tarefa

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

Passo

1. Execute uma das seguintes ações:

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

Modifique o limite máximo de ACE para ACLs NFSv4

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

Sobre esta tarefa

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

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

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

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

O intervalo válido de

`max_ace_limit` é a.192 1024.

3. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

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.