



Configurar estilos de segurança

ONTAP 9

NetApp
January 17, 2025

Índice

- Configurar estilos de segurança 1
 - Como os estilos de segurança afetam o acesso aos dados 1
 - Configurar estilos de segurança em volumes raiz do SVM 4
 - Configurar estilos de segurança no FlexVol volumes 4
 - Configurar estilos de segurança no qtrees 5

Configurar estilos de segurança

Como os estilos de segurança afetam o acesso aos dados

Estilos de segurança e seus efeitos

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

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

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

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

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

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

A partir do ONTAP 9.2, o `show-effective-permissions` parâmetro para o `vserver security file-`

`directory` comando permite exibir permissões efetivas concedidas a um usuário Windows ou UNIX no caminho especificado de arquivo ou pasta. Além disso, o parâmetro opcional `-share-name` permite exibir a permissão de compartilhamento efetivo.



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

Onde e quando definir estilos de segurança

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

Decida qual estilo de segurança usar em SVMs

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

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

Estilo de segurança	Escolha se...
UNIX	<ul style="list-style-type: none">• O sistema de arquivos é gerenciado por um administrador UNIX.• A maioria dos usuários são clientes NFS.• Um aplicativo que acessa os dados usa um usuário UNIX como a conta de serviço.
NTFS	<ul style="list-style-type: none">• O sistema de arquivos é gerenciado por um administrador do Windows.• A maioria dos usuários são clientes SMB.• Um aplicativo que acessa os dados usa um usuário do Windows como a conta de serviço.
Misto	<ul style="list-style-type: none">• O sistema de arquivos é gerenciado por administradores UNIX e Windows e os usuários consistem em clientes NFS e SMB.

Como a herança de estilo de segurança funciona

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

Os estilos de segurança são herdados da seguinte maneira:

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

Como o ONTAP preserva as permissões UNIX

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

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

Quando os clientes Windows executam uma consulta para as propriedades de segurança, eles recebem uma ACL construída que representa exatamente as permissões UNIX. O único propósito desta ACL construída é preservar as permissões UNIX do arquivo, pois os arquivos são atualizados por aplicativos do Windows para garantir que os arquivos resultantes tenham as mesmas permissões UNIX. O ONTAP não define nenhuma ACLs NTFS usando a ACL construída.

Gerenciar permissões UNIX usando a guia Segurança do Windows

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

- Modificação de permissões UNIX

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

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

- Alterando permissões UNIX para permissões NTFS

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

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

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

Configurar estilos de segurança em volumes raiz do SVM

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

Passos

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

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

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

```
vserver show -vserver vserver_name
```

Configurar estilos de segurança no FlexVol volumes

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

Passos

1. Execute uma das seguintes ações:

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

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

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

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

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

```
volume show -volume volume_name -instance
```

Configurar estilos de segurança no qtrees

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

Passos

1. Execute uma das seguintes ações:

Se a qtree...	Use o comando...
Ainda não existe	<code>volume qtree create</code> e inclua o <code>-security-style</code> parâmetro para especificar o estilo de segurança.
Já existe	<code>volume qtree modify</code> e inclua o <code>-security-style</code> parâmetro para especificar o estilo de segurança.

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

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

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

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

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 INTERRUPTÃO 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.