



Acesso SMB seguro usando políticas de exportação

ONTAP 9

NetApp
January 17, 2025

Índice

- Acesso SMB seguro usando políticas de exportação 1
 - Como as políticas de exportação são usadas com o acesso SMB 1
 - Como funcionam as regras de exportação 2
 - Exemplos de regras de política de exportação que restringem ou permitem acesso através de SMB 3
 - Ativar ou desativar políticas de exportação para acesso SMB 5

Acesso SMB seguro usando políticas de exportação

Como as políticas de exportação são usadas com o acesso SMB

Se as políticas de exportação para acesso SMB estiverem habilitadas no servidor SMB, as políticas de exportação serão usadas ao controlar o acesso a volumes SVM por clientes SMB. Para acessar dados, você pode criar uma política de exportação que permita o acesso SMB e, em seguida, associá-la aos volumes que contêm compartilhamentos SMB.

Uma política de exportação tem uma ou mais regras aplicadas a ela que especifica quais clientes têm permissão de acesso aos dados e quais protocolos de autenticação são suportados para acesso somente leitura e gravação. Você pode configurar políticas de exportação para permitir o acesso por SMB a todos os clientes, uma sub-rede de clientes ou um cliente específico e para permitir a autenticação usando autenticação Kerberos, autenticação NTLM ou autenticação Kerberos e NTLM ao determinar o acesso somente leitura e gravação aos dados.

Depois de processar todas as regras de exportação aplicadas à política de exportação, o ONTAP pode determinar se o cliente recebe acesso e que nível de acesso é concedido. As regras de exportação se aplicam a máquinas cliente, não a usuários e grupos do Windows. As regras de exportação não substituem a autenticação e autorização baseadas em grupo e no utilizador do Windows. As regras de exportação fornecem outra camada de segurança de acesso, além das permissões de compartilhamento e acesso a arquivos.

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

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

Cada SVM tem pelo menos uma política de exportação chamada "falha", que não contém regras. Não é possível excluir esta política de exportação, mas você pode renomeá-la ou modificá-la. Por padrão, cada volume no SVM está associado à política de exportação padrão. Se as políticas de exportação para acesso SMB estiverem desativadas no SVM, a política de exportação "falha" não terá efeito no acesso SMB.

Você pode configurar regras que fornecem acesso a hosts NFS e SMB e associar essa regra a uma política de exportação, que pode ser associada ao volume que contém dados ao qual hosts NFS e SMB precisam acessar. Alternativamente, se houver alguns volumes em que apenas clientes SMB exigem acesso, você poderá configurar uma política de exportação com regras que só permitem acesso usando o protocolo SMB e que usa apenas Kerberos ou NTLM (ou ambos) para autenticação para acesso somente leitura e gravação. A política de exportação é então associada aos volumes em que apenas o acesso SMB é desejado.

Se as políticas de exportação para SMB estiverem ativadas e um cliente fizer uma solicitação de acesso não 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 do volume, o acesso será

negado. Se uma política de exportação estiver vazia, todos os acessos serão implicitamente negados. Isso é verdade mesmo se as permissões de compartilhamento e arquivo permitissem o acesso. Isso significa que você deve configurar sua política de exportação para permitir minimamente o seguinte em volumes que contêm compartilhamentos SMB:

- Permitir o acesso a todos os clientes ou ao subconjunto apropriado de clientes
- Permitir acesso através de SMB
- Permitir acesso apropriado somente leitura e gravação usando a autenticação Kerberos ou NTLM (ou ambas)

Saiba mais "[configuração e gerenciamento de políticas de exportação](#)" sobre .

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.

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.

Exemplos de regras de política de exportação que restringem ou permitem acesso através de SMB

Os exemplos mostram como criar regras de política de exportação que restringem ou permitem o acesso ao SMB em um SVM que tenha políticas de exportação para acesso ao SMB ativadas.

As políticas de exportação para o acesso SMB estão desativadas por predefinição. Você precisa configurar regras de política de exportação que restrinjam ou permitam acesso ao SMB somente se você tiver ativado políticas de exportação para acesso ao SMB.

Regra de exportação apenas para acesso SMB

O comando a seguir cria uma regra de exportação no SVM chamado "VS1" que tem a seguinte configuração:

- Nome da política: cifs1
- Número de índice: 1
- Correspondência de cliente: Corresponde apenas a clientes na rede 192.168.1.0/24
- Protocolo: Ativa apenas o acesso SMB
- Acesso somente leitura: Para clientes que usam autenticação NTLM ou Kerberos
- Acesso de leitura-gravação: Para clientes que usam a autenticação Kerberos

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

Regra de exportação para SMB e acesso NFS

O comando a seguir cria uma regra de exportação no SVM chamado "VS1" que tem a seguinte configuração:

- Nome da política: cifsnfs1
- Número de índice: 2
- Correspondência do cliente: Corresponde a todos os clientes
- Protocolo: Acesso SMB e NFS
- Acesso somente leitura: Para todos os clientes
- Acesso de leitura e gravação: Para clientes que usam Kerberos (NFS e SMB) ou autenticação NTLM (SMB)
- Mapeamento para ID de usuário UNIX 0 (zero): Mapeado para ID de usuário 65534 (que normalmente mapeia para o nome de usuário ninguém)
- Acesso suid e sgid: Permite

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule any
-rwrule krb5,ntlm -anon 65534 -allow-suid true
```

Regra de exportação para acesso SMB usando apenas NTLM

O comando a seguir cria uma regra de exportação no SVM chamado "VS1" que tem a seguinte configuração:

- Nome da política: ntlm1
- Número de índice: 1
- Correspondência do cliente: Corresponde a todos os clientes
- Protocolo: Ativa apenas o acesso SMB

- Acesso somente leitura: Somente para clientes que usam NTLM
- Acesso de leitura e gravação: Apenas para clientes que utilizam NTLM



Se você configurar a opção somente leitura ou a opção leitura-gravação para acesso somente NTLM, você deverá usar entradas baseadas em endereço IP na opção correspondência do cliente. Caso contrário, você recebe `access denied` erros. Isso ocorre porque o ONTAP usa os nomes principais do Serviço Kerberos (SPN) ao usar um nome de host para verificar os direitos de acesso do cliente. A autenticação NTLM não suporta nomes SPN.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

Ativar ou desativar políticas de exportação para acesso SMB

Você pode ativar ou desativar políticas de exportação para acesso SMB em máquinas virtuais de armazenamento (SVMs). O uso de políticas de exportação para controlar o acesso SMB a recursos é opcional.

Antes de começar

A seguir estão os requisitos para ativar políticas de exportação para SMB:

- O cliente deve ter um Registro "PTR" no DNS antes de criar as regras de exportação para esse cliente.
- Um conjunto adicional de Registros "A" e "PTR" para nomes de host é necessário se o SVM fornecer acesso a clientes NFS e o nome de host que você deseja usar para acesso NFS for diferente do nome do servidor CIFS.

Sobre esta tarefa

Ao configurar um novo servidor CIFS na SVM, o uso de políticas de exportação para acesso SMB é desativado por padrão. Você pode habilitar políticas de exportação para acesso SMB se quiser controlar o acesso com base no protocolo de autenticação ou em endereços IP de cliente ou nomes de host. Você pode ativar ou desativar políticas de exportação para acesso SMB a qualquer momento.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Ativar ou desativar políticas de exportação:
 - Ativar políticas de exportação: `vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled true`
 - Desativar políticas de exportação: `vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled false`
3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exemplo

O exemplo a seguir permite o uso de políticas de exportação para controlar o acesso de clientes SMB a recursos no SVM VS1:

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them  
only when directed to do so by technical support personnel.
```

```
Do you wish to continue? (y or n): y
```

```
cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy  
-enabled true
```

```
cluster1::*> 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.