



Configurar a digitalização no acesso

ONTAP 9

NetApp
January 17, 2025

Índice

- Configurar a digitalização no acesso 1
 - Crie uma política de acesso 1
 - Ative uma política de acesso 3
 - Modifique o perfil de operações de arquivo Vscan para um compartilhamento SMB 4
 - Comandos para gerenciar políticas de acesso 4

Configurar a digitalização no acesso

Crie uma política de acesso

Uma política de acesso define o escopo de uma digitalização no acesso. Você pode criar uma política de acesso para um SVM individual ou para todos os SVMs em um cluster. Se você criou uma política de acesso para todos os SVMs em um cluster, habilite a política em cada SVM individualmente.

Sobre esta tarefa

- Pode especificar o tamanho máximo do ficheiro a analisar, as extensões e os caminhos de ficheiro a incluir na digitalização e as extensões e caminhos de ficheiro a excluir da digitalização.
- Você pode definir a `scan-mandatory` opção como Desativado para especificar que o acesso ao arquivo é permitido quando nenhum servidor Vscan estiver disponível para verificação de vírus.
- Por padrão, o ONTAP cria uma política de acesso chamada "default_CIFS" e a habilita para todos os SVMs em um cluster.
- Qualquer arquivo que se qualifica para exclusão de digitalização com base nos `paths-to-exclude` parâmetros, `file-ext-to-exclude` ou `max-file-size` não é considerado para digitalização, mesmo que a `scan-mandatory` opção esteja definida como ativado. (Verifique "[solução de problemas](#)" esta seção para problemas de conectividade relacionados à `scan-mandatory` opção.)
- Por padrão, somente os volumes de leitura e gravação são digitalizados. Você pode especificar filtros que ativam a digitalização de volumes somente leitura ou que restringem a digitalização a arquivos abertos com acesso de execução.
- A verificação de vírus não é realizada em um compartilhamento SMB para o qual o parâmetro continuamente disponível está definido como Sim.
- Consulte "[Arquitetura antivírus](#)" a seção para obter detalhes sobre o perfil *Vscan file-operations*.
- Você pode criar um máximo de dez (10) políticas de acesso por SVM. No entanto, você pode ativar apenas uma política de acesso por vez.
 - Você pode excluir um máximo de cem (100) caminhos e extensões de arquivo da verificação de vírus em uma política de acesso.
- Algumas recomendações de exclusão de arquivos:
 - Considere excluir arquivos grandes (o tamanho do arquivo pode ser especificado) da verificação de vírus, porque eles podem resultar em uma resposta lenta ou tempos limite de solicitações de verificação para usuários CIFS. O tamanho padrão do arquivo para exclusão é 2GB.
 - Considere excluir extensões de arquivo como `.vhd` e `.tmp` porque arquivos com essas extensões podem não ser apropriados para a digitalização.
 - Considere excluir caminhos de arquivo, como o diretório de quarentena ou caminhos nos quais apenas discos rígidos virtuais ou bancos de dados são armazenados.
 - Verifique se todas as exclusões estão especificadas na mesma política, pois somente uma diretiva pode ser ativada de cada vez. A NetApp recomenda vivamente que tenha o mesmo conjunto de exclusões especificado no mecanismo antivírus.
- É necessária uma política de acesso para um [digitalização a pedido](#). Para evitar a digitalização no acesso, você deve definir `-scan-files-with-no-ext` como `false` e `-file-ext-to-exclude` como `*` para excluir todas as extensões.

Passos

1. Crie uma política de acesso:

```
vserver vscan on-access-policy create -vserver data_SVM|cluster_admin_SVM
-policy-name policy_name -protocol CIFS -max-file-size
max_size_of_files_to_scan -filters [scan-ro-volume,][scan-execute-access]
-file-ext-to-include extensions_of_files_to_include -file-ext-to-exclude
extensions_of_files_to_exclude -scan-files-with-no-ext true|false -paths-to
-exclude paths_of_files_to_exclude -scan-mandatory on|off
```

- Especifique um SVM de dados para uma política definida para um SVM individual, um administrador de cluster SVM para uma política definida para todos os SVMs em um cluster.
- A `-file-ext-to-exclude` definição substitui a `-file-ext-to-include` definição.
- Defina `-scan-files-with-no-ext` como verdadeiro para digitalizar arquivos sem extensões. O comando a seguir cria uma política de acesso denominada `Policy1` na `vs1` SVM:

```
cluster1::> vserver vscan on-access-policy create -vserver vs1 -policy
-name Policy1 -protocol CIFS -filters scan-ro-volume -max-file-size 3GB
-file-ext-to-include "mp*", "tx*" -file-ext-to-exclude "mp3", "txt" -scan
-files-with-no-ext false -paths-to-exclude "\vol\ a b\"," \vol\ a, b\"
```

2. Verifique se a política de acesso foi criada: `vserver vscan on-access-policy show -instance data_SVM|cluster_admin_SVM -policy-name name`

Para obter uma lista completa de opções, consulte a página de manual do comando.

O comando a seguir exibe os detalhes da `Policy1` política:

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1
```

```

                Vserver: vs1
                Policy: Policy1
                Policy Status: off
                Policy Config Owner: vserver
                File-Access Protocol: CIFS
                Filters: scan-ro-volume
                Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
                File Paths Not to Scan: \vol\ a b\, \vol\ a, b\
                File Extensions Not to Scan: mp3, txt
                File Extensions to Scan: mp*, tx*
                Scan Files with No Extension: false
```

Ative uma política de acesso

Uma política de acesso define o escopo de uma digitalização no acesso. Você deve habilitar uma política de acesso em um SVM antes que seus arquivos possam ser digitalizados.

Se você criou uma política de acesso para todos os SVMs em um cluster, habilite a política em cada SVM individualmente. Você pode ativar apenas uma política de acesso em um SVM de cada vez.

Passos

1. Ativar uma política de acesso:

```
vserver vscan on-access-policy enable -vserver data_SVM -policy-name  
policy_name
```

O comando a seguir habilita uma política de acesso denominada `Policy1` na `vs1` SVM:

```
cluster1::> vserver vscan on-access-policy enable -vserver vs1 -policy  
-name Policy1
```

2. Verifique se a política de acesso está ativada:

```
vserver vscan on-access-policy show -instance data_SVM -policy-name  
policy_name
```

Para obter uma lista completa de opções, consulte a página de manual do comando.

O comando a seguir exibe os detalhes da `Policy1` política de acesso:

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy  
-name Policy1
```

```
                Vserver: vs1  
                Policy: Policy1  
                Policy Status: on  
                Policy Config Owner: vserver  
                File-Access Protocol: CIFS  
                Filters: scan-ro-volume  
                Mandatory Scan: on  
                Max File Size Allowed for Scanning: 3GB  
                File Paths Not to Scan: \vol\a b\, \vol\a,b\  
                File Extensions Not to Scan: mp3, txt  
                File Extensions to Scan: mp*, tx*  
                Scan Files with No Extension: false
```

Modifique o perfil de operações de arquivo Vscan para um compartilhamento SMB

O perfil *Vscan file-operations* de um compartilhamento SMB define as operações no compartilhamento que podem acionar a digitalização. Por padrão, o parâmetro é definido como `standard`. Você pode ajustar o parâmetro conforme necessário ao criar ou modificar um compartilhamento SMB.

Consulte "[Arquitetura antivírus](#)" a seção para obter detalhes sobre o perfil *Vscan file-operations*.



A verificação de vírus não é realizada em um compartilhamento SMB que tenha o `continuously-available` parâmetro definido como `Yes`.

Passo

1. Modifique o valor do perfil de operações de arquivos Vscan para uma partilha SMB:

```
vserver cifs share modify -vserver data_SVM -share-name share -path share_path  
-vscan-fileop-profile no-scan|standard|strict|writes-only
```

Para obter uma lista completa de opções, consulte a página de manual do comando.

O comando a seguir altera o perfil de operações do arquivo Vscan para um compartilhamento SMB para `strict`:

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name  
SALES_SHARE -path /sales -vscan-fileop-profile strict
```

Comandos para gerenciar políticas de acesso

Você pode modificar, desativar ou excluir uma política de acesso. Você pode exibir um resumo e detalhes da política.

Se você quiser...	Digite o seguinte comando...
Crie uma política de acesso	<code>vserver vscan on-access-policy create</code>
Modificar uma política de acesso	<code>vserver vscan on-access-policy modify</code>
Ative uma política de acesso	<code>vserver vscan on-access-policy enable</code>
Desative uma política de acesso	<code>vserver vscan on-access-policy disable</code>
Eliminar uma política de acesso	<code>vserver vscan on-access-policy delete</code>

Veja o resumo e os detalhes de uma política de acesso	<code>vserver vscan on-access-policy show</code>
Adicionar à lista de caminhos a excluir	<code>vserver vscan on-access-policy paths-to-exclude add</code>
Excluir da lista de caminhos a serem excluídos	<code>vserver vscan on-access-policy paths-to-exclude remove</code>
Exibir a lista de caminhos a serem excluídos	<code>vserver vscan on-access-policy paths-to-exclude show</code>
Adicionar à lista de extensões de arquivo a excluir	<code>vserver vscan on-access-policy file-ext-to-exclude add</code>
Excluir da lista de extensões de arquivo a serem excluídas	<code>vserver vscan on-access-policy file-ext-to-exclude remove</code>
Veja a lista de extensões de arquivo a excluir	<code>vserver vscan on-access-policy file-ext-to-exclude show</code>
Adicionar à lista de extensões de arquivo a incluir	<code>vserver vscan on-access-policy file-ext-to-include add</code>
Excluir da lista de extensões de arquivo a incluir	<code>vserver vscan on-access-policy file-ext-to-include remove</code>
Veja a lista de extensões de arquivo a incluir	<code>vserver vscan on-access-policy file-ext-to-include show</code>

Para obter mais informações sobre esses comandos, consulte as páginas `man`.

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.