Sobre a proteção antivírus do NetApp

ONTAP 9

NetApp
January 17, 2025

Índice

Sobre a proteção antivírus do NetApp

Sobre a verificação de vírus NetApp

O Vscan é uma solução de verificação antivírus desenvolvida pela NetApp que permite aos clientes proteger seus dados de serem comprometidos por vírus ou outros códigos maliciosos. Ele combina software antivírus fornecido pelo parceiro com recursos do ONTAP para dar aos clientes a flexibilidade de que precisam para gerenciar a verificação de arquivos.

Como a verificação de vírus funciona

Os sistemas de storage descarregam as operações de verificação para servidores externos que hospedam softwares antivírus de terceiros.

Com base no modo de digitalização ativo, o ONTAP envia solicitações de digitalização quando os clientes acessam arquivos por SMB (on-access) ou acessar arquivos em locais específicos, em um horário ou imediatamente (sob demanda).

- Você pode usar *verificação no acesso* para verificar se há vírus quando os clientes abrem, leem, renomeam ou fecham arquivos pelo SMB. As operações de arquivo são suspensas até que o servidor externo comunique o status de digitalização do arquivo. Se o ficheiro já tiver sido lido, o ONTAP permite a operação do ficheiro. Caso contrário, ele solicita uma verificação do servidor.

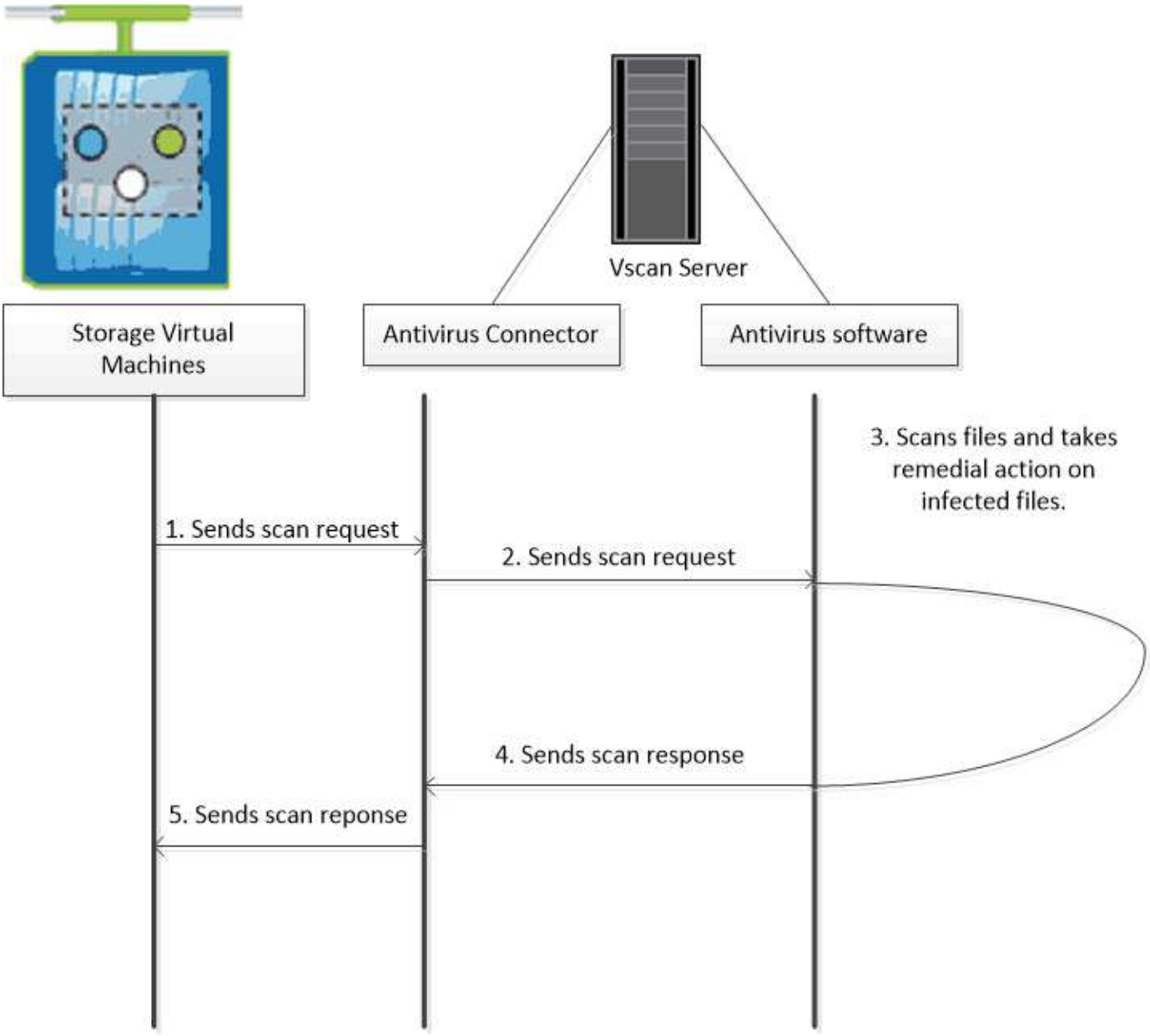
  A verificação no acesso não é suportada para NFS.

- Você pode usar *On-demand scanning* para verificar arquivos para vírus imediatamente ou em uma programação. Recomendamos que as verificações a pedido sejam executadas apenas em horas fora do pico para evitar sobrecarregar a infra-estrutura AV existente, que normalmente é dimensionada para a digitalização no acesso. O servidor externo atualiza o status de verificação dos arquivos verificados, de modo que a latência de acesso ao arquivo seja reduzida em relação ao SMB. Se houver modificações de arquivo ou atualizações de versão de software, ele solicita uma nova verificação de arquivo do servidor externo.

  Você pode usar a verificação sob demanda para qualquer caminho no namespace SVM, até mesmo para volumes exportados somente por NFS.

Normalmente, você ativa os modos de digitalização sob demanda e de acesso sob demanda em uma SVM. Em ambos os modos, o software antivírus toma medidas corretivas em arquivos infetados com base em suas configurações de software.

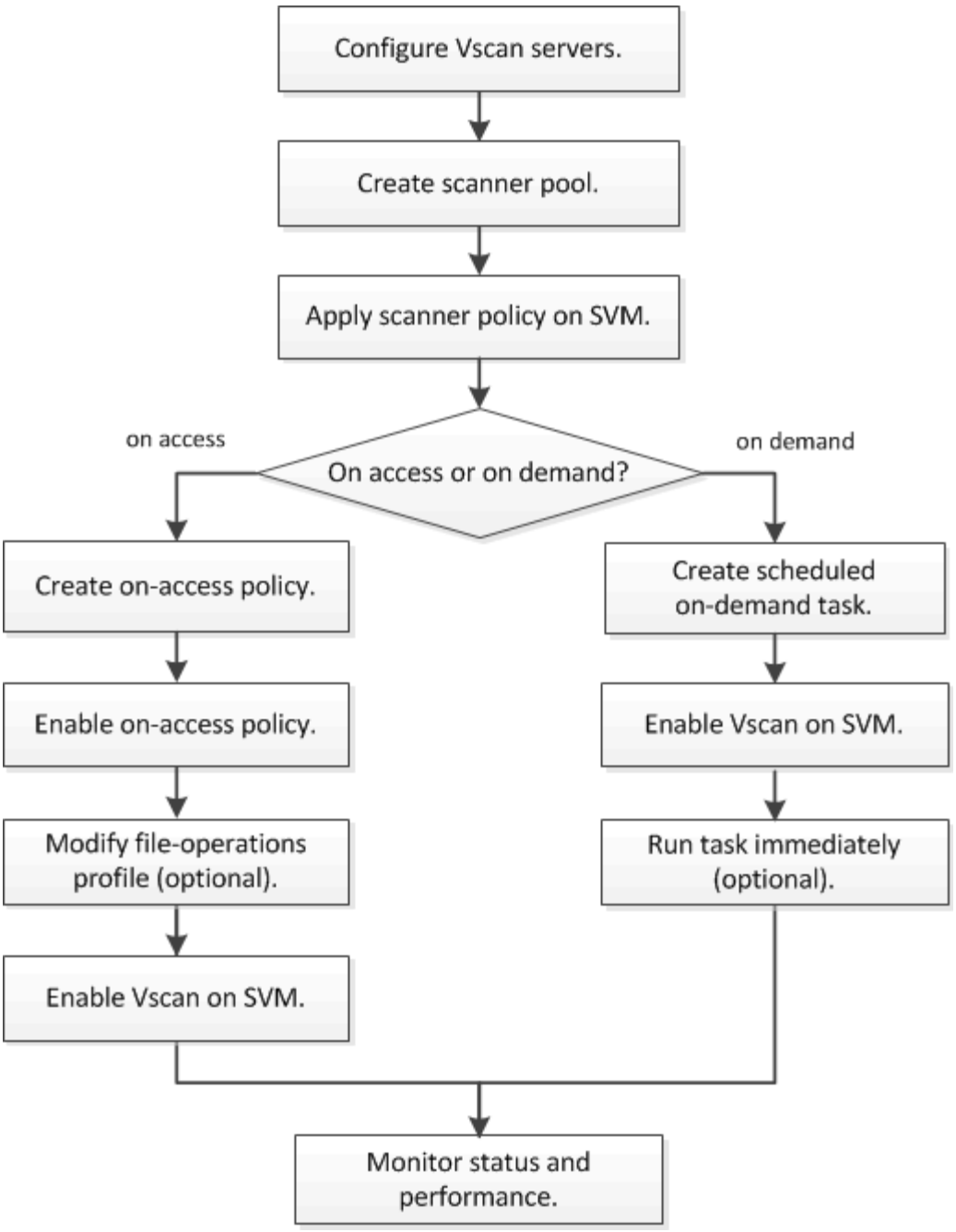
O conetor do antivírus ONTAP, fornecido pelo NetApp e instalado no servidor externo, lida com a comunicação entre o sistema de armazenamento e o software antivírus.



Fluxo de trabalho de verificação de vírus

Você deve criar um pool de scanner e aplicar uma política de scanner antes de ativar a digitalização. Normalmente, você ativa os modos de digitalização sob demanda e de acesso sob demanda em uma SVM.

Você deve ter concluído a configuração CIFS.



Para criar uma tarefa sob demanda, deve haver pelo menos uma política de acesso ativada. Pode ser a política padrão ou uma política de acesso criada pelo usuário.

Próximas etapas

- Crie um pool de scanners em um único cluster
- Aplique uma política de scanner em um único cluster
- Crie uma política de acesso

Arquitetura antivírus

A arquitetura antivírus do NetApp consiste em software de servidor Vscan e configurações associadas.

Software do servidor Vscan

Tem de instalar este software no servidor Vscan.

- **Conetor do antivírus ONTAP**

  Este é um software fornecido pela NetApp que lida com a comunicação de solicitação de verificação e resposta entre os SVMs e o software antivírus. Ele pode ser executado em uma máquina virtual, mas para o melhor desempenho use uma máquina física. Você pode baixar este software a partir do site de suporte da NetApp (requer login).

- **Software antivírus**

  Este é um software fornecido por parceiros que verifica os ficheiros em busca de vírus ou outro código malicioso. Você especifica as ações corretivas a serem tomadas em arquivos infetados ao configurar o software.

Definições do software Vscan

Tem de configurar estas definições de software no servidor Vscan.

- **Piscina do scanner**

  Esta configuração define os servidores Vscan e os usuários privilegiados que podem se conetar a SVMs. Ele também define um período de tempo limite de solicitação de digitalização, após o qual a solicitação de digitalização é enviada para um servidor Vscan alternativo, se houver um disponível.

  > Você deve definir o período de tempo limite no software antivírus no servidor Vscan para cinco segundos a menos do que o período de tempo limite de solicitação de digitalização do pool do scanner. Isso evitará situações em que o acesso ao arquivo seja atrasado ou negado completamente porque o período de tempo limite no software é maior do que o período de tempo limite para a solicitação de digitalização.

- **Usuário privilegiado**

  Essa configuração é uma conta de usuário de domínio que um servidor Vscan usa para se conetar ao SVM. A conta deve existir na lista de utilizadores privilegiados no conjunto do scanner.

- **Política do scanner**

  Esta definição determina se um conjunto de scanners está ativo. As políticas do scanner são definidas pelo sistema, pelo que não é possível criar políticas personalizadas do scanner. Apenas estas três políticas estão disponíveis:

  - `Primary` especifica que o pool do scanner está ativo.
  - `Secondary` Especifica que o pool de scanner está ativo, somente quando nenhum dos servidores Vscan no pool de scanner primário estiver conetado.
  - `Idle` especifica que o conjunto de scanners está inativo.

- **Política de acesso**

  Esta definição define o âmbito de uma digitalização no acesso. 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.

Por padrão, somente os volumes de leitura e gravação são digitalizados. Você pode especificar filtros que permitem a digitalização de volumes somente leitura ou que restringem a digitalização a arquivos abertos com acesso de execução:

- `scan-ro-volume` permite a digitalização de volumes só de leitura.
- `scan-execute-access` restringe a digitalização para arquivos abertos com acesso de execução.

> "Execute Access" é diferente de "execute permission". Um determinado cliente terá "execute access" em um arquivo executável somente se o arquivo tiver sido aberto com "execute intent".

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. No modo de acesso, pode escolher entre estas duas opções mutuamente exclusivas:

- Obrigatório: Com esta opção, o Vscan tenta entregar a solicitação de digitalização ao servidor até que o período de tempo limite expire. Se a solicitação de digitalização não for aceita pelo servidor, a solicitação de acesso do cliente será negada.
- Não obrigatório: Com esta opção, o Vscan sempre permite o acesso do cliente, independentemente de um servidor Vscan estar ou não disponível para verificação de vírus.

- **Tarefa sob demanda**

Esta definição define o âmbito de uma digitalização a pedido. 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. Os arquivos nos subdiretórios são verificados por padrão.

Você usa um cronograma cron para especificar quando a tarefa é executada. Você pode usar o `vserver vscan on-demand-task run` comando para executar a tarefa imediatamente.

- **Perfil de operações de arquivo Vscan (somente digitalização no acesso)**

O `vscan-fileop-profile` parâmetro para `vserver cifs share create` o comando define quais operações de arquivo SMB acionam a verificação de vírus. Por padrão, o parâmetro é definido como `standard`, que é a melhor prática do NetApp. Você pode ajustar esse parâmetro conforme necessário ao criar ou modificar um compartilhamento SMB:

- `no-scan` especifica que as verificações de vírus nunca são acionadas para o compartilhamento.
- `standard` especifica que as verificações de vírus são acionadas por operações abertas, fechadas e renomeadas.
- `strict` especifica que as verificações de vírus são acionadas por operações abertas, lidas, fechadas e renomeadas.

  O `strict` perfil fornece segurança aprimorada para situações em que vários clientes acessam um arquivo simultaneamente. Se um cliente fechar um arquivo depois de gravar um vírus para ele, e o mesmo arquivo permanecer aberto em um segundo cliente, `strict` garante que uma operação de leitura no segundo cliente aciona uma verificação antes que o arquivo seja fechado.

  Você deve ter cuidado para restringir o `strict` perfil a compartilhamentos contendo arquivos que você espera que serão acessados simultaneamente. Uma vez que este perfil gera mais pedidos de

digitalização, pode afetar o desempenho.

- `writes-only` especifica que as verificações de vírus são acionadas apenas quando os arquivos modificados são fechados.

  Como `writes-only` gera menos solicitações de digitalização, geralmente melhora o desempenho.

Se você usar esse perfil, o scanner deve estar configurado para excluir ou colocar em quarentena arquivos infetados não reparáveis, para que eles não possam ser acessados. Se, por exemplo, um cliente fechar um arquivo depois de gravar um vírus para ele, e o arquivo não for reparado, excluído ou em quarentena, qualquer cliente que acesse a gravação do arquivo `without` para ele será infetado.

Se um aplicativo cliente executar uma operação de renomeação, o arquivo será fechado com o novo nome e não será digitalizado. Se tais operações representarem uma preocupação de segurança no seu ambiente, deve utilizar o `standard` perfil ou `strict`.

Soluções de parceiros Vscan

A NetApp colabora com Trellix, Symantec, Trend Micro e Sentinel One para oferecer soluções anti-malware e antivírus líderes do setor, baseadas na tecnologia ONTAP Vscan. Essas soluções ajudam você a verificar arquivos em busca de malware e corrigir quaisquer arquivos afetados.

Como mostrado na tabela abaixo, os detalhes de interoperabilidade para Trellix, Symantec e Trend Micro são mantidos na Matriz de interoperabilidade do NetApp. Os detalhes de interoperabilidade para Trellix e Symantec também podem ser encontrados nos sites de parceiros. Os detalhes de interoperabilidade para o Sentinel One e outros novos parceiros serão mantidos pelo parceiro em seus sites.

Parceiro	Documentação da solução	Detalhes de interoperabilidade
Trellix (anteriormente McAfee)	"Documentação do produto Trellix"	• "Ferramenta de Matriz de interoperabilidade do NetApp" • "Plataformas compatíveis para proteção de armazenamento de segurança de endpoints (trellix.com)"

Parceiro	Documentação da solução	Detalhes de interoperabilidade
Symantec	"Symantec Protection Engine 9.0.0"	• "Ferramenta de Matriz de interoperabilidade do NetApp" • "Matriz de suporte para dispositivos parceiros certificados com Symantec Protection Engine (SPE) para armazenamento conetado à rede (nas) 9.x.x" • "Matriz de suporte para dispositivos de parceiros certificados com Symantec Protection Engine (SPE) para armazenamento conetado à rede (nas) 8.x (broadcom.com)"
Trend Micro	"Guia de introdução do Trend Micro ServerProtect for Storage 6,0"	"Ferramenta de Matriz de interoperabilidade do NetApp"
Sentinel One	• "SentinelOne Singularity Segurança de dados na nuvem" • "Suporte ao SentinelOne" Este link requer um login de usuário. Você pode solicitar acesso a partir do Sentinel One.	Deep Instinct
Deep Instinct Prevention for Storage • "Documentação e Interop" Este link requer um login de usuário. Você pode solicitar acesso do Deep Instinct. • "Folha de dados"	OPSWAT	OPSWAT MetaDefender Storage Security • "Integração de segurança de armazenamento MetaDefender com o NetApp" • "Página de parceiros OPSWAP" • "Resumo da solução de integração"

Informações sobre direitos autorais

Informações sobre marcas comerciais