Proteção contra vírus com Vscan

ONTAP 9

NetApp
January 17, 2025

Índice

Proteção contra vírus com Vscan

Visão geral da configuração do antivírus

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.

O Vscan executa verificações de vírus quando os clientes acessam arquivos por SMB. Você pode configurar o Vscan para digitalizar sob demanda ou em um horário. Você pode interagir com o Vscan usando a interface de linha de comando (CLI) do ONTAP ou as interfaces de programação de aplicativos (APIs) do ONTAP.

Informações relacionadas

"Soluções de parceiros Vscan"

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.

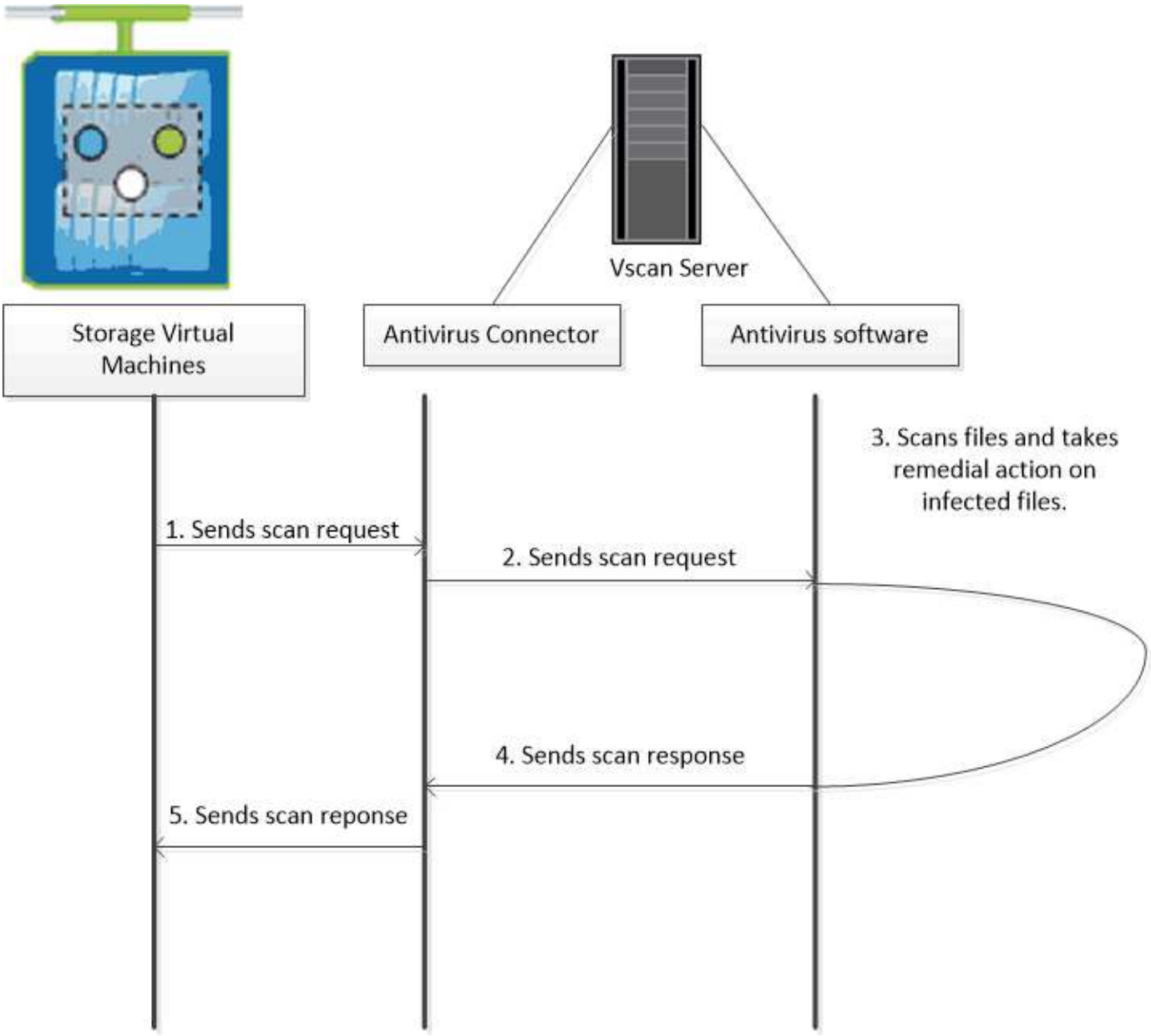
- Você pode usar *On-demand scanning* para verificar arquivos para vírus imediatamente ou em uma programação. Recomendamos que as verificações a pedido sejam executadas apenas em horas fora do pico para evitar sobrecarregar a infra-estrutura AV existente, que normalmente é dimensionada para a digitalização 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.

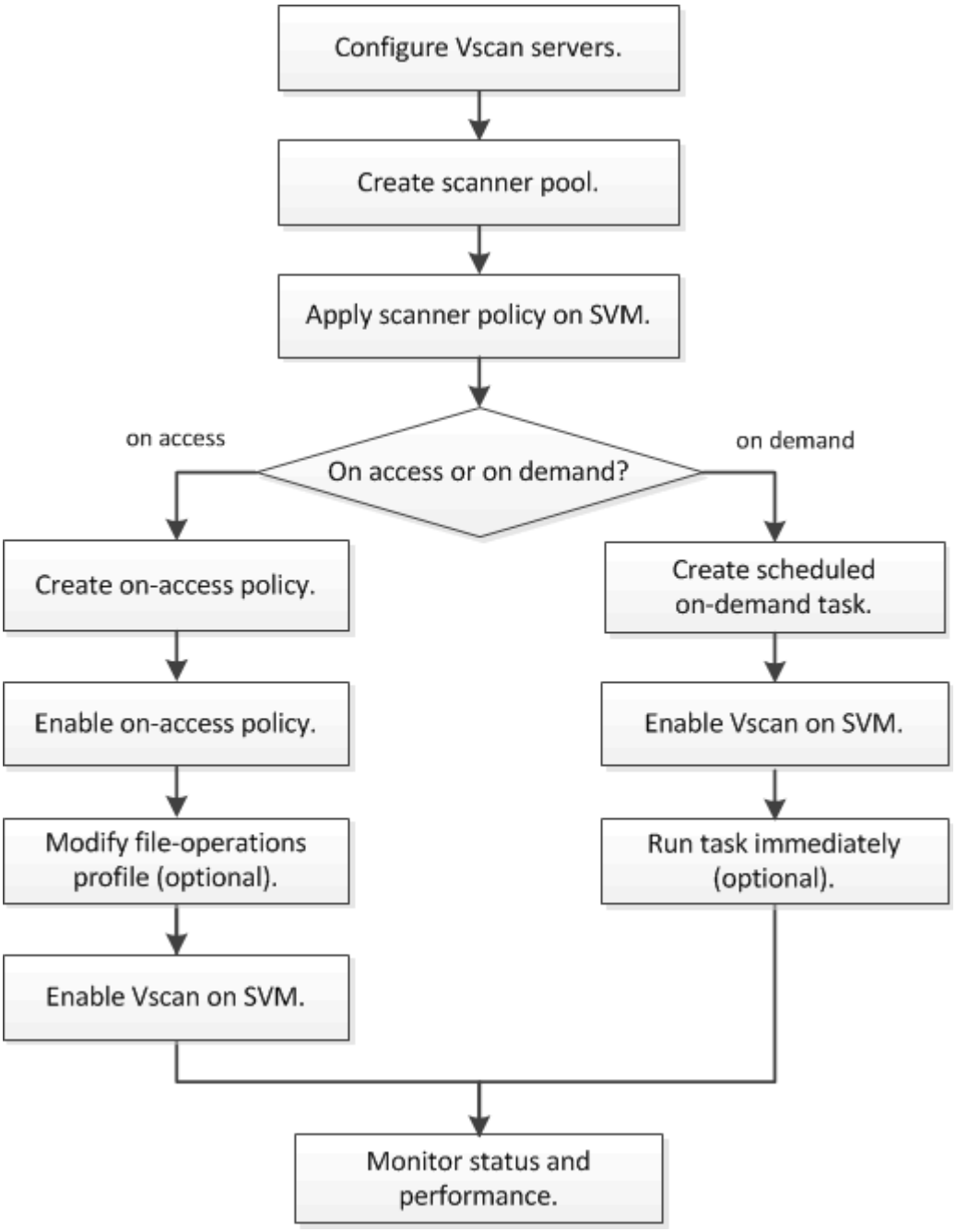
O conetor do antivírus ONTAP, fornecido pelo NetApp e instalado no servidor externo, lida com a comunicação entre o sistema de armazenamento e o software antivírus.



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)"
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)"

Parceiro	Documentação da solução	Detalhes de interoperabilidade
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"

Instalação e configuração do servidor Vscan

Instalação e configuração do servidor Vscan

Configure um ou mais servidores Vscan para garantir que os arquivos no seu sistema sejam verificados por vírus. Siga as instruções fornecidas pelo fornecedor para instalar e configurar o software antivírus no servidor.

Siga as instruções no arquivo README fornecido pelo NetApp para instalar e configurar o conetor antivírus do ONTAP. Em alternativa, siga as instruções na "Instale a página do conetor antivírus do ONTAP".

Para a recuperação de desastres e configurações do MetroCluster, é necessário configurar servidores Vscan separados para os clusters ONTAP primário, local e secundário/parceiro.

Requisitos de software antivírus

- Para obter informações sobre os requisitos de software antivírus, consulte a documentação do fornecedor.
- Para obter informações sobre os fornecedores, software e versões compatíveis com o Vscan, consulte a "Soluções de parceiros Vscan" página.

Requisitos do conetor antivírus do ONTAP

- Você pode baixar o conetor antivírus da ONTAP na página **Download de software** no site de suporte da

NetApp. "Downloads de NetApp: Software"

- Para obter informações sobre as versões do Windows suportadas pelo conetor antivírus do ONTAP e os requisitos de interoperabilidade, "Soluções de parceiros Vscan"consulte .

> Você pode instalar versões diferentes de servidores Windows para diferentes servidores Vscan em um cluster.

- .NET 3,0 ou posterior deve ser instalado no servidor Windows.
- O SMB 2,0 deve estar ativado no servidor Windows.

Instale o conetor antivírus do ONTAP

Instale o conetor do antivírus ONTAP no servidor Vscan para permitir a comunicação entre o sistema que executa o ONTAP e o servidor Vscan. Quando o conetor antivírus do ONTAP é instalado, o software antivírus consegue se comunicar com uma ou mais máquinas virtuais de armazenamento (SVMs).

Sobre esta tarefa

- Consulte a "Soluções de parceiros Vscan" página para obter informações sobre os protocolos suportados, versões de software de fornecedores de antivírus, versões do ONTAP, requisitos de interoperabilidade e servidores Windows.
- .NET 4.5.1 ou posterior deve ser instalado.
- O conetor do antivírus ONTAP pode ser executado em uma máquina virtual. No entanto, para obter o melhor desempenho, a NetApp recomenda o uso de uma máquina física dedicada para verificação de antivírus.
- O SMB 2,0 deve estar habilitado no servidor Windows no qual você está instalando e executando o conetor antivírus do ONTAP.

Antes de começar

- Faça o download do arquivo de configuração do conetor antivírus do ONTAP no site de suporte e salve-o em um diretório no disco rígido.
- Verifique se você atende aos requisitos para instalar o conetor antivírus do ONTAP.
- Verifique se você tem o Privileges administrador para instalar o conetor antivírus.

Passos

1. Inicie o assistente de instalação do Antivirus Connector executando o arquivo de configuração apropriado.
2. Selecione *Next*. Abre-se a caixa de diálogo pasta de destino.
3. Selecione *Next* para instalar o conetor antivírus na pasta listada ou selecione *Change* para instalar em uma pasta diferente.
4. A caixa de diálogo credenciais de serviço do Windows do conetor AV do ONTAP é aberta.
5. Insira suas credenciais de serviço do Windows ou selecione **Adicionar** para selecionar um usuário. Para um sistema ONTAP, esse usuário deve ser um usuário de domínio válido e deve existir na configuração do pool do scanner para o SVM.
6. Selecione **seguinte**. A caixa de diálogo Pronto para instalar o programa é aberta.
7. Selecione **Instalar** para iniciar a instalação ou selecione **voltar** se quiser fazer alterações nas configurações. Uma caixa de status é aberta e mostra o andamento da instalação, seguida pela caixa de

diálogo Assistente InstallShield concluído.

8. Marque a caixa de seleção Configurar LIFs do ONTAP se desejar continuar com a configuração do gerenciamento do ONTAP ou LIFs de dados. Você deve configurar pelo menos um ONTAP Management ou data LIF antes que este servidor Vscan possa ser usado.
9. Marque a caixa de seleção Mostrar o log **Windows Installer** se desejar exibir os logs de instalação.
10. Selecione **Finish** para terminar a instalação e fechar o assistente InstallShield. O ícone **Configurar LIFs ONTAP** é salvo na área de trabalho para configurar os LIFs ONTAP.
11. Adicione um SVM ao Antivirus Connector. Você pode adicionar um SVM ao conetor do antivírus adicionando um LIF de gerenciamento do ONTAP, que é polled para recuperar a lista de LIFs de dados ou configurando diretamente o LIF ou LIFs de dados. Você também deve fornecer as informações da enquete e as credenciais da conta de administrador do ONTAP se o LIF de gerenciamento do ONTAP estiver configurado.
    - Verifique se o LIF de gerenciamento ou o endereço IP do SVM está habilitado para `management-https`. Isso não é necessário quando você está configurando apenas LIFs de dados.
    - Verifique se você criou uma conta de usuário para o aplicativo HTTP e atribuiu uma função que tem (pelo menos somente leitura) acesso à `/api/network/ip/interfaces` API REST.
    - Saiba mais sobre `security login role create` e `security login create` no "Referência do comando ONTAP".

> Você também pode usar o usuário do domínio como uma conta adicionando um túnel de autenticação SVM para um SVM administrativo. Saiba mais sobre `security login domain-tunnel create` o "Referência do comando ONTAP"na .

Passos

1. Clique com o botão direito do Mouse no ícone **Configurar LIFs ONTAP**, que foi salvo em sua área de trabalho quando você concluiu a instalação do conetor antivírus e selecione **Executar como Administrador**.
2. Na caixa de diálogo Configurar LIFs ONTAP , selecione o tipo de configuração preferencial e execute as seguintes ações:

Para criar este tipo de LIF…	Execute estas etapas…
LIF de dados	a. Definir "função" para "dados" b. Definir "protocolo de dados" para "cifs" c. Defina "política de firewall" como "dados" d. Defina "Service policy" como "default-data-files" (ficheiros de dados predefinidos)
LIF de gerenciamento	a. Definir "função* como "dados" b. Defina "data Protocol" (protocolo de dados) para "None" (nenhum) c. Defina "política de firewall" como "mgmt" d. Defina "Service policy" (política de serviço) para "Default-Management" (gestão predefinida)

Leia mais sobre "Criando um LIF".

Depois de criar um LIF, insira os dados ou LIF de gerenciamento ou endereço IP do SVM que você deseja adicionar. Você também pode inserir o LIF de gerenciamento de cluster. Se você especificar o LIF de gerenciamento de cluster, todos os SVMs dentro desse cluster que estão atendendo SMB podem usar o servidor Vscan.

> Quando a autenticação Kerberos é necessária para servidores Vscan, cada LIF de dados SVM deve ter um nome DNS exclusivo e você deve Registrar esse nome como um nome principal do servidor (SPN) no ative Directory do Windows. Quando um nome DNS exclusivo não está disponível para cada LIF de dados ou registrado como um SPN, o servidor Vscan usa o mecanismo NT LAN Manager para autenticação. Se você adicionar ou modificar os nomes DNS e SPNs depois que o servidor Vscan estiver conetado, reinicie o serviço Antivirus Connector no servidor Vscan para aplicar as alterações.

3. Para configurar um LIF de gerenciamento, insira a duração da pesquisa em segundos. A duração da enquete é a frequência na qual o conetor antivírus verifica as alterações nas SVMs ou na configuração LIF do cluster. O intervalo padrão da enquete é de 60 segundos.
4. Introduza o nome e a palavra-passe da conta de administrador do ONTAP para configurar um LIF de gestão.
5. Clique em **Test** para verificar a conetividade e verificar a autenticação. A autenticação é verificada apenas para uma configuração de LIF de gerenciamento.
6. Clique em **Atualizar** para adicionar o LIF à lista de LIFs à pesquisa ou ao qual se conetar.
7. Clique em **Salvar** para salvar a conexão ao Registro.
8. Clique em **Exportar** se quiser exportar a lista de conexões para um arquivo de importação ou exportação de Registro. Isso é útil se vários servidores Vscan usarem o mesmo conjunto de gerenciamento ou LIFs de dados.

Consulte "Configure a página do conetor do antivírus ONTAP"para obter as opções de configuração.

Configure o conetor do antivírus ONTAP

Configure o conetor antivírus do ONTAP para especificar uma ou mais máquinas virtuais de armazenamento (SVMs) às quais você deseja se conetar, inserindo o LIF de gerenciamento do ONTAP, as informações de enquete e as credenciais da conta de administrador do ONTAP ou apenas o LIF de dados. Você também pode modificar os detalhes de uma conexão SVM ou remover uma conexão SVM. Por padrão, o conetor antivírus do ONTAP usa APIS REST para recuperar a lista de LIFs de dados se o LIF de gerenciamento do ONTAP estiver configurado.

Modifique os detalhes de uma conexão SVM

Você pode atualizar os detalhes de uma conexão de máquina virtual de armazenamento (SVM), que foi adicionada ao conetor antivírus, modificando o LIF de gerenciamento do ONTAP e as informações de enquete. Não é possível atualizar LIFs de dados depois de adicionados. Para atualizar LIFs de dados, primeiro você deve removê-los e adicioná-los novamente com o novo endereço IP ou LIF.

Antes de começar

Verifique se você criou uma conta de usuário para o aplicativo HTTP e atribuiu uma função que tem (pelo menos somente leitura) acesso à `/api/network/ip/interfaces` API REST.

Saiba mais sobre `security login role create` e `security login create` no "Referência do comando ONTAP".

Você também pode usar o usuário do domínio como uma conta adicionando um túnel de autenticação SVM para um SVM administrativo. Saiba mais sobre `security login domain-tunnel create` o "Referência do comando ONTAP"na .

Passos

1. Clique com o botão direito do Mouse no ícone **Configurar LIFs ONTAP**, que foi salvo em sua área de trabalho quando você concluiu a instalação do conetor antivírus e selecione **Executar como Administrador**. A caixa de diálogo Configurar LIFs ONTAP será aberta.
2. Selecione o endereço IP SVM e clique em **Update**.
3. Atualize as informações, conforme necessário.
4. Clique em **Salvar** para atualizar os detalhes da conexão no Registro.
5. Clique em **Exportar** se quiser exportar a lista de conexões para uma importação de Registro ou um arquivo de exportação de Registro. Isso é útil se vários servidores Vscan usarem o mesmo conjunto de gerenciamento ou LIFs de dados.

Remova uma conexão SVM do Antivirus Connector

Se você não precisar mais de uma conexão SVM, poderá removê-la.

Passos

1. Clique com o botão direito do Mouse no ícone **Configurar LIFs ONTAP**, que foi salvo em sua área de trabalho quando você concluiu a instalação do conetor antivírus e selecione **Executar como Administrador**. A caixa de diálogo Configurar LIFs ONTAP será aberta.
2. Selecione um ou mais endereços IP SVM e clique em **Remover**.
3. Clique em **Salvar** para atualizar os detalhes da conexão no Registro.
4. Clique em **Exportar** se quiser exportar a lista de conexões para um arquivo de importação ou exportação de Registro. Isso é útil se vários servidores Vscan usarem o mesmo conjunto de gerenciamento ou LIFs de dados.

Solucionar problemas

Antes de começar

Quando estiver criando valores de Registro neste procedimento, use o painel direito.

Você pode ativar ou desativar os logs do Antivirus Connector para fins de diagnóstico. Por padrão, esses logs são desativados. Para um melhor desempenho, você deve manter os logs do Antivirus Connector desabilitados e apenas habilitá-los para eventos críticos.

Passos

1. Selecione **Iniciar**, digite "regedit" na caixa de pesquisa e selecione `regedit.exe` na lista programas.
2. Em **Editor de Registro**, localize a seguinte subchave para o conetor antivírus do ONTAP: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Crie valores de Registro fornecendo o tipo, nome e valores mostrados na tabela a seguir:

Tipo	Nome	Valores

Cadeia de carateres	Tracepath	c: avshim.log

Este valor de registo pode ser qualquer outro caminho válido.

4. Crie outro valor de Registro fornecendo o tipo, nome, valores e informações de Registro mostradas na tabela a seguir:

Tipo	Nome	Registo crítico	Registo intermédio	Registro detalhado
DWORD	Tracelevel	1	2 ou 3	4

Isso permite que os logs do conetor antivírus sejam salvos no valor de caminho fornecido no TracePath na Etapa 3.

5. Desative os logs do Antivirus Connector excluindo os valores de Registro criados nas etapas 3 e 4.
6. Crie outro valor de Registro do tipo "MULTI_SZ" com o nome "LogRotation" (sem aspas). Em "LogRotation", forneça "logFileSize:1" como uma entrada para o tamanho de rotação (onde 1 representa 1MB) e na linha seguinte, forneça "logFileCount:5" como uma entrada para o limite de rotação (5 é o limite).

> Estes valores são opcionais. Se eles não forem fornecidos, os valores padrão de arquivos 20MB e 10 serão usados para o tamanho de rotação e limite de rotação, respetivamente. Os valores inteiros fornecidos não fornecem valores decimais ou frações. Se você fornecer valores superiores aos valores padrão, os valores padrão serão usados.

7. Para desativar a rotação de log configurada pelo usuário, exclua os valores do Registro criados na Etapa 6.

Banner personalizável

Um banner personalizado permite que você coloque uma declaração juridicamente vinculativa e uma isenção de responsabilidade de acesso ao sistema na janela *Configurar ONTAP API*.

Passo

1. Modifique o banner padrão atualizando o conteúdo do `banner.txt` arquivo no diretório de instalação e salvando as alterações. É necessário reabrir a janela Configurar API ONTAP LIF para ver as alterações refletidas no banner.

Ativar o modo de Ordenação alargada (eo)

Você pode ativar e desativar o modo Extended Ordinance (eo) para operação segura.

Passos

1. Selecione **Iniciar**, digite "regedit" na caixa de pesquisa e selecione `regedit.exe` na lista programas.
2. Em **Editor de Registro**, localize a seguinte subchave para o conetor antivírus do ONTAP: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. No painel do lado direito, crie um novo valor de Registro do tipo "DWORD" com o nome "eo_Mode" (sem aspas) e o valor "1" (sem aspas) para ativar o modo eo ou o valor "0" (sem aspas) para desativar o modo eo.

Por padrão, se a `EO_Mode` entrada do Registro estiver ausente, o modo eo será desativado. Ao ativar o modo eo, você deve configurar tanto o servidor syslog externo quanto a autenticação mútua de certificados.

Configure o servidor syslog externo

Antes de começar

Observe que quando você estiver criando valores de Registro neste procedimento, use o painel do lado direito.

Passos

1. Selecione **Iniciar**, digite "regedit" na caixa de pesquisa e selecione `regedit.exe` na lista programas.
2. Em **Editor de Registro**, crie a seguinte subchave para o conetor antivírus do ONTAP para configuração syslog: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0\syslog`
3. Crie um valor de Registro fornecendo o tipo, nome e valor, conforme mostrado na tabela a seguir:

Tipo	Nome	Valor
DWORD	syslog_enabled	1 ou 0

   Observe que um valor "1" ativa o syslog e um valor "0" o desativa.

4. Crie outro valor de Registro fornecendo as informações como mostrado na tabela a seguir:

Tipo	Nome
REG_SZ	Syslog_host

   Forneça o endereço IP do host syslog ou o nome de domínio para o campo valor.

5. Crie outro valor de Registro fornecendo as informações como mostrado na tabela a seguir:

Tipo	Nome
REG_SZ	Syslog_port

   Forneça o número da porta na qual o servidor syslog está sendo executado no campo valor.

6. Crie outro valor de Registro fornecendo as informações como mostrado na tabela a seguir:

Tipo	Nome
REG_SZ	Syslog_Protocol

   Insira o protocolo que está em uso no servidor syslog, "tcp" ou "udp", no campo valor.

7. Crie outro valor de Registro fornecendo as informações como mostrado na tabela a seguir:

Tipo	Nome	LOG_CRIT	LOG_NOTICE	LOG_INFO	LOG_DEBUG
DWORD	Syslog_level	2	5	6	7

8. Crie outro valor de Registro fornecendo as informações como mostrado na tabela a seguir:

Tipo	Nome	Valor
DWORD	syslog_tls	1 ou 0

Observe que um valor "1" ativa o syslog com Transport Layer Security (TLS) e um valor "0" desabilita o syslog com TLS.

Certifique-se de que um servidor syslog externo configurado seja executado sem problemas

- Se a chave estiver ausente ou tiver um valor nulo:
  - O protocolo é predefinido para "tcp".
  - A porta padrão é "514" para "tcp/udp" e padrão é "6514" para TLS.
  - O nível syslog é padrão para 5 (LOG_NOTICE).
- Você pode confirmar que o syslog está habilitado verificando se o `syslog_enabled` valor é "1". Quando o `syslog_enabled` valor é "1", você deve ser capaz de fazer login no servidor remoto configurado, quer o modo eo esteja ou não ativado.
- Se o modo eo estiver definido para "1" e alterar o `syslog_enabled` valor de "1" para "0", aplica-se o seguinte:
  - Não é possível iniciar o serviço se o syslog não estiver ativado no modo eo.
  - Se o sistema estiver sendo executado em um estado estável, um aviso aparece dizendo que syslog não pode ser desativado no modo eo e syslog está definido com força para "1", o que você pode ver no Registro. Se isso ocorrer, você deve desativar o modo eo primeiro e, em seguida, desativar syslog.
- Se o servidor syslog não conseguir executar com êxito quando o modo eo e syslog estão ativados, o serviço pára de ser executado. Isso pode ocorrer por um dos seguintes motivos:
  - Um syslog_host inválido ou nenhum syslog_host está configurado.
  - Um protocolo inválido, além de UDP ou TCP, está configurado.
  - Um número de porta é inválido.
- Para uma configuração TCP ou TLS sobre TCP, se o servidor não estiver escutando na porta IP, a conexão falhará e o serviço será encerrado.

Configurar a autenticação de certificado mútuo X,509

A autenticação mútua baseada em certificado X,509 é possível para a comunicação SSL (Secure Sockets Layer) entre o conetor antivírus e o ONTAP no caminho de gerenciamento. Se o modo eo estiver ativado e o certificado não for encontrado, o conetor AV será encerrado. Execute o seguinte procedimento no Antivirus Connector:

Passos

1. O conetor do antivírus procura o certificado do cliente do conetor do antivírus e o certificado da autoridade de certificação (CA) para o servidor NetApp no caminho do diretório a partir do qual o conetor do antivírus

executa o diretório de instalação. Copie os certificados para este caminho de diretório fixo.

2. Incorpore o certificado do cliente e sua chave privada no formato PKCS12 e nomeie-o "AV_client.P12".
3. Certifique-se de que o certificado de CA (juntamente com qualquer autoridade de assinatura intermediária até a CA raiz) usado para assinar o certificado para o servidor NetApp esteja no formato de email avançado de privacidade (PEM) e chamado "ONTAP_CA.pem". Coloque-o no diretório de instalação do conetor do antivírus. No sistema NetApp ONTAP, instale o certificado CA (juntamente com qualquer autoridade de assinatura intermediária até a CA raiz) usado para assinar o certificado de cliente para o conetor antivírus em "ONTAP" como um certificado de tipo "cliente-CA".

Configurar pools do scanner

Configure a visão geral dos pools de scanner

Um pool de scanners define os servidores Vscan e os usuários privilegiados que podem se conetar a SVMs. Uma política de scanner determina se um pool de scanner está ativo.

Se utilizar uma política de exportação num servidor SMB, tem de adicionar cada servidor Vscan à política de exportação.

Crie um pool de scanners em um único cluster

Um pool de scanners define os servidores Vscan e os usuários privilegiados que podem se conetar a SVMs. Você pode criar um pool de varredor para uma SVM individual ou para todos os SVMs em um cluster.

O que você vai precisar

- Os servidores SVMs e Vscan devem estar no mesmo domínio ou em domínios confiáveis.
- Para pools de scanners definidos para SVM individual, você precisa ter o ONTAP Antivirus Connector configurado com o SVM Management LIF ou LIF de dados SVM.
- Para pools de scanners definidos para todos os SVMs em um cluster, você deve ter configurado o conetor antivírus ONTAP com o LIF de gerenciamento de cluster.
- A lista de usuários privilegiados deve incluir a conta de usuário do domínio que o servidor Vscan usa para se conetar ao SVM.
- Depois que o pool do scanner estiver configurado, verifique o status da conexão com os servidores.

Passos

1. Criar um conjunto de scanners:

```
vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users
privileged_users
```

   - Especifique um SVM de dados para um pool definido para um SVM individual e especifique um SVM admin de cluster para um pool definido para todas as SVMs em um cluster.
   - Especifique um endereço IP ou FQDN para cada nome de host do servidor Vscan.
   - Especifique o domínio e o nome de usuário para cada usuário privilegiado. Para obter uma lista

completa de opções, consulte a página de manual do comando.

O comando a seguir cria um pool de scanner chamado `SP` na `vs1` SVM:

```
cluster1::> vserver vscan scanner-pool create -vserver vs1 -scanner-pool
SP -hostnames 1.1.1.1,vmwin204-27.fsct.nb -privileged-users
cifs\u1,cifs\u2
```

2. Verifique se o conjunto do scanner foi criado:

`vserver vscan scanner-pool show -vserver` *`data_SVM|cluster_admin_SVM`* `-scanner -pool` *`scanner_pool`*

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

O comando a seguir exibe os detalhes do `SP` pool do scanner:

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                    Vserver: vs1
                               Scanner Pool: SP
                             Applied Policy: idle
                             Current Status: off
          Cluster on Which Policy Is Applied: -
                    Scanner Pool Config Owner: vserver
        List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                     List of Privileged Users: cifs\u1, cifs\u2
```

Você também pode usar o `vserver vscan scanner-pool show` comando para exibir todos os pools de scanner em um SVM. Para obter a sintaxe de comando completa, consulte a página man para o comando.

Crie pools de scanner nas configurações do MetroCluster

É necessário criar pools de scanners primários e secundários em cada cluster em uma configuração do MetroCluster, correspondendo aos SVMs primárias e secundárias no cluster.

O que você vai precisar

- Os servidores SVMs e Vscan devem estar no mesmo domínio ou em domínios confiáveis.
- Para pools de scanners definidos para SVM individual, você precisa ter o ONTAP Antivirus Connector configurado com o SVM Management LIF ou LIF de dados SVM.

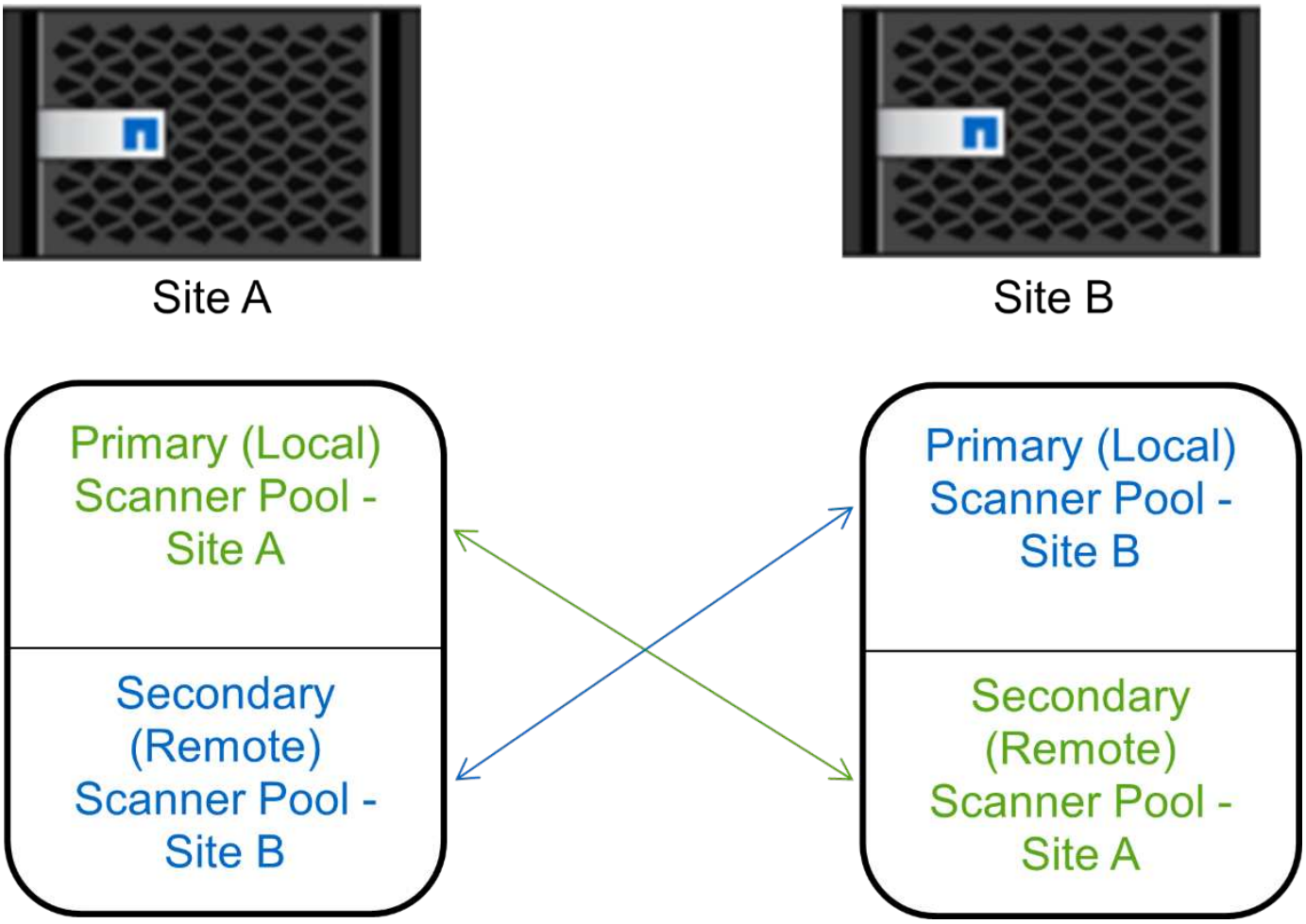
- Para pools de scanners definidos para todos os SVMs em um cluster, você deve ter configurado o conetor antivírus ONTAP com o LIF de gerenciamento de cluster.
- A lista de usuários privilegiados deve incluir a conta de usuário do domínio que o servidor Vscan usa para se conetar ao SVM.
- Depois que o pool do scanner estiver configurado, verifique o status da conexão com os servidores.

Sobre esta tarefa

As configurações do MetroCluster protegem os dados com a implementação de dois clusters espelhados separados fisicamente. Cada cluster replica de forma síncrona os dados e a configuração da SVM do outro. Um SVM principal no cluster local serve dados quando o cluster está on-line. Um SVM secundário no cluster local serve dados quando o cluster remoto está off-line.

Isso significa que você precisa criar pools de scanner primário e secundário em cada cluster em uma configuração do MetroCluster. O pool secundário fica ativo quando o cluster começa a fornecer dados do SVM secundário. Para recuperação de desastres (DR), a configuração é semelhante ao MetroCluster.

Esta figura mostra uma configuração típica de MetroCluster/DR.



Passos

1. Criar um conjunto de scanners:

   ```
   vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
   -pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users
   privileged_users
   ```

- Especifique um SVM de dados para um pool definido para um SVM individual e especifique um SVM admin de cluster para um pool definido para todas as SVMs em um cluster.
- Especifique um endereço IP ou FQDN para cada nome de host do servidor Vscan.
- Especifique o domínio e o nome de usuário para cada usuário privilegiado.

> É necessário criar todos os pools de scanner a partir do cluster que contém o SVM principal.

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

Os comandos a seguir criam pools de scanner primário e secundário em cada cluster em uma configuração do MetroCluster:

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site1 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site2 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site1 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site2 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2
```

2. Verifique se os pools do scanner foram criados:

   `vserver vscan scanner-pool show -vserver` *`data_SVM|cluster_admin_SVM`* `-scanner -pool` *`scanner_pool`*

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

   O comando a seguir exibe os detalhes do pool do scanner `pool1` :

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                                Scanner Pool: pool1_for_site1
                              Applied Policy: idle
                              Current Status: off
         Cluster on Which Policy Is Applied: -
                   Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                    List of Privileged Users: cifs\u1,cifs\u2
```

Você também pode usar o `vserver vscan scanner-pool show` comando para exibir todos os pools de scanner em um SVM. Para obter a sintaxe de comando completa, consulte a página man para o comando.

Aplique uma política de scanner em um único cluster

Uma política de scanner determina se um pool de scanner está ativo. Você deve ativar um pool de scanner antes que os servidores Vscan que ele define possam se conetar a um SVM.

Sobre esta tarefa

- Só é possível aplicar uma política de scanner a um conjunto de scanners.
- Se você criou um pool de scanners para todos os SVMs em um cluster, deverá aplicar uma política de scanner a cada SVM individualmente.

Passos

1. Aplicar uma política de scanner:

   ```
   vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
   scanner_pool -scanner-policy primary|secondary|idle -cluster
   cluster_to_apply_policy_on
   ```

   Uma política de scanner pode ter um dos seguintes valores:

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

   O exemplo a seguir mostra que o pool do scanner chamado `SP` na `vs1` SVM está ativo:

```
cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
-scanner-pool SP  -scanner-policy primary
```

2. Verifique se o conjunto do scanner está ativo:

   `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner -pool scanner_pool`

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

   O comando a seguir exibe os detalhes do `SP` pool do scanner:

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                    Vserver: vs1
                               Scanner Pool: SP
                             Applied Policy: primary
                             Current Status: on
         Cluster on Which Policy Is Applied: cluster1
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                   List of Privileged Users: cifs\u1, cifs\u2
```

   Você pode usar o `vserver vscan scanner-pool show-active` comando para exibir os pools de scanner ativos em um SVM. Para obter a sintaxe completa do comando, consulte a página man para o comando.

Aplique políticas de scanner nas configurações do MetroCluster

Uma política de scanner determina se um pool de scanner está ativo. Você deve aplicar uma política de scanner aos pools de scanner primário e secundário em cada cluster em uma configuração do MetroCluster.

Sobre esta tarefa

- Só é possível aplicar uma política de scanner a um conjunto de scanners.
- Se você criou um pool de scanners para todos os SVMs em um cluster, deverá aplicar uma política de scanner a cada SVM individualmente.
- Para configurações de recuperação de desastres e MetroCluster, você deve aplicar uma política de scanner a cada pool de scanners no cluster local e no cluster remoto.
- Na política criada para o cluster local, tem de especificar o cluster local no `cluster` parâmetro. Na política criada para o cluster remoto, tem de especificar o cluster remoto no `cluster` parâmetro. O cluster remoto pode então assumir operações de verificação de vírus em caso de desastre.

Passos

1. Aplicar uma política de scanner:

   ```
   vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
   scanner_pool -scanner-policy primary|secondary|idle -cluster
   cluster_to_apply_policy_on
   ```

   Uma política de scanner pode ter um dos seguintes valores:

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

   > É necessário aplicar todas as políticas de scanner a partir do cluster que contém o SVM principal.

   Os comandos a seguir aplicam políticas de scanner aos pools de scanner primário e secundário em cada cluster em uma configuração do MetroCluster:

   ```
   cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
   -scanner-pool pool1_for_site1 -scanner-policy primary -cluster cluster1

   cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
   -scanner-pool pool2_for_site1 -scanner-policy secondary -cluster
   cluster1

   cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
   -scanner-pool pool2_for_site2 -scanner-policy primary -cluster cluster2

   cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
   -scanner-pool pool1_for_site2 -scanner-policy secondary -cluster
   cluster2
   ```

2. Verifique se o conjunto do scanner está ativo:

   ```
   vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
   -pool scanner_pool
   ```

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

   O comando a seguir exibe os detalhes do pool do scanner `pool1` :

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                                Scanner Pool: pool1_for_site1
                              Applied Policy: primary
                              Current Status: on
          Cluster on Which Policy Is Applied: cluster1
                   Scanner Pool Config Owner: vserver
        List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                    List of Privileged Users: cifs\u1,cifs\u2
```

Você pode usar o `vserver vscan scanner-pool show-active` comando para exibir os pools de scanner ativos em um SVM. Para obter a sintaxe de comando completa, consulte a página man para o comando.

Comandos para gerenciar pools de scanner

Você pode modificar e excluir pools de scanner e gerenciar usuários privilegiados e servidores Vscan para um pool de scanner. Você também pode exibir informações resumidas sobre o pool do scanner.

Se você quiser…	Digite o seguinte comando…
Modifique um conjunto de scanners	`vserver vscan scanner-pool modify`
Exclua um pool de scanner	`vserver vscan scanner-pool delete`
Adicione usuários privilegiados a um pool de scanners	`vserver vscan scanner-pool privileged-users add`
Excluir usuários privilegiados de um pool de scanner	`vserver vscan scanner-pool privileged-users remove`
Adicione servidores Vscan a um pool de scanners	`vserver vscan scanner-pool servers add`
Excluir servidores Vscan de um pool de scanners	`vserver vscan scanner-pool servers remove`
Exibir resumo e detalhes de um pool de scanners	`vserver vscan scanner-pool show`
Exibir usuários privilegiados de um pool de scanners	`vserver vscan scanner-pool privileged-users show`

Veja os servidores Vscan para todos os pools de scanners	`vserver vscan scanner-pool servers show`

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

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 conetividade 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 ficheiros 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	`vserver vscan on-access-policy create`
Modificar uma política de acesso	`vserver vscan on-access-policy modify`
Ative uma política de acesso	`vserver vscan on-access-policy enable`
Desative uma política de acesso	`vserver vscan on-access-policy disable`
Eliminar uma política de acesso	`vserver vscan on-access-policy delete`
Veja o resumo e os detalhes de uma política de acesso	`vserver vscan on-access-policy show`
Adicionar à lista de caminhos a excluir	`vserver vscan on-access-policy paths-to-exclude add`
Excluir da lista de caminhos a serem excluídos	`vserver vscan on-access-policy paths-to-exclude remove`
Exibir a lista de caminhos a serem excluídos	`vserver vscan on-access-policy paths-to-exclude show`
Adicionar à lista de extensões de arquivo a excluir	`vserver vscan on-access-policy file-ext-to-exclude add`
Excluir da lista de extensões de arquivo a serem excluídas	`vserver vscan on-access-policy file-ext-to-exclude remove`
Veja a lista de extensões de arquivo a excluir	`vserver vscan on-access-policy file-ext-to-exclude show`
Adicionar à lista de extensões de arquivo a incluir	`vserver vscan on-access-policy file-ext-to-include add`
Excluir da lista de extensões de arquivo a incluir	`vserver vscan on-access-policy file-ext-to-include remove`

Veja a lista de extensões de arquivo a incluir	`vserver vscan on-access-policy file-ext-to-include show`

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

Configurar a digitalização a pedido

Configure a visão geral da digitalização a pedido

Você pode usar a verificação sob demanda para verificar arquivos para vírus imediatamente ou em um horário.

Você pode querer executar digitalizações apenas em horas fora do pico, por exemplo, ou você pode querer digitalizar arquivos muito grandes que foram excluídos de uma digitalização no acesso. Você pode usar um cronograma cron para especificar quando a tarefa é executada.

> 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.

Sobre este tópico

- Você pode atribuir um agendamento ao criar uma tarefa.
- Somente uma tarefa pode ser agendada de cada vez em um SVM.
- A digitalização sob demanda não suporta a digitalização de links simbólicos ou arquivos de fluxo.

> A digitalização sob demanda não suporta a digitalização de links simbólicos ou arquivos de fluxo.

> 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.

Crie uma tarefa sob demanda com o ONTAP

Uma tarefa sob demanda define o escopo da verificação de vírus sob demanda. Pode especificar o tamanho máximo dos ficheiros a digitalizar, as extensões e os caminhos dos ficheiros a incluir na digitalização e as extensões e caminhos dos ficheiros a excluir da digitalização. Os arquivos nos subdiretórios são verificados por padrão.

Sobre esta tarefa

- Pode existir no máximo 10 (dez) tarefas sob demanda para cada SVM, mas apenas uma pode estar ativa.
- Uma tarefa a pedido cria um relatório, que tem informações sobre as estatísticas relacionadas com as digitalizações. Este relatório é acessível com um comando ou baixando o arquivo de relatório criado pela tarefa no local definido.

Antes de começar

- Você deve ter criou uma política de acesso. A política pode ser uma política padrão ou criada pelo usuário. Sem a política de acesso, não é possível ativar a digitalização.

Passos

1. Crie uma tarefa sob demanda:

   ```
   vserver vscan on-demand-task create -vserver data_SVM -task-name task_name
   -scan-paths paths_of_files_to_scan -report-directory report_directory_path
   -report-expiry-time expiration_time_for_report -schedule cron_schedule -max
   -file-size max_size_of_files_to_scan -paths-to-exclude paths -file-ext-to
   -exclude file_extensions -file-ext-to-include file_extensions -scan-files-with
   -no-ext true|false -directory-recursion true|false
   ```

   - 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.

     Saiba mais sobre `vserver vscan on-demand-task create` o "Referência do comando ONTAP"na .

     O comando a seguir cria uma tarefa sob demanda chamada `Task1` no SVM VS1:

   ```
   cluster1::> vserver vscan on-demand-task create -vserver vs1 -task-name
   Task1 -scan-paths "/vol1/","/vol2/cifs/" -report-directory "/report"
   -schedule daily -max-file-size 5GB -paths-to-exclude "/vol1/cold-files/"
   -file-ext-to-include "vmdk?","mp*" -file-ext-to-exclude "mp3","mp4"
   -scan-files-with-no-ext false
   [Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"
   command to view the status.
   ```

   +

   > Pode utilizar o `job show` comando para visualizar o estado do trabalho. Pode utilizar os `job pause` comandos e `job resume` para pausar e reiniciar o trabalho ou o `job stop` comando para terminar o trabalho.

2. Verifique se a tarefa a pedido foi criada:

   ```
   vserver vscan on-demand-task show -instance data_SVM -task-name task_name
   ```

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

   O comando a seguir exibe os detalhes `Task1` da tarefa:

```
cluster1::> vserver vscan on-demand-task show -instance vs1 -task-name
Task1

                            Vserver: vs1
                          Task Name: Task1
                List of Scan Paths: /vol1/, /vol2/cifs/
             Report Directory Path: /report
                       Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk?, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
               Directory Recursion: true
                     Scan Priority: low
                  Report Log Level: info
        Expiration Time for Report: -
```

Depois de terminar

Você deve habilitar a digitalização no SVM antes que a tarefa seja agendada para ser executada.

Agende uma tarefa sob demanda

Você pode criar uma tarefa sem atribuir uma programação e usar o `vserver vscan on-demand-task schedule` comando para atribuir uma programação; ou adicionar uma programação ao criar a tarefa.

Sobre esta tarefa

A programação atribuída com o `vserver vscan on-demand-task schedule` comando substitui uma programação já atribuída com o `vserver vscan on-demand-task create` comando.

Passos

1. Agendar uma tarefa a pedido:

   `vserver vscan on-demand-task schedule -vserver` *`data_SVM`* `-task-name` *`task_name`* `-schedule cron_schedule`

   O comando a seguir agenda uma tarefa de acesso chamada `Task2` no `vs2` SVM:

```
cluster1::> vserver vscan on-demand-task schedule -vserver vs2 -task
-name Task2 -schedule daily
[Job 142]: Vscan On-Demand job is queued. Use the "job show -id 142"
command to view the status.
```

Para ver o estado do trabalho, utilize o `job show` comando . Os `job pause` comandos e `job resume`, respetivamente, pausam e reiniciam a tarefa; o `job stop` comando termina a tarefa.

2. Verifique se a tarefa a pedido foi agendada:

   `vserver vscan on-demand-task show -instance` *`data_SVM`* `-task-name` *`task_name`*

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

   O comando a seguir exibe os detalhes `Task 2` da tarefa:

```
cluster1::> vserver vscan on-demand-task show -instance vs2 -task-name
Task2

                           Vserver: vs2
                         Task Name: Task2
                List of Scan Paths: /vol1/, /vol2/cifs/
             Report Directory Path: /report
                      Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
                Directory Recursion: true
                      Scan Priority: low
                   Report Log Level: info
```

Depois de terminar

Você deve habilitar a digitalização no SVM antes que a tarefa seja agendada para ser executada.

Execute uma tarefa sob demanda imediatamente

Você pode executar uma tarefa sob demanda imediatamente, independentemente de ter atribuído ou não uma programação.

Antes de começar

Você deve ter habilitado a verificação na SVM.

Passo

1. Execute uma tarefa sob demanda imediatamente:

   `vserver vscan on-demand-task run -vserver` *`data_SVM`* `-task-name` *`task_name`*

   O comando a seguir executa uma tarefa de acesso chamada `Task1` no `vs1` SVM:

```
cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name
Task1
[Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161"
command to view the status.
```

> Pode utilizar o `job show` comando para visualizar o estado do trabalho. Pode utilizar os `job pause` comandos e `job resume` para pausar e reiniciar o trabalho ou o `job stop` comando para terminar o trabalho.

Comandos para gerenciar tarefas sob demanda

Você pode modificar, excluir ou desagendar uma tarefa sob demanda. Você pode exibir um resumo e detalhes da tarefa e gerenciar relatórios para a tarefa.

Se você quiser…	Digite o seguinte comando…
Crie uma tarefa sob demanda	`vserver vscan on-demand-task create`
Modifique uma tarefa sob demanda	`vserver vscan on-demand-task modify`
Eliminar uma tarefa a pedido	`vserver vscan on-demand-task delete`
Execute uma tarefa sob demanda	`vserver vscan on-demand-task run`
Agende uma tarefa sob demanda	`vserver vscan on-demand-task schedule`
Anule a programação de uma tarefa sob demanda	`vserver vscan on-demand-task unschedule`
Exibir resumo e detalhes de uma tarefa sob demanda	`vserver vscan on-demand-task show`
Veja relatórios sob demanda	`vserver vscan on-demand-task report show`
Eliminar relatórios a pedido	`vserver vscan on-demand-task report delete`

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

Práticas recomendadas para configurar a funcionalidade antivírus off-box no ONTAP

Considere as seguintes recomendações para configurar a funcionalidade off-box no ONTAP.

- Restringir usuários privilegiados a operações de verificação de vírus. Os usuários normais devem ser desencorajados a usar credenciais de usuário privilegiadas. Essa restrição pode ser alcançada desativando os direitos de login para usuários privilegiados no ative Directory.
- Os usuários privilegiados não precisam fazer parte de nenhum grupo de usuários que tenha um grande número de direitos no domínio, como o grupo administradores ou o grupo de operadores de backup. Os usuários privilegiados devem ser validados apenas pelo sistema de armazenamento para que eles possam criar conexões de servidor Vscan e acessar arquivos para verificação de vírus.
- Use os computadores que executam servidores Vscan apenas para fins de verificação de vírus. Para desencorajar o uso geral, desative os serviços de terminal do Windows e outras disposições de acesso remoto nessas máquinas e conceda o direito de instalar novos softwares nessas máquinas somente aos administradores.
- Dedique os servidores Vscan à verificação de vírus e não os use para outras operações, como backups. Você pode decidir executar o servidor Vscan como uma máquina virtual (VM). Se você executar o servidor Vscan como uma VM, certifique-se de que os recursos alocados à VM não sejam compartilhados e sejam suficientes para executar a verificação de vírus.
- Fornecer CPU, memória e capacidade de disco adequados ao servidor Vscan para evitar a alocação excessiva de recursos. A maioria dos servidores Vscan são projetados para usar vários servidores centrais da CPU e para distribuir a carga entre as CPUs.
- A NetApp recomenda o uso de uma rede dedicada com uma VLAN privada para a conexão do SVM ao servidor Vscan para que o tráfego de varredura não seja afetado por outro tráfego de rede cliente. Crie uma placa de interface de rede (NIC) separada dedicada à VLAN antivírus no servidor Vscan e ao LIF de dados na SVM. Esta etapa simplifica a administração e a solução de problemas se surgirem problemas de rede. O tráfego antivírus deve ser segregado usando uma rede privada. O servidor antivírus deve ser configurado para se comunicar com o controlador de domínio (DC) e o ONTAP de uma das seguintes maneiras:
  - O DC deve se comunicar com os servidores antivírus através da rede privada que é usada para segregar o tráfego.
  - O DC e o servidor antivírus devem se comunicar através de uma rede diferente (não a rede privada mencionada anteriormente), que não é a mesma que a rede cliente CIFS.
  - Para ativar a autenticação Kerberos para comunicação antivírus, crie uma entrada DNS para os LIFs privados e um nome principal de serviço no DC correspondente à entrada DNS criada para o LIF privado. Use esse nome ao adicionar um LIF ao conetor do antivírus. O DNS deve ser capaz de retornar um nome exclusivo para cada LIF privado conetado ao conetor Antivirus.

> Se o LIF para tráfego Vscan for configurado em uma porta diferente do LIF para tráfego de cliente, o Vscan LIF pode falhar para outro nó se ocorrer uma falha de porta. A alteração faz com que o servidor Vscan não seja acessível a partir do novo nó e as notificações de digitalização para operações de arquivo no nó falharem. Verifique se o servidor Vscan está acessível através de pelo menos um LIF em um nó para que ele possa processar solicitações de digitalização para operações de arquivo executadas nesse nó.

- Conete o sistema de armazenamento NetApp e o servidor Vscan usando pelo menos uma rede 1GbEG.

- Para um ambiente com vários servidores Vscan, conete todos os servidores com conexões de rede semelhantes de alto desempenho. Conetar os servidores Vscan melhora o desempenho permitindo o compartilhamento de carga.
- Para locais remotos e filiais, a NetApp recomenda o uso de um servidor Vscan local em vez de um servidor Vscan remoto porque o primeiro é um candidato perfeito para alta latência. Se o custo for um fator, use um laptop ou PC para proteção moderada contra vírus. Você pode agendar verificações periódicas completas do sistema de arquivos compartilhando os volumes ou qtrees e digitalizando-os a partir de qualquer sistema no local remoto.
- Use vários servidores Vscan para verificar os dados no SVM para fins de balanceamento de carga e redundância. A quantidade de carga de trabalho CIFS e o tráfego antivírus resultante variam de acordo com a SVM. Monitore a latência de CIFS e verificação de vírus no controlador de storage. Monitore a tendência dos resultados ao longo do tempo. Se a latência CIFS e a latência de verificação de vírus aumentarem devido às filas de CPU ou de aplicativos nos servidores Vscan além dos limites de tendência, os clientes CIFS podem ter longos tempos de espera. Adicione servidores Vscan adicionais para distribuir a carga.
- Instale a versão mais recente do ONTAP Antivirus Connector.
- Mantenha os mecanismos e definições antivírus atualizados. Consulte os parceiros para obter recomendações sobre a frequência com que você deve atualizar.
- Em um ambiente de alocação a vários clientes, um pool de scanners (pool de servidores Vscan) pode ser compartilhado com vários SVMs, desde que os servidores Vscan e os SVMs façam parte do mesmo domínio ou domínio confiável.
- A política de software antivírus para arquivos infetados deve ser definida como "excluir" ou "quarentena", que é o valor padrão definido pela maioria dos fornecedores de antivírus. Se o "vscan-fileop-profile" estiver definido como "write_only", e se um arquivo infetado for encontrado, o arquivo permanece no compartilhamento e pode ser aberto porque a abertura de um arquivo não aciona uma verificação. A verificação antivírus é acionada apenas depois de o ficheiro ser fechado.
- O `scan-engine timeout` valor deve ser inferior ao `scanner-pool request-timeout` valor. Se estiver definido para um valor mais alto, o acesso aos arquivos pode ser atrasado e eventualmente acabar. Para evitar isso, configure o `scan-engine timeout` para 5 segundos menos do que o `scanner-pool request-timeout` valor. Consulte a documentação do fornecedor do mecanismo de digitalização para obter instruções sobre como alterar as `scan-engine timeout` configurações. O `scanner-pool timeout` pode ser alterado usando o seguinte comando no modo avançado e fornecendo o valor apropriado para o `request-timeout` parâmetro: `vserver vscan scanner-pool modify`.
- Para um ambiente dimensionado para cargas de trabalho de verificação de acesso e que exija o uso da verificação sob demanda, a NetApp recomenda agendar o trabalho de verificação sob demanda em horas fora do horário de pico para evitar cargas adicionais na infraestrutura antivírus existente.

Saiba mais sobre as práticas recomendadas específicas dos parceiros em "Soluções de parceiros Vscan".

Ative a verificação de vírus em um SVM

Você deve habilitar a verificação de vírus em uma SVM antes de uma verificação sob demanda ou de acesso poder ser executada.

Passos

1. Ativar a verificação de vírus em um SVM:

   ```
   vserver vscan enable -vserver data_SVM
   ```

Você pode usar o `vserver vscan disable` comando para desativar a verificação de vírus, se necessário.

O seguinte comando permite a verificação de vírus na `vs1` SVM:

```
cluster1::> vserver vscan enable -vserver vs1
```

2. Verifique se a verificação de vírus está ativada na SVM:

   `vserver vscan show -vserver data_SVM`

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

   O comando a seguir exibe o status Vscan do `vs1` SVM:

```
cluster1::> vserver vscan show -vserver vs1

                          Vserver: vs1
                     Vscan Status: on
```

Repor o estado dos ficheiros lidos

Ocasionalmente, você pode querer redefinir o status de digitalização de arquivos digitalizados com êxito em um SVM usando o `vserver vscan reset` comando para descartar as informações em cache dos arquivos. Você pode querer usar este comando para reiniciar o processamento de verificação de vírus em caso de uma verificação mal configurada, por exemplo.

Sobre esta tarefa

Depois de executar o `vserver vscan reset` comando, todos os arquivos elegíveis serão verificados da próxima vez que forem acessados.

Este comando pode afetar negativamente o desempenho, dependendo do número e tamanho dos arquivos a serem regravados.

Antes de começar

São necessários Privileges avançados para esta tarefa.

Passos

1. Alterar para nível de privilégio avançado:

   `set -privilege advanced`

2. Repor o estado dos ficheiros lidos:

   `vserver vscan reset -vserver data_SVM`

O comando a seguir redefine o status dos arquivos digitalizados `vs1` no SVM:

```
cluster1::> vserver vscan reset -vserver vs1
```

Ver informações do registo de eventos Vscan

Você pode usar o `vserver vscan show-events` comando para exibir informações de log de eventos sobre arquivos infetados, atualizações para servidores Vscan e similares. Você pode exibir informações de eventos para o cluster ou para determinados nós, SVMs ou servidores Vscan.

Antes de começar

São necessários Privileges avançados para visualizar o registo de eventos Vscan.

Passos

1. Alterar para nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Ver informações do registo de eventos Vscan:

   ```
   vserver vscan show-events
   ```

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

   O comando a seguir exibe informações de log de eventos para o cluster `cluster1`:

   ```
   cluster1::*> vserver vscan show-events

   Vserver     Node            Server          Event Type        Event Time
   ----------- --------------- --------------- -----------------
   -----------------
   vs1         Cluster-01      192.168.1.1     file-infected     9/5/2014
   11:37:38
   vs1         Cluster-01      192.168.1.1     scanner-updated   9/5/2014
   11:37:08
   vs1         Cluster-01      192.168.1.1     scanner-connected 9/5/2014
   11:34:55
   3 entries were displayed.
   ```

Monitore e solucione problemas de conetividade

Potenciais problemas de conetividade envolvendo a opção de digitalização obrigatória

Você pode usar os `vserver vscan connection-status show` comandos para exibir informações sobre as conexões do servidor Vscan que você pode achar útil na solução de problemas de conetividade.

Por padrão, a `scan-mandatory` opção de digitalização no acesso nega o acesso aos arquivos quando uma conexão do servidor Vscan não está disponível para digitalização. Embora esta opção ofereça caraterísticas de segurança importantes, pode levar a problemas em algumas situações.

- Antes de ativar o acesso do cliente, você deve garantir que pelo menos um servidor Vscan esteja conetado a um SVM em cada nó que tenha um LIF. Se você precisar conetar servidores a SVMs depois de habilitar o acesso ao cliente, desative a `scan-mandatory` opção no SVM para garantir que o acesso ao arquivo não seja negado porque uma conexão com o servidor Vscan não está disponível. Você pode ativar a opção novamente depois que o servidor tiver sido conetado.
- Se um LIF de destino hospedar todas as conexões do servidor Vscan para um SVM, a conexão entre o servidor e o SVM será perdida se o LIF for migrado. Para garantir que o acesso ao arquivo não seja negado porque uma conexão de servidor Vscan não está disponível, você deve desativar a `scan-mandatory` opção antes de migrar o LIF. Você pode ativar a opção novamente após a migração do LIF.

Cada SVM deve ter pelo menos dois servidores Vscan atribuídos a ele. É uma prática recomendada conetar servidores Vscan ao sistema de armazenamento através de uma rede diferente da usada para acesso ao cliente.

Comandos para visualizar o estado da ligação do servidor Vscan

Pode utilizar os `vserver vscan connection-status show` comandos para visualizar informações resumidas e detalhadas sobre o estado da ligação do servidor Vscan.

Se você quiser…	Digite o seguinte comando…
Ver um resumo das ligações do servidor Vscan	`vserver vscan connection-status show`
Ver detalhes das ligações do servidor Vscan	`vserver vscan connection-status show-all`
Ver detalhes dos servidores Vscan ligados	`vserver vscan connection-status show-connected`
Ver detalhes dos servidores Vscan disponíveis que não estão ligados	`vserver vscan connection-status show-not-connected`

Para obter mais informações sobre esses comandos, consulte "Páginas de manual do ONTAP".

Solucionar problemas de verificação de vírus

Para problemas comuns de verificação de vírus, existem possíveis causas e maneiras de

resolvê-los. A verificação de vírus também é conhecida como Vscan.

Problema	Como resolvê-lo
Os servidores Vscan não conseguem se conetar ao sistema de armazenamento ONTAP em cluster.	Verifique se a configuração do conjunto do scanner especifica o endereço IP do servidor Vscan. Verifique também se os utilizadores privilegiados permitidos na lista de conjuntos de scanners estão ativos. Para verificar o conjunto do scanner, execute o `vserver vscan scanner-pool show` comando no prompt de comando do sistema de armazenamento. Se os servidores Vscan ainda não puderem se conetar, pode haver um problema com a rede.
Os clientes observam alta latência.	Provavelmente é hora de adicionar mais servidores Vscan ao pool do scanner.
Demasiados exames são acionados.	Modifique o valor `vscan-fileop-profile` do parâmetro para restringir o número de operações de arquivo monitoradas para verificação de vírus.
Alguns ficheiros não estão a ser lidos.	Verifique a política de acesso. É possível que o caminho para esses arquivos tenha sido adicionado à lista de exclusão de caminho ou que seu tamanho exceda o valor configurado para exclusões. Para verificar a política de acesso, execute o `vserver vscan on-access-policy show` comando no prompt de comando do sistema de armazenamento.
O acesso ao ficheiro foi negado.	Verifique se a definição *scan-mandatory* está especificada na configuração da política. Esta configuração nega o acesso aos dados se nenhum servidor Vscan estiver conetado. Modifique a configuração conforme necessário.

Monitorar as atividades de status e desempenho

Você pode monitorar os aspetos críticos do módulo Vscan, como o status da conexão do servidor Vscan, a integridade dos servidores Vscan e o número de arquivos verificados. Estas informações ajudam-no a diagnosticar problemas relacionados com o servidor Vscan.

Veja as informações de conexão do servidor Vscan

Pode visualizar o estado da ligação dos servidores Vscan para gerir as ligações que já estão a ser utilizadas e as ligações que estão disponíveis para utilização. Vários comandos exibem informações sobre o status da conexão dos servidores Vscan.

Comando…	Informações exibidas…

`vserver vscan connection-status show`	Resumo do estado da ligação
`vserver vscan connection-status show-all`	Informações detalhadas sobre o estado da ligação
`vserver vscan connection-status show-not-connected`	Estado das ligações disponíveis mas não ligadas
`vserver vscan connection-status show-connected`	Informações sobre o servidor Vscan conetado

Ver estatísticas do servidor Vscan

Você pode visualizar estatísticas específicas do servidor Vscan para monitorar o desempenho e diagnosticar problemas relacionados à verificação de vírus. Você deve coletar uma amostra de dados antes de usar o `statistics show` comando para exibir as estatísticas do servidor Vscan. Para concluir um exemplo de dados, execute o seguinte passo:

Passo

1. Executar o `statistics start` comando e o `optional statistics` comando STOP.

Exibir estatísticas para solicitações e latências de servidor Vscan

Você pode usar contadores ONTAP `offbox_vscan` por SVM para monitorar a taxa de solicitações do servidor Vscan que são enviadas e recebidas por segundo e as latências de servidor em todos os servidores Vscan. Para visualizar estas estatísticas, execute o seguinte passo:

Passo

1. Execute o comando statistics show `object offbox_vscan –instance SVM` com os seguintes contadores:

Contador…	Informações exibidas…
`scan_request_dispatched_rate`	Número de solicitações de verificação de vírus enviadas do ONTAP para os servidores Vscan por segundo
`scan_noti_received_rate`	Número de solicitações de verificação de vírus recebidas de volta pelo ONTAP a partir dos servidores Vscan por segundo
`dispatch_latency`	Latência no ONTAP para identificar um servidor Vscan disponível e enviar a solicitação para esse servidor Vscan
`scan_latency`	Latência de ida e volta do ONTAP para o servidor Vscan, incluindo o tempo para a digitalização ser executada

Exemplo de estatísticas geradas a partir de um contador vscan ONTAP offbox

```
Object: offbox_vscan
Instance: SVM
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 2 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_noti_received_rate 292
dispatch_latency 43986us
scan_latency 3433501us
-------------------------------------------------------------------
```

Exibir estatísticas para solicitações e latências individuais de servidor Vscan

Você pode usar contadores ONTAP `offbox_vscan_server` em um servidor Vscan por SVM, por servidor Vscan e por nó para monitorar a taxa de solicitações de servidor Vscan enviadas e a latência do servidor em cada servidor Vscan individualmente. Para coletar essas informações, execute o seguinte passo:

Passo

1. Execute o `statistics show –object offbox_vscan –instance SVM:servername:nodename` comando com os seguintes contadores:

Contador…	Informações exibidas…
`scan_request_dispatched_rate`	Número de solicitações de verificação de vírus enviadas do ONTAP
`scan_latency`	Latência de ida e volta do ONTAP para o servidor Vscan, incluindo o tempo para a digitalização ser executada para os servidores Vscan por segundo

Exemplo de estatísticas geradas a partir de um contador ONTAP offbox_vscan_Server

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_latency 3433830us
-------------------------------------------------------------------
```

Exibir estatísticas para a utilização do servidor Vscan

Você também pode usar contadores ONTAP `offbox_vscan_server` para coletar estatísticas de utilização do servidor Vscan. Essas estatísticas são rastreadas por SVM, por servidor Vscan e por nó. Eles incluem utilização de CPU no servidor Vscan, profundidade de fila para operações de digitalização no servidor Vscan (atual e máximo), memória usada e rede usada. Essas estatísticas são encaminhadas pelo conetor antivírus para os contadores de estatísticas dentro do ONTAP. Eles são baseados em dados que são polidos a cada 20 segundos e devem ser coletados várias vezes para precisão; caso contrário, os valores vistos nas estatísticas refletem apenas a última sondagem. A utilização da CPU e as filas são particularmente importantes para monitorar e analisar. Um valor alto para uma fila média pode indicar que o servidor Vscan tem um gargalo. Para coletar estatísticas de utilização do servidor Vscan por SVM, por servidor Vscan e por nó, execute a seguinte etapa:

Passo

1. Colete estatísticas de utilização para o servidor Vscan

   Execute o `statistics show –object offbox_vscan_server –instance SVM:servername:nodename` comando com os `offbox_vscan_server` seguintes contadores:

Contador…	Informações exibidas…
`scanner_stats_pct_cpu_used`	Utilização da CPU no servidor Vscan
`scanner_stats_pct_input_queue_avg`	Fila média de pedidos de leitura no servidor Vscan
`scanner_stats_pct_input_queue_hiwaterma rk`	Fila de pico de pedidos de leitura no servidor Vscan
`scanner_stats_pct_mem_used`	Memória utilizada no servidor Vscan
`scanner_stats_pct_network_used`	Rede utilizada no servidor Vscan

Exemplo de estatísticas de utilização para o servidor Vscan

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scanner_stats_pct_cpu_used 51
scanner_stats_pct_dropped_requests 0
scanner_stats_pct_input_queue_avg 91
scanner_stats_pct_input_queue_hiwatermark 100
scanner_stats_pct_mem_used 95
scanner_stats_pct_network_used 4
---------------------------------------------------------------
```

Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

Informações sobre direitos autorais

Informações sobre marcas comerciais