Instalação e configuração do servidor Vscan

ONTAP 9

NetApp
January 17, 2025

Índice

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".

Informações sobre direitos autorais

Informações sobre marcas comerciais