



Documentação do ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

Índice

Documentação do ONTAP tools for VMware vSphere	1
Notas de lançamento	2
Notas de lançamento para ONTAP tools	2
Novidades no ONTAP tools for VMware vSphere 10.5	2
Plataformas ONTAP e versões do servidor vCenter suportadas	3
Comparação de recursos das ferramentas ONTAP para VMware vSphere 9 e 10	3
Conceitos	5
Saiba mais sobre as ferramentas ONTAP	5
Conceitos e termos-chave nas ferramentas ONTAP	5
Controle de acesso baseado em funções (RBAC)	8
Saiba mais sobre as ferramentas RBAC do ONTAP	8
RBAC com VMware vSphere	10
RBAC com ONTAP	17
Implante ONTAP tools for VMware vSphere	21
Guia rápido para ONTAP tools for VMware vSphere	21
Fluxo de trabalho de implantação de alta disponibilidade para ONTAP tools	23
Requisitos e limites de configuração do ONTAP tools for VMware vSphere	24
Requisitos do sistema	24
Requisitos mínimos de storage e de aplicativos	24
Requisitos de porta	25
Limites de configuração para implantar ONTAP tools for VMware vSphere para datastores vVols	27
Limitações de configuração para implantar ONTAP tools for VMware vSphere para datastores VMFS e NFS	28
ONTAP tools for VMware vSphere - Adaptador de Replicação de Storage (SRA)	28
Requisitos de pré-implantação para ONTAP tools	29
Planilha de implantação	30
Configuração do firewall de rede	31
Configurações de armazenamento ONTAP	31
Implantar ONTAP tools	31
Solucionar erros de implantação das ONTAP tools	37
Colete os arquivos de log	37
Códigos de erro de implantação	37
Configurar ONTAP tools para VMware vSphere	41
Adicionar instâncias do servidor vCenter às ONTAP tools	41
Registre o provedor VASA com uma instância do vCenter Server nas ONTAP tools	42
Instale o plug-in NFS VAAI usando as ONTAP tools	43
Configure as configurações do host ESXi nas ONTAP tools	44
Configurar as definições de multipath e tempo limite do servidor ESXi	44
Defina os valores do host ESXi	44
Configure funções e privilégios de usuário do ONTAP para ONTAP tools	45
Requisitos de mapeamento de agregado SVM	46
Criar usuário e função do ONTAP manualmente	47
Atualize o ONTAP tools for VMware vSphere 10.1 user para 10.3 user	55

Atualize o usuário do ONTAP tools for VMware vSphere 10.3 para o usuário 10.4	57
Adicionar um backend de armazenamento às ferramentas ONTAP	57
Associe um backend de armazenamento a uma instância do servidor vCenter nas ONTAP tools	60
Configure o acesso à rede nas ONTAP tools	60
Criar um datastore nas ONTAP tools	61
Proteja armazenamentos de dados e máquinas virtuais	66
Proteja um cluster de hosts nas ONTAP tools	66
Proteja usando a proteção SRA	67
Configure o SRA nas ONTAP tools para proteger datastores	67
Configure o SRA em ONTAP tools for VMware vSphere para ambientes SAN e NAS	68
Configure o SRA nas ONTAP tools para ambientes altamente escaláveis	69
Configure o SRA no appliance VMware Live Site Recovery usando as ONTAP tools	70
Atualizar credenciais SRA nas ferramentas ONTAP	71
Configure sites protegidos e de recuperação nas ferramentas ONTAP	72
Configure os recursos do site protegido e do site de recuperação	74
Verifique os sistemas de armazenamento replicados nas ferramentas ONTAP	78
Proteção contra fan-out em ONTAP tools	78
Gerencie as ferramentas ONTAP para VMware vSphere	82
Saiba mais sobre o painel de ferramentas do ONTAP	82
Como as ONTAP tools gerenciam igroups e políticas de exportação	83
Políticas de exportação	87
Como as ONTAP tools gerenciam igroups	88
Resumo rápido do comportamento	88
Contextos de igroup	88
Comportamento de nomeação	90
Comportamento por cenário	90
Reutilização de igroup personalizado e comportamento da API	91
Visão de conversão de nativo para gerenciado	91
Reutilização de igroups nativos descobertos	92
Saiba mais sobre a interface de usuário do ONTAP tools Manager	92
Gerenciar configurações do ONTAP tools Manager	94
Editar configurações do AutoSupport das ferramentas ONTAP	94
Adicionar servidores NTP às ferramentas ONTAP	95
Redefina as credenciais do VASA Provider e do SRA nas ONTAP tools	95
Editar configurações de backup das ferramentas ONTAP	96
Habilitar os serviços do ONTAP tools	96
Alterar as configurações do appliance ONTAP tools	97
Adicionar hosts VMware vSphere às ONTAP tools	98
Gerenciar datastores	99
Montar datastores NFS e VMFS nas ONTAP tools	99
Desmontar datastores NFS e VMFS nas ONTAP tools	99
Montar um datastore vVols nas ONTAP tools	100
Redimensionar datastores NFS e VMFS nas ONTAP tools	100
Expandir vVols datastores nas ONTAP tools	101
Reduzir um datastore vVols nas ONTAP tools	101

Excluir datastores nas ONTAP tools	102
Visualizações de armazenamento ONTAP para datastores em ONTAP tools	103
Visualização do armazenamento da máquina virtual nas ferramentas ONTAP	103
Gerencie os limites de armazenamento nas ONTAP tools	104
Gerencie back-ends de armazenamento nas ONTAP tools	104
Descubra o storage	104
Modificar os storage backends	104
Remover backends de storage	105
Visão detalhada do storage backend	105
Gerencie instâncias do servidor vCenter nas ONTAP tools	106
Desassocie os backends de armazenamento da instância do servidor vCenter	106
Modificar uma instância do servidor vCenter	106
Remover uma instância do servidor vCenter	107
Renovar certificado do servidor vCenter	107
Gerenciar certificados das ferramentas ONTAP	109
Acesse o console de manutenção do ONTAP tools for VMware vSphere	111
Saiba mais sobre o console de manutenção das ONTAP tools	111
Configure o acesso remoto para diagnóstico das ONTAP tools	112
Inicie o SSH em outros nós do ONTAP tools	113
Atualizar as credenciais do servidor vCenter nas ONTAP tools	113
Alterar o indicador de validação do certificado nas ONTAP tools	113
Relatórios das ferramentas ONTAP	115
Gerenciar máquinas virtuais	116
Considerações sobre migração e clonagem de máquinas virtuais para ONTAP tools	116
Migrar máquinas virtuais para datastores vVols nas ONTAP tools	117
Limpe as configurações do VASA nas ferramentas ONTAP	118
Anexar ou desanexar um disco de dados de uma VM nas ONTAP tools	118
Descubra sistemas de armazenamento e hosts nas ferramentas ONTAP	119
Modifique as configurações do host ESXi usando as ferramentas ONTAP	120
Gerenciar senhas	120
Alterar a senha do ONTAP tools Manager	120
Redefinir a senha do ONTAP tools Manager	121
Redefinir senha de usuário do aplicativo nas ONTAP tools	121
Redefina a senha do console de manutenção das ONTAP tools	121
Gerenciar a proteção do cluster de hosts	122
Modificar um cluster de hosts protegido nas ferramentas ONTAP	123
Remover a proteção de cluster de hosts nas ONTAP tools	125
Recupere a configuração das ONTAP tools	126
Desinstalar ONTAP tools	127
Remova os volumes FlexVol após desinstalar as ONTAP tools	128
Atualize as ONTAP tools for VMware vSphere	129
Atualize das ONTAP tools for VMware vSphere 10.x para 10.5	129
Códigos de erro de atualização das ONTAP tools	131
Migrar ONTAP tools for VMware vSphere 9.xx para 10.5	137
Migrar das ONTAP tools for VMware vSphere 9.xx para 10.5	137

Migre o provedor VASA e atualize o SRA nas ONTAP tools	137
Etapas para migrar o provedor VASA	137
Etapas para atualizar o adaptador de replicação de armazenamento (SRA)	142
Automatize usando a API REST	144
Saiba mais sobre a API REST do ONTAP tools	144
Fundamentos de serviços web REST	144
Ambiente do Gerenciador de ferramentas ONTAP	144
Detalhes da implementação da API REST das ferramentas ONTAP	145
Como acessar a API REST	145
Detalhes HTTP	146
Autenticação	147
Requisições síncronas e assíncronas	147
Faça sua primeira chamada à API REST das ONTAP tools	147
Antes de começar	148
Etapa 1: obtenha um token de acesso	148
Etapa 2: faça a chamada à API REST	149
Referência da API REST das ONTAP tools	149
Avisos legais	150
Direitos autorais	150
Marcas registradas	150
Patentes	150
Política de privacidade	150
Código aberto	150

Documentação do ONTAP tools for VMware vSphere

Notas de lançamento

Notas de lançamento para ONTAP tools

Conheça os novos e aprimorados recursos disponíveis em ONTAP tools for VMware vSphere 10.5.

Para obter uma lista completa dos novos recursos e melhorias, consulte [Novidades no ONTAP tools for VMware vSphere 10.5](#).

Para obter as informações de compatibilidade mais atualizadas, consulte "[NetApp Ferramenta de Matriz de Interoperabilidade](#)".

A migração é suportada das ONTAP tools for VMware vSphere versões 9.12D1, 9.13D2 e 9.13P2 para ONTAP tools for VMware vSphere 10.5.

Para obter mais informações, consulte o "[Notas de versão do ONTAP tools for VMware vSphere 10.5](#)". Você precisa fazer login com sua NetApp conta ou criar uma conta para acessar as Notas de Versão.

Novidades no ONTAP tools for VMware vSphere 10.5

Saiba mais sobre os novos recursos disponíveis em ONTAP tools for VMware vSphere 10.5.

- **Qualificação da plataforma**

ONTAP tools for VMware vSphere 10.5 adiciona suporte para sistemas ASA r2, proporcionando compatibilidade com as configurações de hardware e software mais recentes. Esta versão também inclui integração com ONTAP 9.16.1 e 9.17.1, expandindo os ambientes suportados.

- **Qualificações e certificações VMware**

ONTAP tools for VMware vSphere 10.5 está em conformidade com os padrões atuais de certificação de interoperabilidade da VMware, oferecendo suporte tanto ao host ESXi quanto ao vCenter Server.

- **MetroCluster suporte**

Esta versão introduz suporte para configurações MetroCluster, aprimorando os recursos de alta disponibilidade e recuperação de desastres.

- **Gerenciamento de segurança e certificados**

Esta versão introduz uma gestão simplificada de certificados autoassinados, melhorando a experiência do usuário e a conformidade com os padrões de segurança. Ela oferece fluxos de trabalho de validação de certificados aprimorados para proteger as comunicações entre ONTAP e ONTAP tools for VMware vSphere.

- **Aprimoramentos na replicação**

Esta versão oferece suporte à replicação VMFS com grupo de consistência hierárquico, incluindo SRA e SnapMirror active sync em sistemas ASA r2. Ela oferece suporte a backups com RPO zero para melhorar a proteção e a recuperação de dados.

- **Atualização e migração**

O processo de atualização e migração das versões anteriores do ONTAP tools for VMware vSphere para ONTAP tools for VMware vSphere 10.5 foi projetado para ser contínuo e eficiente, minimizando o tempo de inatividade e garantindo uma transição tranquila.

Plataformas ONTAP e versões do servidor vCenter suportadas

ONTAP tools for VMware vSphere 10.5 P1 suporta configurações de Alta Disponibilidade (HA) do vCenter para os componentes SRA e SnapMirror active sync. vVols não é suportado nessa configuração. Durante um failover de HA, o vCenter pode ficar indisponível por vários minutos. Em ambientes grandes ou se ocorrer um erro, os tempos de failover podem exceder 15 minutos.

Para obter mais informações, consulte o ["Documentação de alta disponibilidade do vCenter"](#). Para perguntas sobre vCenter HA, entre em contato com ["Suporte da Broadcom"](#).

Para obter os detalhes mais recentes sobre a compatibilidade de versões, consulte ["NetApp Ferramenta de Matriz de Interoperabilidade"](#).

Comparação de recursos das ferramentas ONTAP para VMware vSphere 9 e 10

Saiba se migrar de ONTAP tools for VMware vSphere 9 para ONTAP tools for VMware vSphere 10.2 ou versões posteriores é a escolha certa para você.



Para obter as informações de compatibilidade mais atualizadas, consulte ["NetApp Ferramenta de Matriz de Interoperabilidade"](#).

Recurso	ONTAP tools 9.13	ONTAP tools 10.2 em diante
Proposta de valor	Simplifique e agilize as operações do dia 0 ao dia 2 com recursos aprimorados de segurança, conformidade e automação	Suporte expandido para incluir FC para VMFS e NVMe-oF somente para VMFS. Facilidade de uso para NetApp SnapMirror, configuração simples para clusters de storage vSphere metro e suporte para VMware Live Site Recovery em três locais.
Qualificação de release do ONTAP	ONTAP 9.9.1 para ONTAP 9.16.1	ONTAP 9.12.1 a 9.15.1 para ONTAP tools 10.2. ONTAP 9.14.1, 9.15.1, 9.16.0 e 9.16.1 para ONTAP tools 10.3. ONTAP 9.14.1, 9.15.1, 9.16.0 e 9.16.1 para ONTAP tools 10.4. ONTAP 9.16.1P3 e versões posteriores são necessários para ONTAP tools 10.4 ao usar sistemas ASA r2. ONTAP 9.15.1, 9.16.1 e 9.17.0 para ONTAP tools 10.5

Recurso	ONTAP tools 9.13	ONTAP tools 10.2 em diante
Suporte para versões da VMware	vSphere 7.x-8.x VMware Site Recovery Manager (SRM) 8.5 para VMware Live Site Recovery 9.0	vSphere 7.x-8.x vSphere 9.0 a partir do ONTAP tools 10.5 VMware Site Recovery Manager (SRM) 8.7 até VMware Live Site Recovery 9.0 NOTA: No ONTAP tools 10.x, o SRM oferece suporte a sites compartilhados, permitindo maior escalabilidade e melhor desempenho.
Suporte de protocolo	Armazenamentos de dados NFS e VMFS: NFS (v3 e v4.1), VMFS (iSCSI e FCP)	Armazenamentos de dados NFS e VMFS: NFS (v3 e v4.1), VMFS (iSCSI/FCP/NVMe-oF)
Escalabilidade	Hosts e VMs: 300 hosts, até 10 mil VMs Datastores: 600 NFS, até 50 VMFS	Hosts e VMs: 600 Hosts
Observabilidade	Painéis de desempenho, capacidade e conformidade do host, relatórios dinâmicos de máquinas virtuais e datastores	Painéis de desempenho, capacidade e conformidade do host atualizados, além de relatórios dinâmicos de máquinas virtuais e datastores
Proteção de dados	Replicação SRA para VMFS e NFS. Integração e interoperabilidade com SCV para backup.	Replicação SRA para datastores iSCSI VMFS e NFS v3 com proteção de três sites, combinando SMAS e VMware Live Site Recovery. Suporte SRA para FCP com VMFS.
Suporte do VASA Provider	VASA 4.0	VASA 3.0

Conceitos

Saiba mais sobre as ferramentas ONTAP

ONTAP tools for VMware vSphere é um conjunto de ferramentas para gerenciamento de ciclo de vida de máquina virtual. Ele se integra ao ecossistema VMware para simplificar o provisionamento de datastores e fornecer proteção básica para máquinas virtuais. É uma coleção de microsserviços horizontalmente escaláveis e orientados a eventos, implantados como um Open Virtual Appliance (OVA).

ONTAP tools for VMware vSphere oferece suporte a:

- Funcionalidades essenciais de máquina virtual (VM), como proteção e recuperação de desastres
- VASA Provider para gerenciamento de storage baseado em políticas
- Gerenciamento de storage baseado em políticas
- Adaptador de Replicação de Storage (SRA)

Alta disponibilidade para ONTAP tools for VMware

ONTAP tools for VMware vSphere oferece suporte de alta disponibilidade (HA) para ajudar você a manter a operação ininterrupta durante falhas.

A solução HA ajuda você a se recuperar rapidamente dos seguintes tipos de interrupção:

- Falha do host: apenas falha em um único nó é suportada.
- Falha na rede
- Falha na máquina virtual (sistema operacional convidado)
- Falha da aplicação (ONTAP tools)

Você não precisa realizar nenhuma configuração adicional para habilitar HA para ONTAP tools for VMware vSphere.



ONTAP tools for VMware vSphere não suporta vCenter HA.

Para usar o recurso de HA, certifique-se de que o adicionar sem desligamento de CPU e o hot-plug de memória estejam habilitados durante a implantação ou nas configurações da máquina virtual.

Conceitos e termos-chave nas ferramentas ONTAP

A seção a seguir descreve os principais conceitos e termos usados no documento.

Autoridade de certificação (CA)

Uma Autoridade Certificadora (CA) é uma entidade confiável que emite certificados Secure Sockets Layer (SSL).

Grupo de consistência

Um grupo de consistência é uma coleção de volumes gerenciados como uma única unidade. Os grupos de consistência são sincronizados para consistência de dados entre unidades e volumes de armazenamento. No ONTAP, eles oferecem gerenciamento simplificado e garantias de proteção para cargas de trabalho de aplicativos que abrangem vários volumes. Saiba mais sobre ["grupos de consistência"](#).

Pilha dupla

Uma rede de pilha dupla é um ambiente de rede que suporta o uso simultâneo de endereços IPv4 e IPv6.

Alta disponibilidade (HA)

Os nós do cluster são configurados em pares de alta disponibilidade (HA) para operações sem interrupção.

Unidade lógica (LUN)

Uma LUN é um número usado para identificar uma unidade lógica dentro de uma SAN (Storage Area Network). Esses dispositivos endereçáveis são normalmente discos lógicos acessados pelo protocolo SCSI (Small Computer System Interface) ou por um de seus derivados encapsulados.

Namespace e subsistema NVMe

Um namespace NVMe é uma quantidade de memória não volátil que pode ser formatada em blocos lógicos. Namespaces são o equivalente a LUNs para os protocolos FC e iSCSI, e um subsistema NVMe é análogo a um igroup. Um subsistema NVMe pode ser associado a iniciadores para que os iniciadores associados possam acessar namespaces dentro do subsistema.

Gerenciador de ferramentas ONTAP

ONTAP tools Manager fornece ONTAP tools for VMware vSphere administradores com maior controle sobre as instâncias de vCenter Server gerenciadas e os backends de armazenamento integrados. Ele auxilia no gerenciamento de instâncias de vCenter Server, backends de armazenamento, certificados, senhas e pacotes de logs.

Open Virtual Appliance (OVA)

OVA é um padrão aberto para empacotar e distribuir appliances virtuais ou software que devem ser executados em máquinas virtuais.

Objetivo de Ponto de Recuperação (RPO)

O RPO mede a frequência com que você faz backup ou replica dados. Ele especifica o momento exato em que você precisa restaurar os dados após uma interrupção para retomar operações de negócios. Por exemplo, se uma organização tem um RPO de 4 horas, ela pode tolerar a perda de até 4 horas de dados em caso de desastre.

SnapMirror active sync

SnapMirror active sync permite que os serviços de negócios continuem operando mesmo com uma falha completa do local, permitindo que os aplicativos realizem failover de forma transparente usando uma cópia secundária. Não é necessária intervenção manual nem scripts personalizados para acionar um failover com SnapMirror active sync. Saiba mais ["SnapMirror active sync"](#).

Backends de armazenamento

Os backends de armazenamento são a infraestrutura de storage subjacente que o host ESXi usa para armazenar arquivos de máquina virtual, dados e outros recursos. Eles permitem que o host ESXi acesse e gerencie dados persistentes, fornecendo a capacidade de storage e o desempenho necessários para um ambiente virtualizado.

Cluster global (storage backend)

Os backends de armazenamento globais, disponíveis apenas com credenciais de cluster ONTAP, são integrados por meio da interface do ONTAP tools Manager. Eles podem ser adicionados com privilégios mínimos para permitir a descoberta de recursos essenciais do cluster necessários para o gerenciamento de vVols. Os clusters globais são ideais para cenários de multilocação em que um usuário SVM é adicionado localmente para o gerenciamento de vVols.

Backend de armazenamento local

Os backends de armazenamento local com credenciais de cluster ou SVM são adicionados por meio da interface de usuário do ONTAP tools e são limitados a um vCenter. Ao usar credenciais de cluster localmente, as SVMs associadas são automaticamente mapeadas com o vCenter para gerenciar vVols ou VMFS. Para o gerenciamento de VMFS, incluindo SRA, ONTAP tools oferece suporte a credenciais de SVM sem a necessidade de um cluster global.

Adaptador de Replicação de Storage (SRA)

O SRA é o software específico do fornecedor de armazenamento instalado dentro do appliance VMware Live Site Recovery. O adaptador permite a comunicação entre o Site Recovery Manager e um controlador de armazenamento no nível da Storage Virtual Machine (SVM) e na configuração do cluster.

Máquina virtual de storage (SVM)

A SVM é a unidade de multilocação no ONTAP. Assim como uma máquina virtual executada em um hipervisor, a SVM é uma entidade lógica que abstrai recursos físicos. A SVM contém volumes de dados e uma ou mais LIFs por meio das quais fornece dados aos clientes.

Configuração uniforme e não uniforme

- **Acesso uniforme ao host** significa que os hosts de dois sites estão conectados a todos os caminhos para os clusters de storage em ambos os sites. Os caminhos entre sites são estendidos por distâncias.
- **Acesso não uniforme ao host** significa que os hosts em cada site estão conectados apenas ao cluster no mesmo site. Caminhos entre sites diferentes e caminhos estendidos não estão conectados.



O acesso uniforme ao host é compatível com qualquer implantação de sincronização ativa do SnapMirror; o acesso não uniforme ao host é compatível apenas com implantações ativo-ativo simétricas. Saiba mais sobre ["SnapMirror visão geral da sincronização ativa no ONTAP"](#).

Sistema de arquivos de máquina virtual (VMFS)

O VMFS é um sistema de arquivos em cluster projetado para armazenar arquivos de máquinas virtuais em ambientes VMware vSphere.

Volumes virtuais (vVols)

vVols fornecem uma abstração em nível de volume para o armazenamento usado por uma máquina virtual. Inclui diversas vantagens e oferece uma alternativa ao uso de um LUN tradicional. Um datastore vVol é normalmente associado a um único LUN que atua como um contêiner para vVols.

Política de armazenamento de VM

As políticas de armazenamento de máquinas virtuais são criadas no vCenter Server em Políticas e Perfis. Para vVols, crie um conjunto de regras usando regras do provedor do tipo de armazenamento NetApp vVols.

VMware Live Site Recovery

O VMware Live Site Recovery, anteriormente conhecido como Site Recovery Manager (SRM), oferece continuidade dos negócios, recuperação de desastres, migração de sites e testes não disruptivos para ambientes virtuais VMware.

APIs da VMware vSphere para reconhecimento de armazenamento (VASA)

VASA é um conjunto de APIs que integra arrays de armazenamento com o vCenter Server para gerenciamento e administração. A arquitetura é baseada em diversos componentes, incluindo o VASA Provider, que lida com a comunicação entre o VMware vSphere e os sistemas de armazenamento.

APIs de armazenamento da VMware vSphere - Integração de arrays (VAAI)

VAAI é um conjunto de APIs que permite a comunicação entre hosts VMware vSphere ESXi e os dispositivos de storage. As APIs incluem um conjunto de operações primitivas usadas pelos hosts para transferir operações de storage para o array. O VAAI pode proporcionar melhorias significativas de desempenho para tarefas intensivas em storage.

vSphere Metro Cluster de armazenamento

vSphere Metro Storage Cluster (vMSC) é uma arquitetura que permite e suporta vSphere em uma implementação de cluster estendido. As soluções vMSC são compatíveis com NetApp MetroCluster e SnapMirror active sync (anteriormente SMBC). Essas soluções proporcionam maior continuidade dos negócios em caso de falha do domínio. O modelo de resiliência é baseado nas suas escolhas de configuração específicas. Saiba mais sobre "[Cluster de armazenamento Metro VMware vSphere](#)".

datastore vVols

O datastore vVols é uma representação lógica de um contêiner vVols criado e mantido por um VASA Provider.

RPO zero

RPO significa ponto de recuperação, ou seja, a quantidade de perda de dados considerada aceitável durante um determinado período. RPO igual a zero significa que nenhuma perda de dados é aceitável.

Controle de acesso baseado em funções (RBAC)

Saiba mais sobre as ferramentas RBAC do ONTAP

O controle de acesso baseado em funções (RBAC) é uma estrutura de segurança para controlar o acesso a recursos dentro de uma organização. O RBAC simplifica a

administração ao definir funções com níveis específicos de autoridade para executar ações, em vez de atribuir autorização a usuários individuais. As funções definidas são atribuídas aos usuários, o que ajuda a reduzir o risco de erro e simplifica o gerenciamento do controle de acesso em toda a sua organização.

O modelo padrão RBAC consiste em diversas tecnologias ou fases de implementação com complexidade crescente. O resultado é que as implementações reais de RBAC, baseadas nas necessidades dos fornecedores de software e de seus clientes, podem variar e ir de relativamente simples até muito complexas.

Componentes RBAC

Em linhas gerais, existem vários componentes que geralmente estão incluídos em toda implementação de RBAC. Esses componentes são interligados de diferentes maneiras como parte da definição dos processos de autorização.

Privileges

Um privilégio é uma ação ou capacidade que pode ser permitida ou negada. Pode ser algo simples, como a capacidade de ler um arquivo, ou uma operação mais abstrata específica de um determinado sistema de software. Privileges também podem ser definidos para restringir o acesso a endpoints da API REST e comandos de CLI. Toda implementação de RBAC inclui privilégios predefinidos e também pode permitir que administradores criem privilégios personalizados.

Funções

Uma *função* é um contêiner que inclui um ou mais privilégios. As funções geralmente são definidas com base em tarefas ou funções de trabalho específicas. Quando uma função é atribuída a um usuário, o usuário recebe todos os privilégios contidos nessa função. E, assim como acontece com os privilégios, as implementações incluem funções predefinidas e geralmente permitem a criação de funções personalizadas.

Objetos

Um *objeto* representa um recurso real ou abstrato identificado no ambiente RBAC. As ações definidas por meio dos privilégios são executadas sobre ou com os objetos associados. Dependendo da implementação, os privilégios podem ser concedidos a um tipo de objeto ou a uma instância de objeto específica.

Usuários e grupos

Usuários são atribuídos ou associados a uma função aplicada após a autenticação. Algumas implementações de RBAC permitem que apenas uma função seja atribuída a um usuário, enquanto outras permitem várias funções por usuário, talvez com apenas uma função ativa por vez. Atribuir funções a grupos pode simplificar ainda mais a administração de segurança.

Permissões

Uma *permissão* é uma definição que vincula um usuário ou grupo, juntamente com uma função, a um objeto. As permissões podem ser úteis em um modelo de objeto hierárquico, onde podem ser opcionalmente herdadas pelos filhos na hierarquia.

Dois ambientes RBAC

Existem dois ambientes RBAC distintos que você precisa considerar ao trabalhar com ONTAP tools for VMware vSphere 10. ONTAP tools for VMware vSphere 10 exige privilégios específicos tanto no vCenter quanto no ONTAP para executar suas operações. Embora o ONTAP tools automatize tarefas de gerenciamento de storage, ele não cria contas de usuário nem no vCenter nem no ONTAP. As contas de serviço devem ser criadas por um administrador do vSphere, conforme necessário. Esta documentação fornece orientações para que os administradores atribuam as funções e permissões necessárias para o gerenciamento eficaz do ONTAP tools.

Servidor VMware vCenter

A implementação do RBAC no VMware vCenter Server é usada para restringir o acesso a objetos expostos pela interface de usuário do vSphere Client. Como parte da instalação do ONTAP tools for VMware vSphere 10, o ambiente RBAC é estendido para incluir objetos adicionais que representam as funcionalidades do ONTAP tools. O acesso a esses objetos é fornecido por meio do plug-in remoto. Veja "[vCenter Server ambiente RBAC](#)" para mais informações.

Cluster ONTAP

ONTAP tools for VMware vSphere 10 se conecta a um cluster ONTAP por meio da API REST do ONTAP para executar operações relacionadas ao storage. O acesso aos recursos de storage é controlado por meio de uma função ONTAP associada ao usuário ONTAP fornecido durante a autenticação. Consulte "[Ambiente ONTAP RBAC](#)" para obter mais informações.

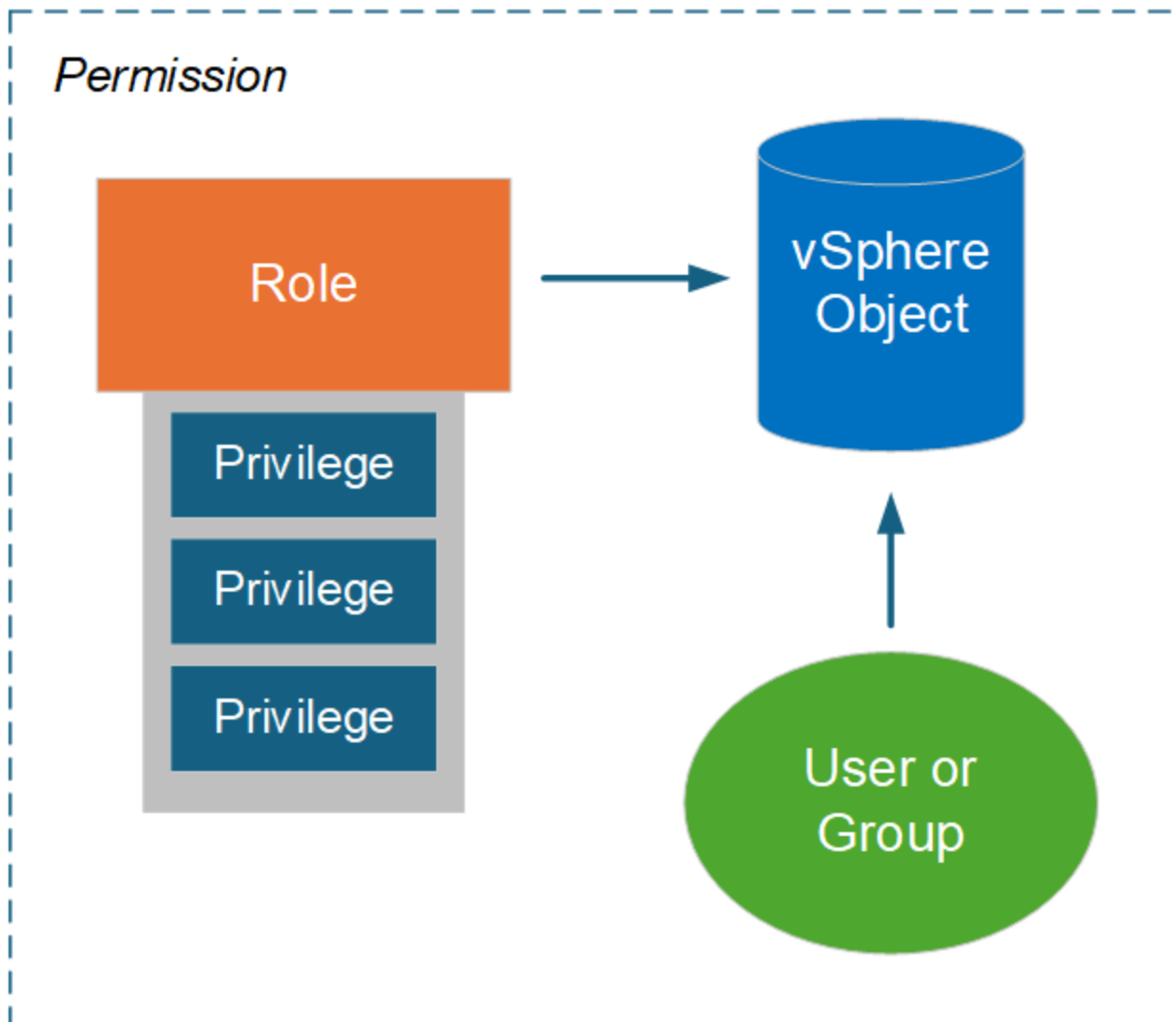
RBAC com VMware vSphere

Como o RBAC do vCenter Server funciona com as ONTAP tools

O VMware vCenter Server oferece um recurso de RBAC que permite que você controle o acesso a objetos do vSphere. É uma parte importante dos serviços de autenticação e autorização centralizados do vCenter.

Ilustração de uma permissão de servidor vCenter

Uma permissão é a base para a aplicação do controle de acesso no ambiente do vCenter Server. Ela é aplicada a um objeto vSphere com um usuário ou grupo incluído na definição da permissão. Uma ilustração de alto nível de uma permissão do vCenter é fornecida na figura abaixo.



Componentes de uma permissão de servidor vCenter

Uma permissão de vCenter Server é um pacote de vários componentes que são vinculados quando a permissão é criada.

vSphere objetos

As permissões estão associadas a objetos do vSphere, como o vCenter Server, hosts ESXi, máquinas virtuais, datastores, data centers e pastas. Com base nas permissões atribuídas ao objeto, o vCenter Server determina quais ações ou tarefas podem ser executadas no objeto por cada usuário ou grupo. Para as tarefas específicas das ONTAP tools for VMware vSphere, todas as permissões são atribuídas e validadas no nível raiz ou na pasta raiz do vCenter Server. Consulte ["Use RBAC com o servidor vCenter"](#) para mais informações.

Privileges e funções

Existem dois tipos de privilégios do vSphere usados com ONTAP tools for VMware vSphere 10. Para simplificar o trabalho com RBAC nesse ambiente, ONTAP tools fornece funções que contêm os privilégios nativos e personalizados necessários. Os privilégios incluem:

- Privilégios nativos do servidor vCenter

Esses são os privilégios concedidos pelo vCenter Server.

- Privilégios específicos das ferramentas ONTAP

Esses são privilégios personalizados exclusivos das ONTAP tools for VMware vSphere.

Usuários e grupos

Você pode definir usuários e grupos usando o Active Directory ou a instância local do vCenter Server. Combinado com uma função, você pode criar uma permissão em um objeto na hierarquia de objetos do vSphere. A permissão concede acesso com base nos privilégios da função associada. Observe que as funções não são atribuídas diretamente aos usuários de forma isolada. Em vez disso, usuários e grupos obtêm acesso a um objeto por meio dos privilégios de função como parte da permissão do vCenter Server.

vCenter considerações sobre RBAC do servidor para ONTAP tools

Existem vários aspectos da implementação do RBAC das ONTAP tools for VMware vSphere 10 com o vCenter Server que você deve considerar antes de usá-la em um ambiente de produção.

vCenter roles e a conta de administrador

Você só precisa definir e usar as funções personalizadas do servidor vCenter se quiser limitar o acesso aos objetos vSphere e às tarefas administrativas associadas. Se limitar o acesso não for necessário, você pode usar uma conta de administrador. Cada conta de administrador é definida com a função de Administrador no nível mais alto da hierarquia de objetos. Isso fornece acesso total aos objetos vSphere, incluindo aqueles adicionados por ONTAP tools for VMware vSphere 10.

hierarquia de objetos do vSphere

O inventário de objetos do vSphere está organizado em uma hierarquia. Por exemplo, você pode navegar pela hierarquia da seguinte forma:

vCenter Server → Datacenter → Cluster → ESXi host → Virtual Machine

Todas as permissões são validadas na hierarquia de objetos do vSphere, exceto as operações do plug-in VAAI, que são validadas em relação ao host ESXi de destino.

Funções incluídas nas ONTAP tools for VMware vSphere 10

Para simplificar o trabalho com o RBAC do servidor vCenter, ONTAP tools for VMware vSphere fornece funções predefinidas adaptadas a várias tarefas administrativas.



Você pode criar novas funções personalizadas, se necessário. Para isso, clone uma das funções existentes das ferramentas ONTAP e edite-a conforme necessário. Após fazer as alterações de configuração, os usuários do cliente vSphere afetados precisam fazer logout e entrar novamente para ativar as alterações.

Para visualizar as funções das ONTAP tools for VMware vSphere, selecione **Menu** na parte superior do vSphere Client e clique em **Administração** e, em seguida, em **Funções** à esquerda. Os seguintes privilégios devem estar incluídos na função atribuída ao usuário vCenter responsável pela implantação ou processo de

ambientação do vCenter Server. Certifique-se de que esses privilégios estejam configurados como pré-requisito para a implantação ou processo de ambientação.

- Alarmes
 - Confirmar alarme
- Biblioteca de Conteúdo
 - Adicionar item da biblioteca
 - Faça check-in em um modelo
 - Confira um modelo
 - Baixar arquivos
 - Importar armazenamento
 - Leitura de storage
 - Sincronizar item da biblioteca
 - Sincronizar biblioteca assinada
 - Exibir configurações de configuração
- Datastore
 - Alocar espaço
 - Navegar no datastore
 - Operações de arquivo de baixo nível
 - Remover arquivo
 - Atualizar arquivos de máquina virtual
 - Atualizar metadados da máquina virtual
- ESX Agent Manager
 - Visualizar
- Pasta
 - Criar pasta
- Host
 - Configuração
 - Configurações avançadas
 - Alterar configurações
 - Configuração de rede
 - Recursos do sistema
 - Configuração de inicialização automática da máquina virtual
 - Operações locais
 - Criar máquina virtual
 - Excluir máquina virtual
 - Reconfigurar máquina virtual
- Rede

- Atribuir rede
 - Configurar
- OvfManager
 - OvfConsumer Acesso
- Perfil do host
 - Visualizar
- Recurso
 - Atribua máquina virtual ao pool de recursos
- Tarefa agendada
 - Criar tarefas
 - Modificar tarefa
 - Executar tarefa
- Tarefas
 - Criar tarefa
 - Tarefa de atualização
- vApp
 - Adicionar máquina virtual
 - Atribuir pool de recursos
 - Atribuir vApp
 - Criar
 - Importar
 - Mover
 - Desligar
 - Ligar
 - Extrair da URL
 - Visualizar ambiente OVF
- Máquina virtual
 - Alterar configuração
 - Adicionar disco existente
 - Adicionar novo disco
 - Adicionar ou remover dispositivo
 - Configuração avançada
 - Alterar contagem de CPU
 - Alterar memória
 - Alterar configurações
 - Alterar recurso
 - Estender disco virtual

- Modificar configurações do dispositivo
- Remover disco
- Redefinir informações do convidado
- Atualizar a compatibilidade da máquina virtual
- Editar inventário
 - Criar a partir de existente
 - Criar novo
 - Mover
 - Cadastre-se
 - Remover
 - Cancelar registro
- Interação
 - Operação de backup em máquina virtual
 - Configurar mídia de CD
 - Configurar mídia de disquete
 - Conecte dispositivos
 - Interação com o console
 - Gerenciamento do sistema operacional convidado por meio da API VIX
 - Desligar
 - Ligar
 - Reiniciar
 - Suspende
- Provisionamento
 - Permitir acesso ao disco
 - Modelo de clone
 - Personalizar convidado
 - Implantar modelo
 - Modificar especificação de personalização
 - Leia as especificações de personalização
- Gerenciamento de Snapshot
 - Criar instantâneo
 - Remover snapshot
 - Renomear snapshot
 - Reverter para o snapshot

Existem três funções predefinidas, conforme descrito abaixo.

Administrador do NetApp ONTAP tools for VMware vSphere

Fornecer todos os privilégios nativos do vCenter Server e os privilégios específicos das ferramentas ONTAP

necessários para executar tarefas administrativas essenciais das ONTAP tools for VMware vSphere.

NetApp ONTAP tools for VMware vSphere somente leitura

Fornecer acesso somente leitura às ferramentas do ONTAP. Esses usuários não podem executar nenhuma ação das ferramentas do ONTAP para VMware vSphere que seja controlada por acesso.

Provisionamento do NetApp ONTAP tools for VMware vSphere

Fornecer alguns dos privilégios nativos do vCenter Server e privilégios específicos das ONTAP tools que são necessários para provisionar storage. Você pode executar as seguintes tarefas:

- Criar novos datastores
- Gerenciar datastores

vSphere objetos e backends de storage ONTAP

Os dois ambientes RBAC funcionam juntos. Ao executar uma tarefa na interface do cliente vSphere, primeiro são verificadas as funções das ONTAP tools definidas para o vCenter Server. Se a operação for permitida pelo vSphere, então os privilégios da função ONTAP são examinados. Essa segunda etapa é realizada com base na função ONTAP atribuída ao usuário quando o backend de storage foi criado e configurado.

Trabalhando com RBAC do vCenter Server

Há alguns pontos a considerar ao trabalhar com os privilégios e permissões do servidor vCenter.

Privilégios necessários

Para acessar a interface de usuário do ONTAP tools for VMware vSphere 10, você precisa ter o privilégio *View* específico das ONTAP tools. Se você fizer login no vSphere sem esse privilégio e clicar no ícone NetApp, o ONTAP tools for VMware vSphere exibirá uma mensagem de erro e impedirá você de acessar a interface de usuário.

O nível de atribuição na hierarquia de objetos da vSphere determina a quais partes da interface de usuário você pode acessar. Atribuir o privilégio "Visualizar" ao objeto raiz permite que você acesse ONTAP tools for VMware vSphere clicando no ícone NetApp.

Você pode, em vez disso, atribuir o privilégio de visualização a outro nível de objeto vSphere inferior. No entanto, isso limitará os menus das ONTAP tools for VMware vSphere que você pode acessar e usar.

Atribuindo permissões

Você precisa usar permissões do vCenter Server se quiser limitar o acesso aos objetos e tarefas do vSphere. O local onde você atribui permissões na hierarquia de objetos do vSphere determina quais tarefas do ONTAP tools for VMware vSphere 10 os usuários podem executar.



A menos que você precise definir um acesso mais restritivo, geralmente é uma boa prática atribuir permissões no nível do objeto raiz ou da pasta raiz.

As permissões disponíveis com ONTAP tools for VMware vSphere 10 aplicam-se a objetos personalizados que não sejam vSphere, como sistemas de storage. Se possível, você deve atribuir essas permissões ao objeto raiz do ONTAP tools for VMware vSphere, pois não há nenhum objeto vSphere ao qual você possa atribuí-las. Por exemplo, qualquer permissão que inclua o privilégio "Adicionar/Modificar/Remover sistemas de storage" do ONTAP tools for VMware vSphere deve ser atribuída no nível do objeto raiz.

Ao definir uma permissão em um nível superior na hierarquia de objetos, você pode configurá-la para que seja

transmitida e herdada pelos objetos filhos. Se necessário, você pode atribuir permissões adicionais aos objetos filhos que substituem as permissões herdadas do pai.

Você pode modificar uma permissão a qualquer momento. Se você alterar algum dos privilégios dentro de uma permissão, os usuários associados a essa permissão precisarão fazer logout do vSphere e entrar novamente para que a alteração seja aplicada.

RBAC com ONTAP

Como o RBAC do ONTAP funciona com as ONTAP tools

ONTAP oferece um ambiente RBAC robusto e extensível. Você pode usar o recurso RBAC para controlar o acesso ao armazenamento e às operações do sistema, conforme exposto pela API REST e pela CLI. É recomendável familiarizar-se com o ambiente antes de usá-lo com uma implantação do ONTAP tools for VMware vSphere 10.

Visão geral das opções administrativas

Existem diversas opções disponíveis ao usar ONTAP RBAC, dependendo do seu ambiente e objetivos. Uma visão geral das principais decisões administrativas é apresentada abaixo. Consulte também ["Automação do ONTAP: visão geral da segurança RBAC"](#) para obter mais informações.



O RBAC do ONTAP é otimizado para um ambiente de storage e é mais simples do que a implementação de RBAC fornecida com vCenter Server. Com ONTAP, você atribui uma função diretamente ao usuário. A configuração de permissões explícitas, como as usadas com o vCenter Server, não é necessária com o RBAC do ONTAP.

Tipos de funções e privilégios

Uma função ONTAP é necessária ao definir um usuário ONTAP. Existem dois tipos de funções ONTAP:

- REST

As funções REST foram introduzidas no ONTAP 9.6 e geralmente são aplicadas a usuários que acessam o ONTAP por meio da API REST. Os privilégios incluídos nessas funções são definidos em termos de acesso aos endpoints da API REST do ONTAP e às ações associadas.

- Tradicional

Essas são as funções legadas que existiam antes do ONTAP 9.6. Elas continuam sendo um aspecto fundamental do RBAC. Os privilégios são definidos em termos de acesso aos comandos da CLI do ONTAP.

Embora as funções REST tenham sido introduzidas mais recentemente, as funções tradicionais oferecem algumas vantagens. Por exemplo, parâmetros de consulta adicionais podem ser incluídos para permitir que os Privileges definam com mais precisão os objetos aos quais se aplicam.

Escopo

As funções do ONTAP podem ser definidas com um de dois escopos diferentes. Elas podem ser aplicadas a um SVM de dados específico (nível de SVM) ou a todo o cluster ONTAP (nível de cluster).

Definições de funções

ONTAP fornece um conjunto de funções predefinidas tanto no nível do cluster quanto no nível da SVM. Você

também pode definir funções personalizadas.

Trabalhando com funções REST do ONTAP

Existem diversas considerações a serem feitas ao usar as funções REST do ONTAP incluídas nas ONTAP tools for VMware vSphere 10.

Mapeamento de funções

Seja usando uma função tradicional ou REST, todas as decisões de acesso do ONTAP são tomadas com base no comando CLI subjacente. Mas, como os privilégios em uma função REST são definidos em termos dos endpoints da API REST, o ONTAP precisa criar uma função tradicional mapeada para cada uma das funções REST. Portanto, cada função REST é mapeada para uma função tradicional subjacente. Isso permite que o ONTAP tome decisões de controle de acesso de forma consistente, independentemente do tipo de função. Você não pode modificar as funções mapeadas paralelamente.

Definindo uma função REST usando privilégios da CLI

Como ONTAP sempre usa os comandos da CLI para determinar o acesso em um nível básico, é possível expressar uma função REST usando privilégios de comando da CLI em vez de endpoints REST. Um dos benefícios dessa abordagem é a granularidade adicional disponível com as funções tradicionais.

Interface administrativa ao definir funções do ONTAP

Você pode criar usuários e funções com a CLI do ONTAP e a API REST. No entanto, é mais conveniente usar a interface do System Manager juntamente com o arquivo JSON disponível no ONTAP tools Manager. Veja ["Use o RBAC do ONTAP com as ONTAP tools for VMware vSphere 10"](#) para mais informações.

Considerações sobre RBAC do ONTAP para ONTAP tools

Existem vários aspectos da implementação do RBAC das ONTAP tools for VMware vSphere 10 com ONTAP que você deve considerar antes de usá-la em um ambiente de produção.

Visão geral do processo de configuração

ONTAP tools for VMware vSphere inclui suporte para criar um usuário ONTAP com uma função personalizada. As definições são fornecidas em um arquivo JSON que você pode carregar no cluster ONTAP. Você pode criar o usuário e adaptar a função para seu ambiente e necessidades de segurança.

As principais etapas de configuração são descritas em alto nível abaixo. Consulte ["Configurar funções e privilégios de usuário do ONTAP"](#) para mais detalhes.

1. Preparar

Você precisa ter credenciais administrativas tanto para o ONTAP tools Manager quanto para o ONTAP cluster.

2. Baixe o arquivo de definição JSON

Após fazer login na interface de usuário do ONTAP tools Manager, você pode baixar o arquivo JSON contendo as definições de RBAC.

3. Crie um usuário ONTAP com uma função

Após iniciar sessão no System Manager, você pode criar o usuário e a função:

1. Selecione **Cluster** à esquerda e depois **Settings**.
2. Desça até **Usuários e funções** e clique →.

3. Selecione **Adicionar** em **Usuários** e selecione **Virtualization products**.
4. Selecione o arquivo JSON em sua estação de trabalho local e faça o upload.

4. Configure a função

Como parte da definição da função, você precisa tomar diversas decisões administrativas. Veja [Configure a função usando System Manager](#) para mais detalhes.

Configure a função usando System Manager

Após começar a criar um novo usuário e função com System Manager e carregar o arquivo JSON, você pode personalizar a função de acordo com seu ambiente e necessidades.

Configuração principal de usuários e funções

As definições de RBAC são agrupadas em diversas funcionalidades de produto, incluindo combinações de VSC, VASA Provider e SRA. Você deve selecionar o(s) ambiente(s) em que precisa de suporte a RBAC. Por exemplo, se você deseja que as funções suportem a funcionalidade de plug-in remoto, selecione VSC. Você também precisa escolher o nome de usuário e a senha associada.

Privileges

Os privilégios de função são organizados em quatro conjuntos com base no nível de acesso necessário para o armazenamento ONTAP. Os privilégios nos quais as funções se baseiam incluem:

- Descoberta

Esta função permite adicionar sistemas de armazenamento.

- Criar storage

Essa função permite que você crie armazenamento. Ela também inclui todos os privilégios associados à função de descoberta.

- Modificar armazenamento

Essa função permite que você modifique o armazenamento. Ela também inclui todos os privilégios associados às funções de descoberta e criação de armazenamento.

- Destruir armazenamento

Essa função permite destruir armazenamento. Ela também inclui todos os privilégios associados às funções de descoberta, criação e modificação de armazenamento.

Gere o usuário com uma função

Após selecionar as opções de configuração para o seu ambiente, clique em **Adicionar** e ONTAP cria o usuário e a função. O nome da função gerada é uma concatenação dos seguintes valores:

- Valor de prefixo constante definido no arquivo JSON (por exemplo "OTV_10")
- Funcionalidade do produto que você selecionou
- Lista dos conjuntos de privilégios.

Exemplo

OTV_10_VSC_Discovery_Create

O novo usuário será adicionado à lista na página 'Usuários e funções'. Observe que os métodos de login de usuário HTTP e ONTAPI são suportados.

Implante ONTAP tools for VMware vSphere

Guia rápido para ONTAP tools for VMware vSphere

Configure as ONTAP tools para VMware vSphere com esta seção de início rápido.

Conclua primeiro estas tarefas principais para tornar as ONTAP tools operacionais para gerenciamento e provisionamento desde o dia 0. Em seguida, conclua as tarefas opcionais com base no seu ambiente e nos requisitos de proteção.

Inicialmente, você implantará ONTAP tools for VMware vSphere como uma configuração de nó único de pequeno porte que fornece serviços essenciais para suportar datastores NFS e VMFS. Para expandir sua configuração para contêineres adicionais por serviço, maior resiliência ou para usar datastores vVols e alta disponibilidade (HA), conclua este fluxo de trabalho primeiro e depois prossiga com as etapas de expansão. Para mais informações, consulte a ["Fluxo de trabalho de implantação de alta disponibilidade"](#).

1

Planeje sua implantação

Confirme se seu ambiente está pronto para uma implantação com suporte. Verifique se as versões do seu vSphere, ONTAP e host ESXi são compatíveis com a versão das ONTAP tools. Aloque CPU, memória e espaço de disco suficientes. Com base nas suas regras de segurança, talvez seja necessário configurar firewalls ou outras ferramentas de segurança para permitir o tráfego de rede.

Certifique-se de que o vCenter Server esteja instalado e acessível.

- ["Ferramenta de Matriz de Interoperabilidade"](#)
- ["Requisitos e limites de configuração do ONTAP tools for VMware vSphere"](#)
- ["Antes de começar"](#)

2

Implante ONTAP tools for VMware vSphere

Implante o appliance ONTAP tools para estabelecer serviços básicos para os datastores NFS e VMFS.

Inicialmente, você implantará ONTAP tools for VMware vSphere como uma configuração de nó único de pequeno porte. Se você planeja expandir sua configuração para usar datastores vVols e alta disponibilidade (HA), você fará isso após concluir este fluxo de trabalho. Para expandir para uma configuração de HA, certifique-se de que CPU hot-add e memória hot-plug estejam habilitadas.

Durante a implementação, revise cuidadosamente os campos em **Personalizar modelo**, especialmente o nome do host, o uso do endereço IP das ferramentas ONTAP e os requisitos de DNS.

- ["Implante ONTAP tools for VMware vSphere"](#)

3

Registre e instale o plug-in de cliente vCenter

Adicione uma instância do vCenter Server para registrar o plug-in do cliente vCenter e aplicar os privilégios e funções necessários. Quando você adiciona uma instância do vCenter Server, ONTAP tools registra o plug-in remoto, aplica privilégios personalizados de plug-in e API, cria funções personalizadas e adiciona um atalho do plug-in na interface de usuário do vSphere.

- ["Adicionar instâncias do servidor vCenter às ONTAP tools"](#)

4

Configure os backends de storage

Conecte recursos de storage ONTAP para permitir que as ferramentas ONTAP provisionem e gerenciem datastores. Adicione um backend de storage a um cluster ONTAP. Em ambientes multitenant onde um vCenter Server está associado a uma SVM de tenant, use o ONTAP tools Manager para adicionar o cluster. Em seguida, associe o backend de storage ao vCenter Server para criar um mapeamento global para essa instância do vCenter.

Adicione os backends de storage locais com credenciais de cluster ou SVM usando a interface de usuário do ONTAP tools. Esses backends de storage são limitados a um único vCenter. Ao usar credenciais de cluster localmente, as SVMs associadas são mapeadas automaticamente para o vCenter para gerenciar vVols ou VMFS. Para o gerenciamento de VMFS, incluindo SRA, ONTAP tools oferece suporte a credenciais de SVM sem a necessidade de um cluster global.

- ["Adicionar um backend de storage"](#)
- ["Associe o backend de armazenamento a uma instância do vCenter Server"](#)

Próximas tarefas opcionais

1

Configurar funções e privilégios de usuário do ONTAP

Configure funções ONTAP personalizadas para acesso com privilégios mínimos em vez da conta admin padrão.

- ["Configurar funções e privilégios de usuário do ONTAP"](#)

2

Atualizar certificados para várias instâncias do vCenter Server

Atualize os certificados para usar comunicação confiável baseada em certificados em várias instâncias do vCenter Server.

- ["Gerenciar certificados"](#)

3

Configurar proteção SRA

Habilite a funcionalidade SRA para configurar a proteção de recuperação de desastres para os datastores NFS e VMFS.

- ["Habilite os serviços do ONTAP tools for VMware vSphere"](#)
- ["Configure o SRA no appliance VMware Live Site Recovery"](#)

4

Ative a proteção de sincronização ativa do SnapMirror

Configure a proteção de cluster de hosts com SnapMirror active sync para proteger datastores VMFS. Nos sistemas ONTAP, faça o pareamento do cluster e do SVM necessários e, em seguida, configure a proteção do cluster de hosts em ONTAP tools for VMware vSphere. Esta opção se aplica somente a datastores VMFS.

- ["Proteja usando a proteção de cluster de hosts"](#)

5

Configure backup e recuperação para sua implantação do ONTAP tools

Configure backup e recuperação para proteger a configuração das ferramentas ONTAP e recuperar-se rapidamente de falhas.

O backup está ativado por padrão no ONTAP tools for VMware vSphere 10.5 e ocorre a cada 10 minutos. Agende backups da sua instalação do ONTAP tools for VMware vSphere para que você possa recuperar a instalação em caso de falha.

- ["Edite as configurações de backup"](#)
- ["Recupere a configuração das ONTAP tools"](#)

Fluxo de trabalho de implantação de alta disponibilidade para ONTAP tools

Para aumentar a resiliência e suportar mais contêineres por serviço, expanda sua implantação inicial das ONTAP tools para uma configuração de alta disponibilidade (HA). Habilitar o serviço VASA Provider é necessário para datastores vVols em uma configuração de HA.

1

Ampliar a implementação

Você pode expandir a configuração do ONTAP tools for VMware vSphere para aumentar o número de nós na implantação e alterar a configuração para um ambiente HA.

- ["Alterar a configuração do ONTAP tools for VMware vSphere"](#)

2

Habilitar serviços

Para configurar os datastores vVols, você deve habilitar o serviço VASA Provider. Registre o provedor VASA no vCenter e certifique-se de que suas políticas de armazenamento atendam aos requisitos de HA, incluindo configurações adequadas de rede e armazenamento.

Habilite os serviços SRA para usar ONTAP tools Storage Replication Adapter (SRA) para VMware Site Recovery Manager (SRM) ou VMware Live Site Recovery (VLSR).

- ["Habilite os serviços VASA Provider e SRA"](#)

3

Atualize os certificados

Se você estiver usando armazenamentos de dados vVol com várias instâncias do servidor vCenter, atualize o certificado autoassinado para um certificado assinado por uma autoridade certificadora (CA).

- ["Gerenciar certificados"](#)

Requisitos e limites de configuração do ONTAP tools for VMware vSphere

Antes de implantar o ONTAP tools for VMware vSphere, você deve estar familiarizado com os requisitos de espaço para o pacote de implantação e alguns requisitos básicos do sistema host.

Você pode usar ONTAP tools for VMware vSphere com VMware vCenter Server Virtual Appliance (vCSA). Você deve implantar ONTAP tools for VMware vSphere em um ambiente vSphere compatível que inclua hosts ESXi.

Requisitos do sistema

- **Requisitos de espaço do pacote de instalação por nó**
 - 15 GB para instalações com provisionamento dinâmico
 - 348 GB para instalações com provisionamento espesso
- **Requisitos de dimensionamento do sistema host** A tabela abaixo mostra a memória recomendada para cada tamanho de implantação. Para implantações de alta disponibilidade (HA), você precisa de três vezes o tamanho do appliance listado.

Tipo de implantação	CPUs por nó	Memória (GB) por nó	Espaço em disco (GB) provisionado de forma thick por nó
Pequeno	9	18	350
Médio	13	26	350
Observação: a implantação de grande porte destina-se apenas à configuração de alta disponibilidade (HA).	17	34	350



Quando o backup está ativado, cada cluster de ONTAP tools precisa de mais 50 GB de espaço no datastore onde as máquinas virtuais estão implantadas. Portanto, a configuração sem HA requer 400 GB, e a configuração com HA requer 1100 GB de espaço no total.

Requisitos mínimos de storage e de aplicativos

Armazenamento, host e aplicativos	Requisitos de versão
ONTAP	9.15.1, 9.16.1 e 9.17.0
Hosts ESXi compatíveis com ONTAP tools	7.0.3 em diante
Ferramentas ONTAP com suporte para vCenter Server	7.0U3 em diante
VASA Provider	3,0
Aplicativo OVA	10,5

Armazenamento, host e aplicativos	Requisitos de versão
Host ESXi para implantar a máquina virtual ONTAP tools	7.0U3 e 8.0U3
vCenter Server para implantar a máquina virtual ONTAP tools	7.0 e 8.0



A partir do ONTAP tools for VMware vSphere 10.4, o hardware da máquina virtual é alterado da versão 10 para a 17.

A Ferramenta de Matriz de Interoperabilidade (IMT) contém as informações mais recentes sobre as versões suportadas de ONTAP, vCenter Server, hosts ESXi e aplicativos plug-in.

["Ferramenta de Matriz de Interoperabilidade"](#)

Requisitos de porta

A tabela a seguir descreve as portas de rede que a NetApp utiliza e suas finalidades. Existem três tipos diferentes de portas:

- Portas externas: Essas portas são acessíveis de fora do cluster ou nó do Kubernetes. Elas permitem que os serviços se comuniquem com redes ou usuários externos, possibilitando a integração com sistemas fora do ambiente do cluster.
- Portas entre nós: Essas portas permitem a comunicação entre nós dentro do cluster Kubernetes. Elas são necessárias para tarefas do cluster, como compartilhamento de dados e trabalho em conjunto. Em implantações com um único nó, as portas entre nós são usadas apenas dentro do nó e não precisam de acesso externo. As portas entre nós podem aceitar tráfego de fora do cluster. Bloqueie o acesso à internet pelas portas entre nós com regras de firewall.
- Portas internas: Essas portas comunicam-se dentro do cluster Kubernetes usando endereços ClusterIP. Elas não são expostas externamente e não precisam ser adicionadas às regras do firewall.



Garanta que todos os nós das ONTAP tools estejam na mesma sub-rede para manter a comunicação ininterrupta entre si.

Clique para expandir ou recolher a tabela de requisitos de porta.

Nome do serviço/componente	Porta	Protocolo	Tipo de porta	Descrição
ntv-gateway-svc (LB)	443, 8443	TCP	Externo	Porta de passagem para comunicação de entrada do serviço VASA Provider. O certificado autoassinado do VASA Provider e o certificado de CA personalizado estão hospedados nesta porta.
SSH	22	TCP	Externo	Shell seguro para login em servidor remoto e execução de comandos.
servidor rke2	9345	TCP	Inter-nó	API supervisora RKE2 (restringir a redes confiáveis).
kube-apiserver	6443	TCP	Inter-nó	Porta do servidor da API do Kubernetes (restringir a redes confiáveis).
rpcbind/portmapper	111	TCP/UDP	Inter-nó	Utilizado para comunicação RPC entre serviços.
coredns (DNS)	53	TCP/UDP	Inter-nó	Serviço de Sistema de Nomes de Domínio (DNS) para resolução de nomes dentro do cluster.
NTP	123	UDP	Inter-nó	Protocolo de Tempo de Rede (NTP) para sincronização de tempo.
etcd	2379, 2380, 2381	TCP	Inter-nó	Armazenamento de chave-valor para dados de cluster.
kube-vip	2112	TCP	Inter-nó	Porta do servidor da API do Kubernetes.

Nome do serviço/componente	Porta	Protocolo	Tipo de porta	Descrição
kubelet	10248, 10250	TCP	Inter-nó	Componente do Kubernetes
kube-controller	10257	TCP	Inter-nó	Componente do Kubernetes
controlador de nuvem	10258	TCP	Inter-nó	Componente do Kubernetes
kube-scheduler	10259	TCP	Inter-nó	Componente do Kubernetes
kube-proxy	10249, 10256	TCP	Inter-nó	Componente do Kubernetes
calico-node	9091, 9099	TCP	Inter-nó	Componente de rede Calico.
containerd	10010	TCP	Inter-nó	Serviço daemon de contêiner.
VXLAN (Flannel)	8472	UDP	Inter-nó	Rede sobreposta para comunicação entre pods.



Para implantações de alta disponibilidade (HA), certifique-se de que a porta UDP 8472 esteja aberta entre todos os nós. Essa porta permite a comunicação entre pods em diferentes nós; bloqueá-la interromperá a rede entre os nós.

Limites de configuração para implantar ONTAP tools for VMware vSphere para datastores vVols

Você pode usar a tabela a seguir como um guia para configurar ONTAP tools for VMware vSphere.

Implantação	Tipo	Número de vVols	Número de hosts
Não HA	Pequeno (S)	até 12K	32
Não HA	Médio (M)	até 24K	64
Alta disponibilidade	Pequeno (S)	até 24K	64
Alta disponibilidade	Médio (M)	até 50k	128
Alta disponibilidade	Grande (L)	até 100k	256



A contagem de hosts na tabela representa o total combinado em todos os vCenters conectados.

Limitações de configuração para implantar ONTAP tools for VMware vSphere para datastores VMFS e NFS

Os limites de configuração listados nesta seção são validados e suportados pela NetApp. Os limites reais podem variar dependendo do seu ambiente e carga de trabalho. Exceder esses limites pode afetar o desempenho ou a capacidade de suporte e não é recomendado. Considere o seguinte ao analisar a tabela:

- A recuperação de desastres (DR) de máquinas virtuais é configurada usando políticas síncronas, assíncronas ou de sincronização estrita. DR não é compatível com o protocolo NVMe.
- A proteção de cluster de hosts ESXi usa SnapMirror Active Sync, que não suporta implantações multi-vCenter.
- As ONTAP tools restringem apenas o número de hosts ESXi e datastores com base no tamanho da implementação. Não há restrições quanto ao número de servidores vCenter que podem ser conectados às ONTAP tools.
- ONTAP tools realiza a descoberta paralela de todos os objetos de armazenamento. Os limites de configuração para objetos de armazenamento ONTAP se aplicam independentemente do número de objetos em uso ativo.
- ONTAP tools não impõe um limite ao número de vCenter Servers que podem ser integrados. Os limites de configuração são determinados pelo número de hosts e datastores suportados, conforme detalhado na tabela a seguir.

Implantação	Número de datastores VMFS e NFS	Número de datastores VMFS com DR habilitado	Número de hosts
Não-HA pequenos	200	80	32
Médio não HA	250	100	32
HA pequeno	350	200	64
HA Médio	600	200	128
HA Grande	1024	250	256

ONTAP tools for VMware vSphere - Adaptador de Replicação de Storage (SRA)

A tabela a seguir mostra os números suportados por instância do VMware Live Site Recovery usando ONTAP tools para VMware vSphere.

vCenter Tamanho da implantação	Pequeno	Médio
Número total de máquinas virtuais configuradas para proteção usando replicação baseada em arrays	2000	5000
Número total de grupos de proteção de replicação baseados em array	250	250
Número total de grupos de proteção por plano de recuperação	50	50
Número de datastores replicados	255	255

vCenter Tamanho da implantação	Pequeno	Médio
Número de VMs	4000	7000

A tabela a seguir mostra o número de instâncias do VMware Live Site Recovery e o tamanho correspondente de implementação das ONTAP tools for VMware vSphere.

Número de instâncias do VMware Live Site Recovery	Tamanho da implantação das ONTAP tools
Até 4	Pequeno
4 a 8	Médio
Mais de 8	Grande

Para obter mais informações, consulte ["Limitações operacionais do VMware Live Site Recovery"](#).

Requisitos de pré-implantação para ONTAP tools

Certifique-se de que os seguintes requisitos sejam atendidos antes de prosseguir com a implantação:

Requisitos	Seu status
vSphere versão, versão do ONTAP e versão do host ESXi são compatíveis com a versão das ONTAP tools.	☐ Sim ☐ Não
O ambiente do vCenter Server está configurado e instalado	☐ Sim ☐ Não
O cache do navegador é excluído	☐ Sim ☐ Não
Você possui as credenciais do servidor vCenter pai	☐ Sim ☐ Não
Você possui as credenciais de login para a instância do servidor vCenter, à qual as ONTAP tools for VMware vSphere se conectarão após a implantação para registro	☐ Sim ☐ Não
O nome de domínio no qual o certificado é emitido é mapeado para o endereço IP virtual em uma implantação multi-vCenter onde certificados de CA personalizados são obrigatórios.	☐ Sim ☐ Não
Você executou a verificação nslookup no nome de domínio para verificar se o domínio está sendo resolvido para o endereço IP pretendido.	☐ Sim ☐ Não
O certificado é criado com o nome de domínio e o endereço IP das ONTAP tools.	☐ Sim ☐ Não
As ferramentas, aplicações e serviços internos do ONTAP podem ser acessados a partir do vCenter Server.	☐ Sim ☐ Não

Requisitos	Seu status
Ao usar SVMs de alocação a vários clientes, você tem uma LIF de gerenciamento de SVM em cada SVM.	☐ Sim ☐ Não

Planilha de implantação

Para implantação de nó único

Utilize a planilha a seguir para coletar as informações necessárias para a implantação inicial do ONTAP tools for VMware vSphere:

Requisito	Seu valor
Endereço IP para o aplicativo ONTAP tools. Este é o endereço IP para acessar a interface web do ONTAP tools manager (balanceador de carga) em <a href="https://<ip>:8443/virtualization/ui/">https://<ip>:8443/virtualization/ui/	
Endereço IP virtual do ONTAP tools para comunicação interna. Este endereço IP é usado para comunicação interna em uma configuração com várias instâncias do ONTAP tools. Este endereço IP não deve ser o mesmo que o endereço IP do aplicativo ONTAP tools. (o plano de controle do Kubernetes)	
Nome de host DNS para o nó de gerenciamento das ONTAP tools	
Servidor DNS primário	
Servidor DNS secundário	
Domínio de pesquisa DNS	
Endereço IPv4 para o nó de gerenciamento das ONTAP tools. Trata-se de um endereço IPv4 exclusivo para a interface de gerenciamento na rede de gerenciamento. Isso é usado para conectar-se ao appliance das ferramentas ONTAP para acesso remoto de diagnóstico via SSH.	
Máscara de sub-rede para o endereço IPv4	
Gateway padrão para o endereço IPv4	
Endereço IPv6 (opcional)	
Comprimento do prefixo IPv6 (opcional)	
Gateway para o endereço IPv6 (opcional)	



Crie registros DNS para todos os endereços IP acima. Antes de atribuir nomes de host, mapeie-os para os endereços IP livres no DNS. Todos os endereços IP devem estar na mesma VLAN selecionada para implantação.

Para implantação de alta disponibilidade (HA)

Além dos requisitos de implantação de nó único, você precisará das seguintes informações para a implantação de alta disponibilidade (HA):

Requisito	Seu valor
Servidor DNS primário	
Servidor DNS secundário	
Domínio de pesquisa DNS	
Nome de host DNS para o segundo nó	
Endereço IP para o segundo nó	
Nome de host DNS para o terceiro nó	
Endereço IP para o terceiro nó	

Configuração do firewall de rede

Certifique-se de que as portas de firewall necessárias estejam abertas para todos os endereços IP relevantes. ONTAP tools exigem acesso à LIF pela porta 443. Para obter uma lista completa das portas necessárias, consulte a seção de requisitos de porta em ["Requisitos e limites de configuração do ONTAP tools for VMware vSphere"](#).

Configurações de armazenamento ONTAP

Para garantir a integração perfeita do storage ONTAP com ONTAP tools for VMware vSphere, considere as seguintes configurações:

- Se você estiver usando Fibre Channel (FC) para conectividade de armazenamento, configure o zoneamento em seus switches FC para conectar os hosts ESXi às LIFs FC da SVM. ["Aprenda sobre zoneamento FC e FCoE com sistemas ONTAP"](#)
- Para usar a replicação SnapMirror gerenciada por ferramentas do ONTAP, o administrador de storage do ONTAP deve criar ["Relações de peer de cluster ONTAP"](#) e ["Relações de peer de SVM intercluster ONTAP"](#) no ONTAP antes de usar o SnapMirror.

Implantar ONTAP tools

O appliance ONTAP tools for VMware vSphere é implantado como um nó único de tamanho pequeno com serviços essenciais para suportar os datastores NFS e VMFS. O processo de implantação do ONTAP tools pode levar até 45 minutos.

Antes de começar

Se você estiver implantando um único nó pequeno, uma biblioteca de conteúdo é opcional. Para implantações com vários nós ou de alta disponibilidade (HA), uma biblioteca de conteúdo é obrigatória. No VMware, uma biblioteca de conteúdo armazena modelos de máquinas virtuais, vApp templates e outros arquivos. Implantar com uma biblioteca de conteúdo proporciona uma experiência perfeita, pois não depende da conectividade de rede.

Considere o seguinte antes de criar uma biblioteca de conteúdo:

- Crie a biblioteca de conteúdo em um datastore compartilhado para que todos os hosts do cluster possam acessá-la.
- Configure a biblioteca de conteúdo antes de implantar o ONTAP tools for VMware vSphere OVA.
- Certifique-se de que a biblioteca de conteúdo seja criada antes de configurar o appliance para HA.



Não exclua o modelo OVA na biblioteca de conteúdo após a implantação.



Para permitir a implementação de HA no futuro, evite implantar a máquina virtual ONTAP tools diretamente em um host ESXi. Em vez disso, implante-a dentro de um cluster de hosts ESXi ou pool de recursos.

Siga estes passos para criar uma biblioteca de conteúdo:

1. Baixe o arquivo que contém os binários (.ova) e os certificados assinados para ONTAP tools for VMware vSphere do "[NetApp site de suporte](#)".
2. Faça login no cliente vSphere
3. Selecione o menu do cliente vSphere e selecione **bibliotecas de conteúdo**.
4. Selecione **Criar** à direita da página.
5. Forneça um nome para a biblioteca e crie a biblioteca de conteúdo.
6. Acesse a biblioteca de conteúdo que você criou.
7. Selecione **Ações** à direita da página, selecione **Importar item** e importe o arquivo OVA.



Para obter mais informações, consulte o "[Criação e uso de biblioteca de conteúdo](#)"blog.



Antes de prosseguir com a implantação, defina o Distributed Resource Scheduler (DRS) do cluster como Conservative. Isso garante que as VMs não sejam migradas durante a instalação.

As ONTAP tools for VMware vSphere são inicialmente implantadas como uma configuração sem HA. Para escalar para uma implantação HA, você precisará habilitar o adicionar sem desligamento de CPU e o hot-plug de memória. Você pode realizar esta etapa como parte do processo de implantação ou editar as configurações da máquina virtual após a implantação.

Passos

1. Baixe o arquivo que contém os binários (.ova) e os certificados assinados para o ONTAP tools for VMware vSphere do "[NetApp site de suporte](#)". Se você já importou o OVA para a biblioteca de conteúdo, pode pular esta etapa e prosseguir para a próxima etapa.
2. Faça login no servidor vSphere.
3. Acesse o pool de recursos, cluster ou host onde você pretende implantar o OVA.



Nunca armazene a máquina virtual do ONTAP tools for VMware vSphere em datastores vVols que ela gerencia.

4. Você pode implantar o OVA a partir da biblioteca de conteúdo ou do sistema local.

Do sistema local	Da biblioteca de conteúdo
------------------	---------------------------

a. Clique com o botão direito do mouse e selecione **Implantar modelo OVF....** b. Escolha o arquivo OVA na URL ou navegue até o local onde ele está armazenado, depois selecione **Avançar**.

a. Acesse sua biblioteca de conteúdo e selecione o item da biblioteca que você deseja implantar. b. Selecione **Ações > Nova VM a partir deste modelo**

5. No campo **Selecione um nome e uma pasta**, insira o nome da máquina virtual e escolha sua localização.

- Se você estiver usando a versão vCenter Server 8.0.3, selecione a opção **Personalizar o hardware desta máquina virtual**, que ativará uma etapa adicional chamada **Personalizar hardware** antes de prosseguir para a janela **Pronto para concluir**.
- Se você estiver usando a versão 7.0.3 do vCenter Server, siga as etapas na seção **What's next?** ao final da implantação.

netapp-ontap-tools-for-vmware-vsphere-10.5-1740090540 - New Virtual Machine from Content Library

- 1 Select a creation type
- 2 Select a template
- 3 Select a name and folder
- 4 Select a compute resource
- 5 Review details
- 6 Select storage
- 7 Ready to complete

Select a name and folder

Specify a unique name and target location

Virtual machine name: demootv

Select a location for the virtual machine.

vcf-vc01.ontappmtme.openenglab.netapp.com
> Raleigh

- ☐ Customize the operating system
- ☐ Customize this virtual machine's hardware

CANCEL

BACK

NEXT

6. Selecione um recurso de computador e selecione **Avançar**. Opcionalmente, marque a caixa para **Ligar automaticamente a máquina virtual implantada**.

7. Analise os detalhes do modelo e selecione **Avançar**.

8. Leia e aceite o contrato de licença e selecione **Avançar**.

9. Selecione o armazenamento para a configuração e o formato do disco e selecione **Avançar**.

10. Selecione a rede de destino para cada rede de origem e selecione **Avançar**.

11. Na janela **Personalizar modelo**, preencha os campos obrigatórios.

netapp-ontap-tools-for-vmware-vsphere-10.5-1773361740 - New Virtual Machine from Content Library

1 Select a name and folder

2 Select a compute resource

3 Review details

4 License agreements

5 Select storage

6 Select networks

7 Customize template

8 Customize hardware

9 Ready to complete

Customize template

ONTAP tools IP address

This will be the primary interface for communication with ONTAP tools

ONTAP tools virtual IP address*

ONTAP tools uses this IP address for internal communication

✓

vCenter Server configuration for ONTAP tools deployment

3 settings

vCenter Server hostname*

Enter the hostname of the target vCenter Server for ONTAP tools deployment.

vCenter Server username
(user@domain.com)*

Enter the user principal name of the vCenter Server account (for example, username@vsphere.local).
backup@vsphere.local

vCenter Server password*

Enter the vCenter Server password to authenticate your login.

Password

Password is required.

Confirm Password

CANCEL

BACK

NEXT

- **Nome do host:** Insira o nome do host da VM ONTAP tools. Use um formato de nome de host válido.
- **Endereço IP das ONTAP tools:** Esta é a interface de gerenciamento principal usada para acessar as ONTAP tools.
- **Endereço IPv4:** Este é o endereço IP do nó usado para acesso ao shell de diagnóstico e SSH para resolução de problemas e manutenção.

O nome do host do vCenter é o nome da instância do servidor vCenter onde o appliance ONTAP tools está implantado.

Para a instância do vCenter que será gerenciada pelas ONTAP tools, certifique-se de que a conta de usuário do vCenter tenha privilégios de administrador.

- Os nomes de host devem incluir letras (A-Z, a-z), dígitos (0-9) e hífens (-). Para configurar dual stack, especifique o nome do host mapeado para o endereço IPv6.



O IPv6 puro não é suportado. O modo misto é suportado com VLAN contendo endereços IPv6 e IPv4.

- O endereço IP do ONTAP tools é a interface principal para comunicação com o ONTAP tools.
- O IPv4 é o componente de endereço IP da configuração do nó, que pode ser utilizado para habilitar o acesso ao shell de diagnóstico e ao SSH no nó para fins de depuração e manutenção.

12. Ao usar a versão vCenter Server 8.0.3, na janela **Personalizar hardware**, habilite as opções **adicionar sem desligamento de CPU** e **hot-plug de memória** para permitir a funcionalidade de HA.

netapp-ontap-tools-for-vmware-vsphere-10.5-1773361740 - New Virtual Machine from Content Library

- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Select storage
- Select networks
- Customize template
- Customize hardware**
- Ready to complete

Customize hardware

Configure the virtual machine hardware

Virtual Hardware VM Options Advanced Parameters

[ADD NEW DEVICE](#)

CPU *

9 ⓘ

Cores per Socket

1

Sockets: 9

CPU Hot Plug

☒ Enable CPU Hot Add

Reservation

10305

MHz

Limit

Unlimited

MHz

Shares

Normal

1000

Hardware virtualization

☐ Expose hardware assisted virtualization to the guest OS

Performance Counters

☐ Enable virtualized CPU performance counters

Scheduling Affinity

ⓘ

CANCEL

BACK

NEXT

netapp-ontap-tools-for-vmware-vsphere-10.5-1773361740 - New Virtual Machine from Content Library

- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Select storage
- Select networks
- Customize template
- Customize hardware**
- Ready to complete

Customize hardware

Limit

Unlimited

MIN

Shares

Normal

1000

Hardware virtualization

☐

Expose hardware assisted virtualization to the guest OS

Performance Counters

☐

Enable virtualized CPU performance counters

Scheduling Affinity

I/O MMU

☐

Enabled

Memory *

18

GB

Reservation

9

GB

☐

Reserve all guest memory (All locked)

Limit

Unlimited

MB

Shares

Normal

368640

Memory Hot Plug

☒

Enable

Hard disks *

5 total | 348 GB

CANCEL

BACK

NEXT

13. Confira os detalhes na janela **Pronto para concluir** e selecione **Concluir**.

À medida que a tarefa de implantação é criada, o progresso é exibido na barra de tarefas do vSphere.

14. Ligue a máquina virtual após concluir a tarefa se a opção de ligar a máquina virtual automaticamente não tiver sido selecionada.

Você pode acompanhar o progresso da instalação no console web da máquina virtual.

Se houver discrepâncias no formulário OVF, uma caixa de diálogo solicitará ações corretivas. Use a tecla Tab para navegar, faça as alterações necessárias e selecione **OK**. Você tem três tentativas para resolver quaisquer problemas. Se os problemas persistirem após três tentativas, o processo de instalação será interrompido e recomenda-se tentar a instalação em uma nova máquina virtual.

Qual o próximo passo?

Se você implantou ONTAP tools for VMware vSphere com vCenter Server 7.0.3, siga estas etapas após a implantação.

- Faça login no cliente vCenter
- Desligue o nó do ONTAP tools.
- Vá para a máquina virtual ONTAP tools for VMware vSphere em **Inventários** e selecione a opção **Editar configurações**.
- Nas opções de **CPU**, marque a caixa de seleção **Habilitar adicionar sem desligamento de CPU**
- Nas opções de **Memória**, marque a caixa de seleção **Ativar** ao lado de **Memory hot plug**.

Solucionar erros de implantação das ONTAP tools

Se você encontrar problemas de implantação, revise os logs e os códigos de erro para diagnosticar e resolver problemas. A partir do ONTAP tools for VMware vSphere 10.5, os pacotes de logs coletados dos pods incluem logs do MongoDB, RabbitMQ e Vault, juntamente com o status e as descrições de todos os pods. Esses logs são fornecidos além dos logs de serviço existentes do ONTAP tools, aprimorando a capacidade de suporte e a solução de problemas.

Colete os arquivos de log

Você pode coletar arquivos de log para ONTAP tools for VMware vSphere a partir das opções disponíveis na interface de usuário do ONTAP tools Manager. O suporte técnico pode solicitar que você colete os arquivos de log para ajudar na solução de um problema.



A geração de logs a partir do ONTAP tools Manager inclui todos os logs de todas as instâncias do servidor vCenter. A geração de logs a partir da interface de usuário do cliente vCenter é limitada ao servidor vCenter selecionado.

Passos

1. Inicie o ONTAP tools Manager a partir de um navegador da web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as credenciais de administrador das ONTAP tools for VMware vSphere que você forneceu durante a implantação.
3. Selecione **Pacotes de Logs** na barra lateral.

Essa operação pode levar vários minutos.

4. Selecione **Gerar** para gerar os arquivos de log.
5. Insira o rótulo para o pacote de logs e selecione **Gerar**.

Baixe o arquivo tar.gz e envie-o para o suporte técnico.

Siga os passos abaixo para gerar um pacote de logs usando a interface de usuário do cliente vCenter:

Passos

1. Faça login no cliente vSphere.
2. Na página inicial do vSphere Client, acesse **Suporte > Pacote de logs > Gerar**.
3. Forneça o rótulo do pacote de logs e gere o pacote de logs. Você verá a opção de download quando os arquivos forem gerados. O download pode levar algum tempo.



O pacote de logs gerado substitui o pacote de logs gerado nos últimos 3 dias ou 72 h.

Códigos de erro de implantação

Você pode encontrar códigos de erro durante a implantação, reinicialização e operações de recuperação das ONTAP tools for VMware vSphere. Os códigos de erro têm cinco dígitos, onde os dois primeiros dígitos representam o script que encontrou o problema e os três últimos dígitos representam o fluxo de trabalho

específico dentro desse script.

Todos os registros de erros são gravados no arquivo `ansible-perl-errors.log`, localizado no diretório `/var/log`, para facilitar o rastreamento e a resolução de problemas. Este arquivo de log contém o código de erro e a tarefa Ansible que falhou.



Os códigos de erro fornecidos nesta página são apenas para referência. Entre em contato com a equipe de suporte se o erro persistir ou se não houver resolução mencionada.

A tabela a seguir lista os códigos de erro e os nomes de arquivo correspondentes.

Código de erro	Nome do script
00	firstboot-network-config.pl, modo deploy
01	firstboot-network-config.pl, modo upgrade
02	firstboot-inputs-validation.pl
03	firstboot-deploy-otv-ng.pl, implantar, HA
04	firstboot-deploy-otv-ng.pl, deploy, non-HA
05	firstboot-deploy-otv-ng.pl, reinicializar
06	firstboot-deploy-otv-ng.pl, upgrade, HA
07	firstboot-deploy-otv-ng.pl, atualização, não HA
08	firstboot-otv-recovery.pl
09	post-deploy-upgrade.pl

Os três últimos dígitos do código de erro indicam o erro específico no fluxo de trabalho dentro do script:

Código de erro de implantação	Fluxo de trabalho	Resolução
049	Para rede e validação, o script Perl também os atribuirá em breve	-
050	A geração da chave SSH falhou	Reinicie a máquina virtual (VM) primária.
053	Falha ao instalar o RKE2	Execute os seguintes comandos e reinicie a VM primária ou reimplante: <code>sudo rke2-killall.sh</code> (todas as VMs) <code>sudo rke2-uninstall.sh</code> (todas as VMs).
054	Falha ao configurar o kubeconfig	Reimplantar
055	Falha ao implantar o registry	Se o pod de registro estiver presente, aguarde até que ele esteja pronto e, em seguida, reinicie a VM primária ou reimplante.

059	KubeVip A implantação falhou	Certifique-se de que o endereço IP virtual para o plano de controle do Kubernetes e o endereço IP das ONTAP tools fornecidos durante a implantação pertençam à mesma VLAN e sejam endereços IP livres. Reinicie se todos os pontos anteriores estiverem corretos. Caso contrário, reimplente.
060	A implantação do operador falhou	Reiniciar
061	A implantação dos serviços falhou	Execute a depuração básica do Kubernetes, como get pods, get rs, get svc e assim por diante, no namespace ntv-system para obter mais detalhes e logs de erros em /var/log/ansible-perl-errors.log e /var/log/ansible-run.log e reimplante.
062	A implantação dos serviços das ONTAP tools falhou	Consulte os registros de erros em /var/log/ansible-perl-errors.log para obter mais detalhes e reimplente.
065	O URL da página Swagger não está acessível	Reimplantar
066	As etapas pós-implantação para o certificado de gateway falharam	Siga as etapas abaixo para recuperar/concluir a atualização: • Ativar shell de diagnóstico. • Execute o comando 'sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postDeploy'. • Verifique os registros em /var/log/post-deploy-upgrade.log.
088	A configuração de rotação de logs para o journald falhou	Verifique as configurações de rede da máquina virtual que são compatíveis com o host no qual a máquina virtual está hospedada. Você pode tentar migrar para outro host e reiniciar a máquina virtual.
089	A alteração da propriedade do arquivo de configuração de rotação do log de resumo falhou	Reinicie a máquina virtual primária.
096	Instale o provisionador de armazenamento dinâmico	-
108	O script de seeding falhou	-

114	A atualização do certificado interno na coleção do MongoDB falhou	Se a implantação falhar com o código de erro 114, siga os passos abaixo: • Ative o shell de diagnóstico. • Execute o seguinte comando: <pre>sudo perl /home/maint/scripts/post- deploy-upgrade.pl --internal_cert_update_ collection</pre> • Analise os registros em <pre>/var/log/otvng/post- deploy-upgrade.log</pre>
-----	---	--

Código de erro de reinicialização	Fluxo de trabalho	Resolução
067	A espera pelo rke2-server expirou.	-
101	Falha ao redefinir a senha do usuário de manutenção/console.	-
102	Falha ao excluir o arquivo de senha durante a redefinição da senha do usuário de manutenção/console.	-
103	Falha ao atualizar a senha do novo usuário de manutenção/console no cofre.	-
088	A configuração de rotação de logs para o journald falhou.	Verifique as configurações de rede da máquina virtual que são compatíveis com o host no qual a máquina virtual está hospedada. Você pode tentar migrar para outro host e reiniciar a máquina virtual.
089	A alteração da propriedade do arquivo de configuração de rotação do log de resumo falhou.	Reinicie a máquina virtual.

Configurar ONTAP tools para VMware vSphere

Adicionar instâncias do servidor vCenter às ONTAP tools

Adicione instâncias do vCenter Server ao ONTAP tools for VMware vSphere para configurar, gerenciar e proteger seus datastores virtuais no seu ambiente vCenter Server. Ao adicionar várias instâncias do vCenter Server, certificados CA personalizados são necessários para a comunicação segura entre o ONTAP tools e cada vCenter Server.

Sobre esta tarefa

As ferramentas ONTAP se integram ao vCenter Server para executar tarefas de storage como provisionamento, Snapshots e proteção de dados diretamente do cliente vSphere.

Adicionar uma instância do servidor vCenter às ONTAP tools aciona automaticamente as seguintes ações:

- As ferramentas ONTAP registram o plug-in do cliente vCenter como um plug-in remoto.
- Privilégios personalizados para os plug-ins e APIs são aplicados à instância do servidor vCenter.
- Funções personalizadas são criadas para gerenciar os usuários.
- O plug-in aparece como um atalho na interface de usuário do vSphere.

Antes de começar

- Certifique-se de que o certificado do servidor vCenter inclua uma extensão de Nome Alternativo do Assunto (SAN) válida, com entradas de DNS e endereço IP. Por exemplo:

```
X509v3 extensions:  
    X509v3 Subject Alternative Name:  
        DNS: vcenter.example.com, DNS: vcenter, IP Address: 192.168.0.50
```

Se o certificado não incluir uma extensão SAN, ou se a extensão SAN não contiver os valores corretos de DNS ou endereço IP, as operações das ONTAP tools poderão falhar devido a erros de validação do certificado.

- O Identificador de Rede Primário (PNID) do vCenter Server deve estar incluído nos detalhes do SAN. O PNID e o nome DNS devem ser idênticos e resolvíveis no DNS.
- Recomenda-se implantar o vCenter Server usando seu domínio totalmente qualificado (FQDN), garantindo que o SAN no certificado inclua DNS Name=machine_FQDN para compatibilidade e suporte ideais.
- Para obter mais informações, consulte a documentação VMware:
 - ["vSphere Requisitos de Certificação para Diferentes Caminhos de Solução"](#)
 - ["Substituir vCenter certificado SSL da máquina Certificado assinado por autoridade certificadora personalizada"](#)
 - ["Erro: o campo Nome Alternativo do Assunto \(SAN\) não contém o PNID. Forneça um certificado válido"](#)



Caso o FQDN não esteja disponível, você pode definir o PNID para o endereço IP e incluir o endereço IP no SAN. No entanto, isso não é recomendado pela VMware.

Passos

1. Abra um navegador da web e acesse a URL:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as credenciais de administrador das ONTAP tools for VMware vSphere que você forneceu durante a implantação.
3. Selecione **vCenters** > **Adicionar** para integrar as instâncias do servidor vCenter. Forneça seu endereço IP ou nome do host do vCenter, nome de usuário, senha e detalhes da porta.
4. Nas opções avançadas, obtenha o certificado do servidor vCenter automaticamente (autorize-o) ou carregue-o manualmente.



Você não precisa de uma conta de administrador para adicionar instâncias do vCenter às ONTAP tools. Você pode criar uma função personalizada sem a conta de administrador, com permissões limitadas. Consulte ["Use o RBAC do vCenter Server com ONTAP tools for VMware vSphere 10"](#) para obter detalhes.

Registre o provedor VASA com uma instância do vCenter Server nas ONTAP tools

Use ONTAP tools for VMware vSphere para registrar o VASA Provider em uma instância do vCenter Server. Isso permite o gerenciamento de armazenamento baseado em políticas, suporte a vVols e integração com appliances VMware Live Site Recovery em sistemas ONTAP.

As configurações do provedor VASA mostram o status de registro para o vCenter Server selecionado.

Passos

1. Faça login no cliente vSphere.
2. Selecione **Atalhos** > **NetApp ONTAP tools** na seção de plug-ins.
3. Selecione **Configurações** > **Configurações do VASA Provider**. As ONTAP tools exibem o status de registro do VASA Provider como não registrado.
4. Selecione o botão **Registrar** para registrar o VASA Provider.
5. Insira um nome e as credenciais do VASA Provider. O nome de usuário pode conter apenas letras, números e sublinhados. A senha deve ter entre 8 e 256 caracteres.
6. Selecione **Registrar**.
7. Após o registro bem-sucedido e a atualização da página, ONTAP tools exibe o status, o nome e a versão do VASA Provider registrado.

O que vem a seguir

Verifique se o provedor VASA integrado está listado em VASA Provider no cliente vCenter:

Passos

1. Acesse a instância do servidor vCenter.
2. Faça login com as credenciais de administrador.
3. Selecione **Provedores de armazenamento** > **Configurar**. Verifique se o provedor VASA integrado está listado corretamente.

Instale o plug-in NFS VAAI usando as ONTAP tools

O plug-in NFS vStorage API for Array Integration (NFS VAAI) conecta o VMware vSphere a arrays de storage NFS. Use ONTAP tools for VMware vSphere para instalar o plug-in VAAI. Isso permite que o array de storage NFS realize determinadas operações de armazenamento em vez dos hosts ESXi.

Antes de começar

- Baixe o ["NetApp NFS Plug-in para VMware VAAI"](#) pacote de instalação.
- Certifique-se de ter hosts ESXi com vSphere 7.0 U3 (patch mais recente ou posterior) e ONTAP 9.14.1 ou posterior.
- Monte um datastore NFS.

Passos

1. Faça login no cliente vSphere.
2. Selecione **Atalhos > NetApp ONTAP tools** na seção de plug-ins.
3. Selecione **Configurações > NFS VAAI Tools**.
4. Se você já carregou o plug-in VAAI no vCenter Server, selecione **Alterar em Versão existente**. Se não carregou, selecione **Carregar**.
5. Navegue e selecione o arquivo `.vib` e selecione **Carregar** para enviar o arquivo para ONTAP tools.
6. Selecione **Instalar no host ESXi**, selecione o host ESXi no qual deseja instalar o plug-in NFS VAAI e, em seguida, selecione **Instalar**.

O vSphere Web Client exibe apenas os hosts ESXi que podem instalar o plug-in. Você pode monitorar o progresso da instalação na seção de tarefas recentes.
7. Reinicie o host ESXi manualmente após a instalação.

Após reiniciar o host ESXi, ONTAP tools for VMware vSphere detecta e habilita automaticamente o plug-in NFS VAAI.

Qual é o próximo passo?

Após instalar o plug-in NFS VAAI e reinicializar seu host ESXi, configure as políticas de exportação NFS para o descarregamento de cópia VAAI. Certifique-se de que as regras da política de exportação atendam a estes requisitos:

- O volume ONTAP relevante permite chamadas NFSv4.
- O usuário raiz permanece como root e o NFSv4 é permitido em todos os volumes pai de junção.
- A opção de suporte ao VAAI está configurada no servidor NFS.

Para obter mais informações, consulte o ["Configure as políticas de exportação NFS corretas para o descarregamento de cópia VAAI"](#) artigo da Base de Conhecimento.

Informações relacionadas

["Suporte para VMware vStorage sobre NFS"](#)

["Ativar ou desativar NFSv4.0"](#)

Configure as configurações do host ESXi nas ONTAP tools

Configurar multipath e as definições de tempo limite do servidor ESXi ajuda a manter a disponibilidade de dados e a integridade. Isso permite o failover automático para um caminho de storage de backup caso o caminho primário fique indisponível.

Configurar as definições de multipath e tempo limite do servidor ESXi

ONTAP tools for VMware vSphere verifica e configura as configurações de multipath do host ESXi e as configurações de tempo limite do HBA que funcionam melhor com os sistemas de storage NetApp.

Sobre esta tarefa

Esse processo pode demorar, dependendo da sua configuração e da carga do sistema. Você pode acompanhar o progresso no painel Tarefas Recentes.

Passos

1. Na página inicial do cliente Web vSphere da VMware, selecione **Hosts and Clusters**.
2. Na página de atalhos do cliente Web do VMware vSphere, selecione **NetApp ONTAP tools** na seção de plug-ins.
3. Acesse o cartão **Conformidade do host ESXi** na visão geral (dashboard) do ONTAP tools for VMware vSphere plug-in.
4. Selecione o link **Aplicar configurações recomendadas**.
5. Na janela **Aplicar configurações de host recomendadas**, selecione os hosts que você deseja atualizar para usar as configurações recomendadas da NetApp e selecione **Avançar**.



Você pode expandir o host ESXi para ver os valores atuais.

6. Na página de configurações, selecione os valores recomendados conforme necessário.
7. No painel de resumo, verifique os valores e selecione **Concluir**. Você pode acompanhar o progresso no painel de tarefas recentes.

Defina os valores do host ESXi

Use as ONTAP tools for VMware vSphere para definir tempos limite e outros valores em hosts ESXi para desempenho e failover ideais. Esses valores são definidos com base em testes da NetApp.

Você pode definir os seguintes valores em um host ESXi:

Configurações do adaptador HBA/CNA

Define os seguintes parâmetros com os valores padrão:

- Disk.QFullSampleSize
- Disk.QFullThreshold
- Timeouts do HBA Emulex FC
- Timeouts do HBA FC da QLogic

Configurações MPIO

As configurações MPIO selecionam os melhores caminhos para os sistemas de armazenamento NetApp. As configurações MPIO escolhem o melhor caminho e o utilizam.

Para ambientes de alto desempenho ou ao testar com um único datastore LUN, ajuste a configuração de balanceamento de carga da política de seleção de caminho round-robin (VMW_PSP_RR) para melhorar o desempenho. Defina o valor padrão de IOPS de 1000 para 1.



As configurações MPIO não se aplicam aos protocolos NVMe, NVMe/FC e NVMe/TCP.

Configurações de NFS

Parâmetro	Defina este valor para...
Net.TcpipHeapSize	32
Net.TcpipHeapMax	1024 MB
NFS.MaxVolumes	256
NFS41.MaxVolumes	256
NFS.MaxQueueDepth	128 ou superior
NFS.HeartbeatMaxFailures	10
NFS.HeartbeatFrequency	12
NFS.HeartbeatTimeout	5

Configure funções e privilégios de usuário do ONTAP para ONTAP tools

Use esta seção para configurar funções e privilégios de usuário do ONTAP para backends de armazenamento com ONTAP tools for VMware vSphere e ONTAP System Manager. Você pode atribuir funções usando os arquivos JSON fornecidos, criar usuários e funções manualmente e aplicar os privilégios mínimos necessários para contas que não sejam de administrador.

Antes de começar

- Baixe o arquivo ONTAP Privileges das ONTAP tools for VMware vSphere usando https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip. Após baixar o arquivo zip, você encontra dois arquivos JSON. Use o arquivo JSON específico do ASA r2 ao configurar um sistema ASA r2.



Você pode criar usuários no nível do cluster ou diretamente no nível das máquinas virtuais de armazenamento (SVMs). Se você não usar o arquivo user_roles.json, certifique-se de que o usuário tenha as permissões mínimas necessárias para a SVM.

- Faça login com privilégios de administrador para o backend de armazenamento.

Passos

1. Extraia o arquivo https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip que você baixou.
2. Acesse o System Manager do ONTAP usando o endereço IP de gerenciamento do cluster.
3. Faça login no cluster com privilégios de administrador. Para configurar um usuário:
 - a. Para configurar um usuário das ONTAP tools em um cluster, selecione **Cluster > Configurações > Usuários e Funções**.
 - b. Para configurar um usuário das ONTAP tools SVM, selecione **Storage SVM > Settings > painel Users and Roles**.
 - c. Selecione **Adicionar** em Usuários.
 - d. Na caixa de diálogo **Adicionar Usuário**, selecione **produtos de virtualização**.
 - e. Navegue para selecionar e carregar o arquivo JSON do ONTAP Privileges. Para sistemas que não sejam ASA r2, selecione o arquivo users_roles.json e, para sistemas ASA r2, selecione o arquivo users_roles_ASAr2.json.

As ferramentas ONTAP preenchem automaticamente o campo Produto.

- f. Selecione a funcionalidade do produto como **VSC, VASA Provider e SRA** no menu suspenso.

As ferramentas ONTAP preenchem automaticamente o campo **Função** com base na funcionalidade do produto que você seleciona.

- g. Insira o nome de usuário e a senha necessários.
- h. Selecione os privilégios (Discovery, Create Storage, Modify Storage, Destroy Storage, NAS/SAN Role) que o usuário precisa e, em seguida, selecione **Adicionar**.

ONTAP tools adiciona a nova função e o novo usuário. Você pode visualizar os privilégios da função que você configurou.

Requisitos de mapeamento de agregado SVM

Ao provisionar datastores usando credenciais de usuário SVM, ONTAP tools for VMware vSphere cria volumes no agregado especificado na API POST dos datastores. ONTAP impede que usuários SVM criem volumes em agregados não mapeados para o SVM. Mapeie o SVM para os agregados necessários usando a API REST do ONTAP ou a CLI antes de criar volumes.

API REST:

```
PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"aggregates":{"name":["aggr1","aggr2","aggr3"]}}'
```

ONTAP CLI:

```

still15_vsim_ucs630f_aggr1 vserver show-aggregates
AvailableVserver      Aggregate      State      Size Type      SnapLock
Type-----
-----svm_test      still15_vsim_ucs630f_aggr1
online      10.11GB vmdisk  non-snaplock

```

Criar usuário e função do ONTAP manualmente

Crie usuários e funções manualmente sem o arquivo JSON.

1. Acesse o System Manager do ONTAP usando o endereço IP de gerenciamento do cluster.
2. Faça login no cluster com privilégios de administrador.
 - a. Para configurar as funções das ONTAP tools do cluster, selecione **Cluster > Configurações > Usuários e Funções**.
 - b. Para configurar as funções das ferramentas ONTAP do cluster SVM, selecione **Storage SVM > Configurações > Usuários e Funções**.
3. Crie funções:
 - a. Selecione **Adicionar** na tabela **Roles**.
 - b. Insira o **Nome da função** e os **Atributos da função**.

Adicione o **Caminho da API REST** e escolha o acesso na lista suspensa.
 - c. Adicione todas as APIs necessárias e salve as alterações.
4. Crie usuários:
 - a. Selecione **Adicionar** na tabela **Usuários**.
 - b. Na caixa de diálogo **Adicionar Usuário**, selecione **System Manager**.
 - c. Digite o **nome de usuário**.
 - d. Selecione **Função** nas opções criadas na etapa **Criar Funções** acima.
 - e. Insira os aplicativos aos quais deseja conceder acesso e o método de autenticação. ONTAPI e HTTP são os aplicativos obrigatórios, e o método de autenticação é **Senha**.
 - f. Defina a **senha do usuário** e **salve** o usuário.

Lista de privilégios mínimos necessários para usuário de cluster com escopo global que não seja administrador

Esta página lista os privilégios mínimos necessários para um usuário de cluster com escopo global que não seja administrador e que não possua um arquivo JSON. Se o cluster estiver em escopo local, use o arquivo JSON para criar usuários porque ONTAP tools for VMware vSphere precisa de mais do que apenas os privilégios de leitura para provisionamento no ONTAP.

Você pode acessar funcionalidades usando APIs:

API	Nível de acesso	Usado para
/api/cluster	Somente leitura	Descoberta de configuração de cluster

/api/cluster/licensing/licenses	Somente leitura	Verificação de licença para licenças específicas de protocolo
/api/cluster/nodes	Somente leitura	Descoberta de tipo de plataforma
/api/security/accounts	Somente leitura	Descoberta de privilégios
/api/security/roles	Somente leitura	Descoberta de privilégios
/api/storage/aggregates	Somente leitura	Verificação de espaço agregado durante o provisionamento de datastore/volume
/api/storage/cluster	Somente leitura	Para obter dados de espaço e eficiência em nível de cluster
/api/storage/disks	Somente leitura	Para obter os discos associados em um agregado
/api/storage/qos/policies	Ler/Criar/Modificar	Gerenciamento de QoS e políticas de VM
/api/svm/svms	Somente leitura	Para obter a configuração do SVM quando o cluster é adicionado localmente.
/api/network/ip/interfaces	Somente leitura	Adicionar backend de armazenamento - Para identificar o escopo do LIF de gerenciamento é cluster/SVM
/api/storage/availability-zones	Somente leitura	Descoberta SAZ. Aplicável à versão 9.16.1 do ONTAP e posteriores e aos sistemas ASA r2.
/api/cluster/metrocluster	Somente leitura	Obtém o status e os detalhes da configuração do MetroCluster.

Criar usuário com escopo de cluster baseado na API ONTAP para ONTAP tools for VMware vSphere



Para operações PATCH e reversão automática em datastores, são necessários os privilégios de descoberta, criação, modificação e destruição. A falta desses privilégios pode causar problemas no fluxo de trabalho e na limpeza.

Um usuário baseado na API do ONTAP com privilégios de descoberta, criação, modificação e destruição pode gerenciar os fluxos de trabalho das ONTAP tools.

Para criar um usuário com escopo de cluster e todos os privilégios mencionados acima, execute os seguintes comandos:

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all

security login rest-role create -role <role-name> -api
/api/private/cli/snapmirror -access all
```

```

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all

security login rest-role create -role <role-name> -api /api/storage/luns
-access all

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all

security login rest-role create -role <role-name> -api
/api/storage/qos/policies -access all

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create

```

```

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify

security login rest-role create -role <role-name> -api /api/cluster
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly

security login rest-role create -role <role-name> -api
/api/cluster/licensing/licenses -access readonly

security login rest-role create -role <role-name> -api /api/cluster/nodes
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly

security login rest-role create -role <role-name> -api

```

```

/api/protocols/san/fcp/services -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/aggregates -access readonly

security login rest-role create -role <role-name> -api
/api/storage/cluster -access readonly

security login rest-role create -role <role-name> -api /api/storage/disks
-access readonly

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly

security login rest-role create -role <role-name> -api
/api/cluster/metrocluster -access readonly

```

Além disso, para versões do ONTAP 9.16.0 e superiores, execute o seguinte comando:

```

security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all

```

Para sistemas ASA r2 com versões do ONTAP 9.16.1 ou superior, execute o seguinte comando:


```
security login rest-role create -role <role-name> -api  
/api/storage/availability-zones -access readonly
```

Criar usuário com escopo SVM baseado na API ONTAP para ONTAP tools for VMware vSphere

Execute os seguintes comandos para criar um usuário com escopo SVM e todos os privilégios:

```
security login rest-role create -role <role-name> -api  
/api/application/consistency-groups -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/private/cli/snapmirror -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/nfs/export-policies -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/nvme/subsystem-maps -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/nvme/subsystems -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/san/igroups -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/san/lun-maps -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/san/vvol-bindings -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/snapmirror/relationships -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/storage/volumes -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
"/api/storage/volumes/*/snapshots" -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api /api/storage/luns  
-access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/storage/namespaces -access all -vserver <vserver-name>
```

```

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create -vserver <vserver-
name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly -vserver <vserver-
name>

```

```

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly -vserver <vserver-name>

```

Além disso, para versões do ONTAP 9.16.0 e superiores, execute o seguinte comando:

```

security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all -vserver <vserver-name>

```

Para criar um novo usuário baseado em API usando as funções baseadas em API criadas anteriormente, execute o seguinte comando:

```

security login create -user-or-group-name <user-name> -application http
-authentication-method password -role <role-name> -vserver <cluster-or-
vserver-name>

```

Exemplo:

```
security login create -user-or-group-name testvpsraall -application http
-authentication-method password -role
OTV_10_VP_SRA_Discovery_Create_Modify_Destroy -vserver Cl_stil60-cluster_
```

Execute o seguinte comando para desbloquear a conta e habilitar o acesso à interface de gerenciamento:

```
security login unlock -user <user-name> -vserver <cluster-or-vserver-name>
```

Exemplo:

```
security login unlock -username testvpsraall -vserver Cl_stil60-cluster
```

Atualize o ONTAP tools for VMware vSphere 10.1 user para 10.3 user

Para usuários do ONTAP tools for VMware vSphere 10.1 com um usuário com escopo de cluster criado usando o arquivo JSON, use os seguintes comandos da CLI do ONTAP com privilégios de administrador para atualizar para a versão 10.3.

Para informações sobre as funcionalidades do produto:

- VSC
- VSC e VASA Provider
- VSC e SRA
- VSC, VASA Provider e SRA.

Privilégios de cluster:

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace show" -access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem show" -access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host show"
-access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map show"
-access all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host add" -access
all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map add" -access
all
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace delete" -access
all
```

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem delete" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host remove" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map remove" -access all

Para usuários do ONTAP tools for VMware vSphere 10.1 com um usuário com escopo SVM criado usando o arquivo json, use os comandos da CLI do ONTAP com privilégios de administrador para atualizar para a versão 10.3.

Privilégios SVM:

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host add" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map add" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace delete" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem delete" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host remove" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map remove" -access all -vserver <vserver-name>

Para habilitar os seguintes comandos, adicione os comandos *vserver nvme namespace show* e *vserver nvme subsystem show* à função existente.

```
vserver nvme namespace create  
  
vserver nvme namespace modify  
  
vserver nvme subsystem create  
  
vserver nvme subsystem modify
```

Atualize o usuário do ONTAP tools for VMware vSphere 10.3 para o usuário 10.4

A partir do ONTAP 9.16.1, atualize o usuário do ONTAP tools for VMware vSphere 10.3 para o usuário 10.4.

Para usuários do ONTAP tools for VMware vSphere 10.3 com um usuário com escopo de cluster criado usando o arquivo JSON e versão do ONTAP 9.16.1 ou superior, use o comando da CLI do ONTAP com privilégios de administrador para atualizar para a versão 10.4.

Para informações sobre as funcionalidades do produto:

- VSC
- VSC e VASA Provider
- VSC e SRA
- VSC, VASA Provider e SRA.

Privilégios de cluster:

```
security login role create -role <existing-role-name> -cmddirname "storage  
availability-zone show" -access all
```

Adicionar um backend de armazenamento às ferramentas ONTAP

Use ONTAP tools for VMware vSphere para adicionar e gerenciar storage backends para seus hosts ESXi. Você pode integrar clusters ou SVMs, habilitar suporte ao MetroCluster e validar certificados para conectividade segura. Você pode configurar storage backends usando o ONTAP tools Manager ou o cliente vSphere, monitorar o status dos certificados e redescobrir recursos manualmente após alterações no cluster.

Para adicionar um backend de armazenamento localmente, use as credenciais do cluster ou da SVM na interface do ONTAP tools. Os backends de armazenamento locais estão disponíveis apenas para o vCenter Server selecionado. ONTAP tools mapeia as SVMs para o vCenter Server para gerenciamento de vVols ou datastores VMFS. Para datastores VMFS e fluxos de trabalho SRA, você pode usar as credenciais da SVM sem mapear um cluster globalmente.

Para adicionar um backend de storage global, use as credenciais do cluster ONTAP no ONTAP tools Manager. Backends de storage globais permitem que fluxos de trabalho de descoberta identifiquem os recursos do cluster necessários para o gerenciamento de vVol. Em ambientes de alocação a vários clientes, você pode

adicionar um usuário SVM localmente para gerenciar datastores de vVols.

Consulte o artigo da base de conhecimento: ["OTV 10: O que é o escopo global e local do backend de armazenamento"](#) para obter mais informações sobre backends de armazenamento globais e locais.

Se o suporte ao MetroCluster estiver habilitado no ONTAP, integre ambos os clusters de origem e destino como backends de storage locais ou globais.

Antes de começar

Verifique se o certificado inclui um campo de Nome Alternativo do Assunto (SAN) válido. Os sistemas ONTAP usam o campo SAN para identificar as LIFs de gerenciamento de cluster e SVM.

Usando o Gerenciador de Ferramentas ONTAP



Em uma configuração de alocação a vários clientes, você pode adicionar um cluster de storage backend globalmente e o SVM localmente para usar as credenciais de usuário do SVM.

Passos

1. Inicie o ONTAP tools Manager a partir de um navegador da web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as credenciais de administrador das ONTAP tools for VMware vSphere que você forneceu durante a implantação.
3. Selecione **Storage Backends** na barra lateral.
4. Adicione o backend de armazenamento e forneça o endereço IP ou FQDN do servidor, nome de usuário e senha.



LIFs para gerenciamento de endereços IPv4 e IPv6 são suportados.

5. Busque automaticamente os certificados do cluster ONTAP e autorize o certificado, ou faça o upload manualmente navegando até sua localização.



Se necessário, você pode desativar a validação do Nome Alternativo do Assunto (SAN) no console de manutenção. Para obter instruções, consulte ["Alterar indicador de validação do certificado"](#).

6. Se o backend de armazenamento que você adicionar fizer parte de uma configuração MetroCluster, ONTAP tools Manager exibirá uma mensagem pop-up para adicionar o cluster emparelhado. Selecione **Add** e forneça os detalhes do backend de armazenamento peer MetroCluster.



Após o sistema ONTAP realizar um switchover e um switchback, execute manualmente a descoberta das ONTAP tools.

Utilizando a interface de usuário do cliente vSphere



Os datastores vVols não suportam a adição direta de um usuário SVM através da interface de usuário do cliente vSphere.

1. Faça login no cliente vSphere.
2. Na página de atalhos, selecione **NetApp ONTAP tools** na seção de plug-ins.
3. Selecione **Storage Backends** na barra lateral.
4. Adicione o backend de armazenamento e forneça o endereço IP do servidor, nome de usuário, senha e detalhes da porta.



Você pode adicionar um backend de armazenamento usando credenciais baseadas em cluster com LIFs de gerenciamento IPv4 ou IPv6. Para adicionar um usuário SVM diretamente, forneça credenciais baseadas em SVM juntamente com uma LIF de gerenciamento SVM. Se um cluster já estiver integrado, você não poderá integrar um usuário SVM desse cluster novamente.

5. Busque automaticamente os certificados do cluster ONTAP e autorize o certificado, ou faça o upload manualmente navegando até sua localização.
6. Se o backend de armazenamento adicionado fizer parte da configuração MetroCluster, as ONTAP tools exibem a tela **Adicionar par MetroCluster**. Selecione **Adicionar par** para adicionar o backend de armazenamento par.



Após o sistema ONTAP realizar um switchover e um switchback, execute manualmente a descoberta das ONTAP tools.

ONTAP tools lista o storage backend recém-adicionado na página **Storage backends**. Se um certificado expirar em 30 dias ou menos, ONTAP tools exibe um aviso na coluna de data de expiração do certificado. Após a expiração, ONTAP tools marca o storage backend como desconhecido porque não pode se conectar ao sistema de storage.

Informações relacionadas

["OTV 10: O que é o escopo global e local do backend de armazenamento"](#)

["Configurando os clusters em uma configuração MetroCluster"](#)

Associe um backend de armazenamento a uma instância do servidor vCenter nas ONTAP tools

Associe um backend de armazenamento a uma instância do servidor vCenter para habilitar o acesso para todas as instâncias do servidor vCenter. Para configuração do MetroCluster, ao associar um cluster de backend de armazenamento, certifique-se de associar também o cluster correspondente ao servidor vCenter.

Passos

1. Inicie o ONTAP tools Manager a partir de um navegador da web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as credenciais de administrador das ONTAP tools for VMware vSphere que você forneceu durante a implantação.
3. Selecione vCenter na barra lateral.
4. Selecione as elipses verticais ao lado da instância do servidor vCenter à qual você deseja conectar aos storage backends.
5. No menu suspenso, escolha o backend de armazenamento que você deseja associar à instância do servidor vCenter selecionada.

Configure o acesso à rede nas ONTAP tools

Por padrão, todos os endereços IP descobertos no host ESXi são adicionados automaticamente à política de exportação, a menos que você configure o acesso à rede. Você pode modificar a política de exportação para permitir acesso somente de endereços IP específicos. Se um host ESXi excluído tentar uma operação de montagem, a operação falhará.

Passos

1. Faça login no cliente vSphere.
2. Selecione **NetApp ONTAP tools** na página de atalhos, na seção de plug-ins.
3. No painel esquerdo do ONTAP tools, vá para **Configurações > Gerenciar acesso à rede > Editar**.

Para adicionar vários endereços IP, separe a lista com vírgulas, intervalos, Classless Inter-Domain Routing (CIDR) ou uma combinação dos três.

4. Selecione **Salvar**.

Criar um datastore nas ONTAP tools

Ao criar um datastore no nível do cluster de hosts, ONTAP tools o monta em todos os hosts de destino e habilita a ação somente se você tiver os privilégios necessários.

Interoperabilidade entre armazenamentos de dados nativos com vCenter Server e armazenamentos de dados gerenciados por ONTAP tools

A partir do ONTAP tools for VMware vSphere 10.4, o ONTAP tools cria igroups aninhados para datastores, com igroups pai específicos para datastores e igroups filho mapeados para os hosts. Você pode criar igroups planos a partir do ONTAP System Manager e usá-los para criar datastores VMFS sem usar o ONTAP tools. Consulte "[Gerencie iniciadores SAN e igroups](#)" para mais informações.

Após você integrar o armazenamento e executar a descoberta de datastore, ONTAP tools altera os igroups planos em datastores VMFS para igroups aninhados. Você não pode usar os igroups planos anteriores para criar novos datastores. Use a interface do ONTAP tools ou a API REST para reutilizar os igroups aninhados.

Crie um datastore vVols

A partir do ONTAP tools for VMware vSphere 10.3, você pode criar um datastore vVols em sistemas ASA r2 com eficiência de espaço como thin vVol. O VASA Provider cria um contêiner e os endpoints de protocolo desejados ao criar o datastore vVol. O VASA Provider não atribui nenhum volume de suporte a esse contêiner.

Antes de começar

- Certifique-se de que os agregados raiz não estejam mapeados para a SVM.
- Certifique-se de que o provedor VASA esteja registrado no vCenter selecionado.
- No sistema de storage ASA r2, a SVM deve ser mapeada para o agregado do usuário da SVM.

Passos

1. Faça login no cliente vSphere.
2. Clique com o botão direito do mouse em um sistema host, cluster de hosts ou data center e selecione **NetApp ONTAP tools > Create Datastore**.
3. Selecione vVols como **Tipo de armazenamento de dados**.
4. Insira o **Nome do repositório de dados** e as informações do **Protocolo**.



O sistema ASA r2 suporta os protocolos iSCSI e FC para vVols.

5. Selecione a máquina virtual de armazenamento onde você deseja criar o datastore.
6. Em opções avançadas:
 - Se você selecionar a **Política de exportação personalizada**, certifique-se de executar a descoberta em vCenter para todos os objetos. Recomenda-se que você não use esta opção.
 - Você pode selecionar um nome de **Grupo de iniciadores personalizado** para os protocolos iSCSI e FC.



No sistema de storage ASA do tipo SVM, as unidades de armazenamento (LUN/namespace) não são criadas porque o datastore é apenas um contêiner lógico.

7. No painel **Atributos de armazenamento**, você pode criar novos volumes ou usar os volumes existentes. No entanto, você não pode combinar esses dois tipos de volumes para criar um datastore vVols.

Ao criar um novo volume, você pode habilitar o QoS no datastore. Por padrão, um volume é criado para cada solicitação de criação de LUN. Ignore esta etapa para datastores vVols em sistemas de armazenamento ASA r2.

8. Revise sua seleção no painel **Resumo** e selecione **Concluir**.

Criar um datastore NFS

Um NFS datastore conecta hosts ESXi a storage compartilhado usando o protocolo NFS. Eles são simples e flexíveis e são usados em ambientes VMware vSphere.

Passos

1. Faça login no cliente vSphere.

2. Clique com o botão direito do mouse em um sistema host, cluster de hosts ou data center e selecione **NetApp ONTAP tools > Create datastore**.
3. Selecione NFS no campo **Datastore type**.
4. Insira o nome, o tamanho e as informações de protocolo do datastore no painel **Nome e protocolo**. Selecione **Datastore cluster** e **Kerberos authentication** nas opções avançadas.



A autenticação Kerberos está disponível somente quando o protocolo NFS 4.1 é selecionado.

5. Selecione **Plataforma e VM de armazenamento** no painel **Storage**.
6. Se você selecionar **Política de exportação personalizada** nas opções avançadas, execute a descoberta no vCenter para todos os objetos. Recomenda-se que você não use essa opção.



Você não pode criar um datastore NFS usando a política de volume padrão ou volume raiz do SVM.

- Nas opções avançadas, o botão de alternância **Assimétrico** só fica visível se desempenho ou capacidade estiver selecionado no menu suspenso da plataforma.
 - Ao selecionar a opção **Qualquer** no menu suspenso da plataforma, você pode ver todas as SVMs no vCenter. A plataforma e o sinalizador de assimetria não afetam a visibilidade.
7. Selecione o agregado para criação de volume no painel **Atributos de armazenamento**. Nas opções avançadas, escolha **Reserva de espaço** e **Habilitar QoS** conforme necessário.
 8. Revise as seleções no painel **Resumo** e selecione **Concluir**.

As ferramentas ONTAP criam o datastore NFS e o montam em todos os hosts.

Criar um datastore VMFS

VMFS é um sistema de arquivos em cluster para armazenar arquivos de máquinas virtuais. Vários hosts ESXi podem acessar os mesmos arquivos de VM simultaneamente para os recursos de vMotion e alta disponibilidade.

Em um cluster protegido:

- Você só pode criar datastores VMFS. Adicionar um datastore VMFS a um cluster protegido o protege automaticamente.
- Você não pode criar um datastore em um data center com um ou mais clusters de hosts protegidos.
- Você não pode criar um datastore em um host ESXi se o cluster do host pai estiver protegido por uma "Automated Failover Duplex policy" (configuração uniforme ou não uniforme).
- Você só pode criar um datastore VMFS em um host ESXi protegido por um relacionamento assíncrono. Você não pode criar e montar um datastore em um host ESXi que faça parte de um cluster de hosts protegido pela política "Automated Failover Duplex".

Antes de começar

- Habilite os serviços e LIFs para cada protocolo no lado de storage do ONTAP.
- Mapear SVM para agregado para usuário SVM no sistema de storage ASA r2.
- Configure o host ESXi se você estiver usando o protocolo NVMe/TCP:
 - a. Analise o ["Guia de compatibilidade da VMware"](#)



VMware vSphere 7.0 U3 e versões posteriores suportam o protocolo NVMe/TCP. No entanto, recomenda-se o uso do VMware vSphere 8.0 e versões posteriores.

- b. Verifique se o fornecedor da placa de interface de rede (NIC) oferece suporte à NIC ESXi com o protocolo NVMe/TCP.
 - c. Configure a placa de rede (NIC) do ESXi para NVMe/TCP de acordo com as especificações do fornecedor da placa de rede.
 - d. Ao usar o VMware vSphere 7 release, siga as instruções no site da VMware "[Configurar o vínculo VMkernel para o adaptador NVMe over TCP](#)" para configurar a vinculação de porta NVMe/TCP. Ao usar o VMware vSphere 8 release, siga "[Configurando NVMe sobre TCP no ESXi](#)", para configurar a vinculação de porta NVMe/TCP.
 - e. Para o lançamento do VMware vSphere 7, siga as instruções na página "[Ativar adaptadores de software NVMe sobre RDMA ou NVMe sobre TCP](#)" para configurar os adaptadores de software NVMe/TCP. Para o lançamento do VMware vSphere 8, siga "[Adicionar adaptadores de software NVMe sobre RDMA ou NVMe sobre TCP](#)" para configurar os adaptadores de software NVMe/TCP.
 - f. Execute a ação "[Descubra sistemas de armazenamento e hosts](#)" no host ESXi. Para obter mais informações, consulte "[Como configurar NVMe/TCP com vSphere 8.0 Update 1 e ONTAP 9.13.1 para datastores VMFS](#)".
- Se você estiver usando o protocolo NVMe/FC, execute as seguintes etapas para configurar o host ESXi:
 - a. Caso ainda não esteja habilitado, habilite o NVMe over Fabrics (NVMe-oF) em seus hosts ESXi.
 - b. Zoneamento SCSI completo.
 - c. Certifique-se de que os hosts ESXi e o sistema ONTAP estejam conectados nas camadas física e lógica.

Para configurar uma SVM do ONTAP para o protocolo FC, consulte "[Configurar uma SVM para FC](#)".

Para obter mais informações sobre como usar o protocolo NVMe/FC com VMware vSphere 8.0, consulte "[Configuração de host NVMe-oF para ESXi 8.x com ONTAP](#)".

Para obter mais informações sobre como usar NVMe/FC com VMware vSphere 7.0, consulte "[Guia de configuração do host ONTAP NVMe/FC](#)" e "[TR-4684](#)".

Passos

1. Faça login no cliente vSphere.
2. Clique com o botão direito do mouse em um sistema host, cluster de hosts ou data center e selecione **NetApp ONTAP tools > Create Datastore**.
3. Selecione o tipo de datastore VMFS.
4. Insira o nome, o tamanho e as informações de protocolo do datastore no painel **Nome e Protocolo**. Para adicionar o novo datastore a um cluster VMFS existente, selecione o cluster de datastore em Opções Avançadas.
5. Selecione uma VM de armazenamento no painel **Armazenamento**. Forneça o **Custom initiator group name** na seção **Advanced options**, conforme necessário. Você pode escolher um igroup existente para o datastore ou criar um novo igroup com um nome personalizado.

Quando o protocolo NVMe/FC ou NVMe/TCP é selecionado, um novo subsistema de namespace é criado e usado para o mapeamento de namespace. ONTAP tools cria o subsistema de namespace

usando o nome gerado automaticamente, que inclui o nome do datastore. Você pode renomear o subsistema de namespace no campo **nome do subsistema de namespace personalizado** nas opções avançadas do painel **Storage**.

6. No painel **atributos de armazenamento**:

- a. Selecione **Aggregate** nas opções do menu suspenso.



Para sistemas de storage ASA r2, a opção **Aggregate** não é exibida porque o storage é desagregado. Ao escolher um sistema de storage ASA r2 do tipo SVM, a página de atributos de storage exibe as opções para habilitar o QoS.

- b. As ferramentas ONTAP criam uma unidade de armazenamento (LUN/Namespase) com uma reserva de espaço reduzida com base no protocolo selecionado.



A partir do ONTAP 9.16.1, os sistemas de storage ASA r2 suportam até 12 nós por cluster.

- c. Selecione o **nível de serviço de desempenho** para sistemas de storage ASA r2 com SVM de 12 nós que seja um cluster heterogêneo. Esta opção não está disponível se o SVM selecionado for um cluster homogêneo ou usar um usuário SVM.

'Any' é o valor padrão do nível de serviço de desempenho (PSL). Essa configuração cria a unidade de armazenamento usando o algoritmo de alocação balanceada do ONTAP. No entanto, você pode selecionar a opção de desempenho ou extrema, conforme necessário.

- d. Selecione as opções **Usar volume existente** e **Ativar QoS**, conforme necessário, e forneça os detalhes.



No tipo de armazenamento ASA r2, a criação ou seleção de volume não se aplica à criação de unidade de armazenamento (LUN/Namespase). Portanto, essas opções não são exibidas.



Não é possível usar o volume existente para criar um datastore VMFS com protocolo NVMe/FC ou NVMe/TCP. Crie um novo volume para o datastore VMFS.

7. Analise os detalhes do datastore no painel **Resumo** e selecione **Concluir**.



Se você criar o datastore em um cluster protegido, verá uma mensagem somente leitura: "O datastore está sendo montado em um cluster protegido."

Resultado

As ferramentas ONTAP criam o datastore VMFS e o montam em todos os hosts.

Proteja armazenamentos de dados e máquinas virtuais

Proteja um cluster de hosts nas ONTAP tools

ONTAP tools for VMware vSphere gerencia a proteção de clusters de hosts. Todos os datastores pertencentes à SVM selecionada e montados em um ou mais hosts do cluster são protegidos sob um cluster de hosts.

Antes de começar

Certifique-se de atender a esses requisitos antes de proteger um cluster de hosts:

- O cluster de hosts contém datastores de uma única SVM.
- Os datastores no cluster de hosts não são montados em hosts fora do cluster.
- Os datastores montados no cluster host são datastores VMFS com protocolo iSCSI ou FC. Você não pode usar vVols, NFS ou datastores VMFS com protocolos NVMe/FC e NVMe/TCP.
- Os armazenamentos de dados baseados em volumes FlexVol/LUN montados em um host não fazem parte de nenhum grupo de consistência.
- Os armazenamentos de dados baseados em volumes FlexVol/LUN montados em um host não fazem parte de nenhum relacionamento SnapMirror.
- O cluster de hosts contém pelo menos um datastore.

Passos

1. Faça login no cliente vSphere.
2. Clique com o botão direito do mouse em um cluster de hosts e selecione **NetApp ONTAP tools > Proteger Cluster**.
3. Na janela de proteção do cluster, o sistema preenche automaticamente o tipo de datastore e os detalhes da máquina virtual de storage (VM) de origem. Selecione o link de datastores para visualizar os datastores protegidos.
4. Selecione **Adicionar relacionamento**.
5. Na janela **Adicionar SnapMirror Relationship**, selecione a **VM de armazenamento de destino** e o tipo de **política**.

O tipo de política pode ser Assíncrono ou AutomatedFailOverDuplex.

Ao adicionar a relação do SnapMirror como uma política do tipo AutomatedFailOverDuplex, você deve adicionar a VM de armazenamento de destino como um backend de armazenamento no mesmo vCenter onde ONTAP tools for VMware vSphere está implantado.

No tipo de política AutomatedFailOverDuplex, existem configurações de host uniformes e não uniformes. Ao selecionar o botão de alternância **Configuração de host uniforme**, a configuração do grupo iniciador do host é replicada implicitamente no site de destino. Para mais informações, consulte "[Conceitos e termos-chave](#)".

6. Se optar por uma configuração de host não uniforme, selecione o acesso ao host (origem/destino) para cada host dentro desse cluster.

7. Selecione **Add**.
8. Você pode editar a proteção do cluster de hosts usando a operação **Modificar proteção do cluster de hosts**. Você pode editar ou excluir os relacionamentos usando as opções do menu de reticências.
9. Selecione o botão **Proteger**.

O sistema cria uma tarefa do vCenter com detalhes do ID do trabalho e mostra seu progresso no painel de tarefas recentes. Esta é uma tarefa assíncrona; a interface de usuário mostra apenas o status de envio da solicitação e não aguarda a conclusão da tarefa.

10. Para visualizar os clusters de hosts protegidos, acesse **NetApp ONTAP tools > Proteção > Relacionamentos de clusters de hosts**. Selecione um grupo de consistência para visualizar sua capacidade, datastores associados e grupos de consistência filhos.



Se você precisar remover a proteção dentro de uma hora após a criação, execute primeiro a descoberta de armazenamento.

Informações relacionadas

["VMware vSphere Metro Storage Cluster \(vMSC\)"](#)

Proteja usando a proteção SRA

Configure o SRA nas ONTAP tools para proteger datastores

ONTAP tools for VMware vSphere oferece a opção de habilitar o recurso SRA para configurar a recuperação de desastres.

Antes de começar

- Você já deve ter configurado sua instância de servidor vCenter e os hosts ESXi.
- Você deveria ter implantado ONTAP tools for VMware vSphere.
- Você deveria ter baixado o arquivo do adaptador SRA `.tar.gz` do ["NetApp site de suporte"](#).
- Você deve ter os mesmos agendamentos personalizados de SnapMirror em ambos os clusters ONTAP de origem e destino antes de executar os fluxos de trabalho do SRA.
- ["Habilite os serviços do ONTAP tools for VMware vSphere"](#) para habilitar a funcionalidade SRA.

Passos

1. Faça login na interface de gerenciamento do VMware Live Site Recovery appliance usando o URL: `https://<srm_ip>:5480`, e então acesse Adaptadores de Replicação de Storage na interface de gerenciamento do VMware Live Site Recovery appliance.
2. Selecione **Novo Adaptador**.
3. Faça o upload do instalador `.tar.gz` do plug-in SRA para o VMware Live Site Recovery.
4. Analise novamente os adaptadores para verificar se os detalhes foram atualizados na página Storage Replication Adapters do VMware Live Site Recovery.



Após um failover, ações como expandir, montar e excluir podem não estar disponíveis para os datastores. Execute a descoberta de datastores para atualizar e exibir as ações apropriadas do menu de contexto.



Após cada operação de reproteção, você deve executar a descoberta de armazenamento em ambos os sites.

Em uma nova configuração com proteção SRA, sempre execute um teste de failover. Ignorar o teste de failover pode fazer com que a operação de reprotect falhe.

Em uma configuração de fan-out, após um failover do SnapMirror Active Sync em que a fonte do SnapMirror muda para o site B para Automated Failover Duplex e Asynchronous SnapMirror, execute um failover de teste entre os sites B e C. Ignorar esta etapa pode resultar em falha na operação de reproteção.

Informações relacionadas

["Configurar a recuperação de desastres para datastores NFS usando o VMware Site Recovery Manager"](#)

Configure o SRA em ONTAP tools for VMware vSphere para ambientes SAN e NAS

Você deve configurar os sistemas de armazenamento antes de executar o Storage Replication Adapter (SRA) para VMware Live Site Recovery.

Configurar o SRA para ambientes SAN



Os grupos de consistência em fluxos de trabalho SRA são suportados apenas com protocolos SAN (iSCSI e Fibre Channel) em sistemas de storage Unified e ASA r2.

Antes de começar

Você deve ter os seguintes programas instalados no site protegido e no site de recuperação:

- VMware Live Site Recovery: o site da VMware fornece documentação de instalação para o VMware Live Site Recovery.

["Sobre o VMware Live Site Recovery"](#)

- SRA: instale o adaptador no VMware Live Site Recovery.

Para configurações do protocolo iSCSI, observe o seguinte antes de executar os fluxos de trabalho do SRA:

- **Site protegido:** os adaptadores de armazenamento iSCSI e os detalhes da LIF de dados são configurados automaticamente ao provisionar datastores. Nenhuma configuração manual é necessária.
- **Local de recuperação:** os adaptadores de storage iSCSI devem ser configurados manualmente em cada host ESXi incluído no mapeamento de recursos para recuperação de desastres. Para evitar configurar adaptadores individualmente em cada host, crie um datastore de espaço reservado do tipo iSCSI no local de recuperação usando a SVM na qual os fluxos de trabalho do SRA estão configurados. Isso adiciona automaticamente o adaptador iSCSI e os endereços IP LIF de dados necessários a todos os hosts ESXi mapeados. Consulte ["Configure armazenamentos de dados de espaço reservado nas ONTAP tools"](#) para mais detalhes.

Passos

1. Verifique se os hosts ESXi primários estão conectados aos LUNs no sistema de storage primário no site protegido.
2. Verifique se os LUNs estão em igroups que têm a `ostype` opção definida como *VMware* no sistema de storage primário.
3. Verifique se os hosts ESXi no site de recuperação possuem conectividade iSCSI e Fibre Channel

apropriada com a storage virtual machine (SVM). Os hosts ESXi do site secundário devem ter acesso ao storage do site secundário, e os hosts ESXi do site primário devem ter acesso ao storage do site primário.

Você pode fazer isso verificando se os hosts ESXi possuem LUNs locais conectados à SVM ou executando o comando `iscsi show initiators` nas SVMs. Verifique o acesso às LUNs mapeadas no host ESXi para verificar a conectividade iSCSI.

Configurar o SRA para ambientes NAS



Grupos de consistência não são suportados para NFS em fluxos de trabalho do SRA. Se volumes de datastore NFS forem colocados em um grupo de consistência e protegidos, a operação Discover Devices falhará. Não use grupos de consistência ao proteger datastores NFS com o SRA.

Antes de começar

Você deve ter os seguintes programas instalados no site protegido e no site de recuperação:

- VMware Live Site Recovery: Você pode encontrar a documentação de instalação do VMware Live Site Recovery no site da VMware. "[Sobre o VMware Live Site Recovery](#)"
- SRA: instale o adaptador no VMware Live Site Recovery e no servidor SRA.

Passos

1. Verifique se os armazenamentos de dados no site protegido contêm máquinas virtuais registradas no vCenter Server.
2. Verifique se os hosts ESXi no site protegido montaram os volumes de exportação NFS da storage virtual machine (SVM).
3. Verifique se os endereços IP válidos nos quais as exportações NFS estão presentes estão especificados no campo **Endereços NFS** ao usar o assistente do Array Manager para adicionar arrays ao VMware Live Site Recovery. Não use o nome do host NFS ou o FQDN no campo **Endereços NFS**.
4. Use o comando `ping` em cada host ESXi no site de recuperação para verificar se o host possui uma porta VMkernel que pode acessar os endereços IP usados para fornecer exports NFS da SVM.

Configure o SRA nas ONTAP tools para ambientes altamente escaláveis

Você deve configurar os intervalos de tempo limite de armazenamento de acordo com as configurações recomendadas para o Storage Replication Adapter (SRA) para obter o melhor desempenho em ambientes de alta escalabilidade.

Configurações do provedor de armazenamento

Você deve definir os seguintes valores de tempo limite no VMware Live Site Recovery para ambientes dimensionados:

Configurações avançadas	Valores de tempo limite
<code>StorageProvider.resignatureTimeout</code>	Aumente o valor da configuração de 900 segundos para 12000 segundos.
<code>storageProvider.hostRescanDelaySec</code>	60

<code>storageProvider.hostRescanRepeatCnt</code>	20
<code>storageProvider.hostRescanTimeoutSec</code>	Defina um valor alto (por exemplo: 99999)

Você também deve habilitar a `StorageProvider.autoResignatureMode` opção.

Consulte ["Alterar configurações do provedor de armazenamento"](#) para obter mais informações sobre como modificar as configurações do Storage Provider.

Configurações de armazenamento

Quando você atingir um tempo limite, aumente os valores de `storage.commandTimeout` e `storage.maxConcurrentCommandCnt` para um valor mais alto.



O intervalo de tempo limite especificado é o valor máximo. Não é necessário esperar que o tempo limite máximo seja atingido. A maioria dos comandos termina dentro do intervalo de tempo limite máximo definido.

Consulte ["Alterar configurações de armazenamento"](#) para modificar as configurações do provedor SAN.

Configure o SRA no appliance VMware Live Site Recovery usando as ONTAP tools

Após implantar o appliance VMware Live Site Recovery, configure o Storage Replication Adapter (SRA) para habilitar o gerenciamento de recuperação de desastres.

Configurar o SRA no appliance VMware Live Site Recovery salva as credenciais das ONTAP tools for VMware vSphere dentro do appliance, permitindo a comunicação entre o VMware Live Site Recovery e o SRA.

Antes de começar

- Baixe o arquivo `.tar.gz` do ["NetApp site de suporte"](#).
- Habilite os serviços SRA no ONTAP tools Manager. Para obter mais informações, consulte a ["Habilitar serviços"](#) seção.
- Adicione servidores vCenter à appliance ONTAP tools for VMware vSphere. Para obter mais informações, consulte a ["Adicionar servidores vCenter"](#) seção.
- Adicione backends de armazenamento às ONTAP tools for VMware vSphere. Para obter mais informações, consulte a ["Adicionar backends de armazenamento"](#) seção.



Se você aplicou o patch de certificado do vCenter das ONTAP tools, atualize a configuração do vCenter no appliance VMware Live Site Recovery usando a porta (:5480). Para obter instruções, consulte ["Reconfigure o appliance do Site Recovery Manager"](#).

Passos

1. Na tela do appliance VMware Live Site Recovery, selecione **Storage Replication Adapter > New Adapter**.
2. Faça o upload do arquivo `.tar.gz` para o VMware Live Site Recovery.
3. Faça login no appliance VMware Live Site Recovery usando uma conta de administrador por meio de um cliente SSH, como o PuTTY.

4. Alterne para o usuário raiz usando o comando: `su root`
5. Execute o comando `cd /var/log/vmware/srm` para acessar o diretório de logs.
6. No local do log, insira o comando para obter o docker id usado pelo SRA: `docker ps -l`
7. Para fazer login no ID do contêiner, digite o comando: `docker exec -it -u srm <container id> sh`
8. Configure o VMware Live Site Recovery com o endereço IP e a senha das ONTAP tools for VMware vSphere usando o comando: `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`
 - Forneça a senha entre aspas simples para que o script Perl trate os caracteres especiais como parte da senha, não como delimitadores.
 - Você pode definir o nome de usuário e a senha do aplicativo (VASA Provider/SRA) no ONTAP tools Manager ao habilitar esses serviços pela primeira vez. Use essas credenciais para registrar o SRA no VMware Live Site Recovery.
 - Para localizar o GUID do vCenter, vá para a página do servidor vCenter em ONTAP tools Manager após adicionar sua instância do vCenter. Consulte a seção ["Adicionar servidores vCenter"](#).
9. Verifique novamente os adaptadores para confirmar que os detalhes atualizados aparecem na página Adaptadores de Replicação de Storage do VMware Live Site Recovery.

Resultados Uma mensagem de confirmação é exibida, indicando que as credenciais de armazenamento foram salvas. Agora você pode usar o SRA para se comunicar com o servidor SRA usando o endereço IP, a porta e as credenciais especificadas.

Atualizar credenciais SRA nas ferramentas ONTAP

Para que o VMware Live Site Recovery se comunique com o SRA, você deve atualizar as credenciais do SRA no servidor VMware Live Site Recovery caso as tenha modificado.

Antes de começar

Você deveria ter executado os passos mencionados no tópico ["Configurando o SRA no appliance VMware Live Site Recovery"](#).

Passos

1. Execute os seguintes comandos para excluir as credenciais armazenadas em cache das ferramentas ONTAP da máquina VMware Live Site Recovery:
 - a. `sudo su <enter root password>`
 - b. `docker ps`
 - c. `docker exec -it <container_id> sh`
 - d. `cd conf/`
 - e. `rm -rf *`
2. Execute o comando Perl para configurar o SRA com as novas credenciais:
 - a. `cd ..`
 - b. ``perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv`

-password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>`Você precisa colocar o valor da senha entre aspas simples.

Uma mensagem de sucesso confirmando que as credenciais de armazenamento foram salvas é exibida. O SRA pode se comunicar com o servidor SRA usando o endereço IP, a porta e as credenciais fornecidas.

Reconfigure vCenter no appliance VMware Live Site Recovery após uma alteração de certificado

Se o certificado do vCenter for alterado, por exemplo, após uma atualização do vCenter, você poderá encontrar um erro de incompatibilidade de impressão digital na extensão Site Recovery. Execute as seguintes etapas para resolvê-lo.

Passos

1. Reconfigure vCenter no appliance VMware Live Site Recovery

- Abra a interface de gerenciamento do VMware Live Site Recovery appliance em um navegador:
`https://<SRM_IP>:5480`
- Selecione a aba **Resumo**.
- Selecione **Reconfigurar** para a conexão do servidor vCenter.

Isso busca e aceita a impressão digital do certificado mais recente de vCenter.

2. Reconectar o emparelhamento do site (se o erro persistir)

Se o erro de incompatibilidade de impressão digital persistir após a reconfiguração:

- Faça login na interface de usuário do vCenter.
- Acesse a extensão **Site Recovery**.
- Localize a seção **Emparelhamento de Sites**.
- Selecione **Reconectar** para restabelecer o emparelhamento do site com o certificado atualizado.

Configure sites protegidos e de recuperação nas ferramentas ONTAP

Você deve criar grupos de proteção para proteger um grupo de máquinas virtuais no site protegido.

Ao adicionar um novo datastore, você pode incluí-lo no grupo de datastore existente ou adicionar um novo datastore e criar um novo volume ou grupo de consistência para proteção. Após adicionar um novo datastore a um grupo de consistência ou volume protegido, atualize SnapMirror e execute a descoberta de storage nos sites protegido e de recuperação. Você pode executar a descoberta manualmente ou em um agendamento para garantir que o novo datastore seja detectado e protegido.

Pareie os sites protegidos e de recuperação

Você deve emparelhar os sites protegidos e de recuperação criados usando seu vSphere Client para permitir que o Storage Replication Adapter (SRA) descubra os sistemas de storage.



O Adaptador de Replicação de Armazenamento (SRA) suporta fan-out com um relacionamento síncrono do tipo Automated Failover Duplex e um relacionamento assíncrono SnapMirror em grupo de consistência. No entanto, fan-out com dois relacionamentos assíncronos SnapMirror em grupos de consistência ou relacionamentos de fan-out SnapMirror em volumes não é suportado. Relacionamentos do tipo Vault SnapMirror não são considerados nessas restrições de fan-out. O suporte a grupo de consistência no SRA é limitado a protocolos SAN (iSCSI e fibre channel) em sistemas de armazenamento Unified e ASA r2. Grupos de consistência não são suportados para NFS. Se volumes de datastore NFS forem colocados em um grupo de consistência, a operação de descoberta de dispositivos falhará.

Antes de começar

- Você deve ter o VMware Live Site Recovery instalado nos sites protegidos e de recuperação.
- Você deve ter o SRA instalado nos sites protegidos e de recuperação.

Passos

1. Na página inicial do cliente vSphere, clicar duas vezes no ícone **Recuperação de Site** e depois selecione **Sites**.
2. Selecione **Objetos > Ações > Parear Sites**.
3. Na caixa de diálogo **Emparelhar servidores do Site Recovery Manager**, insira o endereço do Platform Services Controller do site protegido e selecione **Next**.
4. Na seção Selecionar vCenter Server, faça o seguinte:
 - a. Verifique se o servidor vCenter do site protegido aparece como um candidato compatível para emparelhamento.
 - b. Insira as credenciais administrativas do SSO e selecione **Concluir**.
5. Se solicitado, selecione **Sim** para aceitar os certificados de segurança.

Resultado

A caixa de diálogo **Objetos** exibe os sites protegidos e de recuperação.

Configurar grupos de proteção

Antes de começar

Você deve garantir que os sites de origem e destino estejam configurados para o seguinte:

- Mesma versão do VMware Live Site Recovery instalada
- Máquinas virtuais
- Locais protegidos e de recuperação emparelhados
- Os armazenamentos de dados de origem e destino devem ser montados em seus respectivos sites

Passos

1. Faça login no vCenter Server e selecione **Recuperação do Site > Grupos de Proteção**.
2. No painel **Grupos de Proteção**, selecione **Novo**.
3. Especifique um nome e uma descrição para o grupo de proteção, a direção e selecione **Next**.
4. No campo **Tipo**, selecione a opção **Tipo** como grupos de datastore (replicação baseada em array) para datastore NFS e VMFS. O domínio de falha consiste em SVMs com replicação habilitada. As SVMs que possuem apenas o peering implementado e não apresentam problemas são exibidas.

5. Na guia Grupos de replicação, selecione o par de arrays ativado ou os grupos de replicação que têm a máquina virtual que você configurou e, em seguida, selecione **Avançar**.

Todas as máquinas virtuais no grupo de replicação são adicionadas ao grupo de proteção.

6. Você pode selecionar o plano de recuperação existente ou criar um novo selecionando **Adicionar a um novo plano de recuperação**.
7. Na guia Pronto para concluir, revise os detalhes do grupo de proteção que você criou e selecione **Concluir**.

Configure os recursos do site protegido e do site de recuperação

Configure os mapeamentos de rede nas ferramentas ONTAP

Você deve configurar seus mapeamentos de recursos, como redes de máquinas virtuais, hosts ESXi e pastas em ambos os sites para permitir o mapeamento de cada recurso do site protegido para o recurso apropriado no site de recuperação.

Você deve concluir as seguintes configurações de recursos:

- Mapeamentos de rede
- Mapeamento de pastas
- Mapeamentos de recursos
- Datastores de espaço reservado

Antes de começar

Você deveria ter conectado os sites de proteção e de recuperação.

Passos

1. Faça login no vCenter Server e selecione **Recuperação de Site > Sites**.
2. Selecione seu site protegido e selecione **Gerenciar**.
3. Selecione **Mapeamentos de Rede > Novo** na guia manage para criar um novo mapeamento de rede.
4. No assistente Criar Mapeamento de Rede, faça o seguinte:
 - a. Selecione **Preparar mapeamentos automaticamente para redes com nomes correspondentes** e selecione **Avançar**.
 - b. Selecione os objetos de data center necessários para os sites protegidos e de recuperação e selecione **Adicionar mapeamentos**.
 - c. Selecione **Avançar** após os mapeamentos serem criados com sucesso.
 - d. Selecione o objeto usado anteriormente para criar o mapeamento reverso e, em seguida, selecione **Finish**.

Resultado

A página Mapeamentos de Rede exibe os recursos do site protegido e os recursos do site de recuperação. Você pode seguir os mesmos passos para outras redes em seu ambiente.

Configure o mapeamento de pastas nas ferramentas ONTAP

Você deve mapear suas pastas no site protegido e no site de recuperação para permitir a comunicação entre eles.

Antes de começar

Você deveria ter conectado os sites de proteção e de recuperação.

Passos

1. Faça login no vCenter Server e selecione **Recuperação de Site > Sites**.
2. Selecione seu site protegido e selecione **Gerenciar**.
3. Selecione **Mapeamentos de Pastas > ícone Pasta** na guia Gerenciar para criar um novo mapeamento de pastas.
4. No assistente Criar Mapeamento de Pastas, execute o seguinte:
 - a. Selecione **Preparar mapeamentos automaticamente para pastas com nomes correspondentes** e selecione **Avançar**.
 - b. Selecione os objetos de data center necessários para os sites protegidos e de recuperação e selecione **Adicionar mapeamentos**.
 - c. Selecione **Avançar** após os mapeamentos serem criados com sucesso.
 - d. Selecione o objeto usado anteriormente para criar o mapeamento reverso e, em seguida, selecione **Finish**.

Resultado

A página Mapeamento de Pastas exibe os recursos do site protegido e os recursos do site de recuperação. Você pode seguir os mesmos passos para outras pastas em seu ambiente.

Configure os mapeamentos de recursos nas ONTAP tools

Você deve mapear seus recursos no site protegido e no site de recuperação para que as máquinas virtuais sejam configuradas para realizar failover para um grupo de hosts ou outro.

Antes de começar

Você deveria ter conectado os sites de proteção e de recuperação.



No VMware Live Site Recovery, os recursos podem ser pools de recursos, hosts ESXi ou vSphere clusters.

Passos

1. Faça login no vCenter Server e selecione **Recuperação de Site > Sites**.
2. Selecione seu site protegido e selecione **Gerenciar**.
3. Selecione **Mapeamentos de Recursos > Novo** na guia manage para criar um novo mapeamento de recursos.
4. No assistente Criar Mapeamento de Recursos, execute o seguinte:
 - a. Selecione **Preparar mapeamentos automaticamente para recursos com nomes correspondentes** e selecione **Avançar**.

- b. Selecione os objetos de data center necessários para os sites protegidos e de recuperação e selecione **Adicionar mapeamentos**.
- c. Selecione **Avançar** após os mapeamentos serem criados com sucesso.
- d. Selecione o objeto usado anteriormente para criar o mapeamento reverso e, em seguida, selecione **Finish**.

Resultado

A página Mapeamento de Recursos exibe os recursos do site protegido e os recursos do site de recuperação. Você pode seguir os mesmos passos para outros recursos em seu ambiente.

Configure armazenamentos de dados de espaço reservado nas ONTAP tools

Configure um datastore de espaço reservado para reservar espaço no inventário do vCenter no site de recuperação para máquinas virtuais (VMs) protegidas. Os datastores de espaço reservado exigem capacidade mínima, pois as VMs de espaço reservado são pequenas e normalmente usam apenas algumas centenas de kilobytes.

Antes de começar

- Certifique-se de que os locais protegidos e de recuperação estejam conectados.
- Verifique se os mapeamentos de recursos foram configurados.

Passos

1. Faça login no vCenter Server e selecione **Recuperação de Site > Sites**.
2. Selecione seu site protegido e selecione **Gerenciar**.
3. Selecione **Datastores de espaço reservado > Novo** na guia gerenciar para criar um novo datastore de espaço reservado.
4. Selecione o datastore apropriado e clique em **OK**.



Os armazenamentos de dados provisórios podem residir em storage local ou remoto, mas não requerem replicação.

5. Repita os passos 3 a 5 para configurar um datastore provisório para o site de recuperação.

Configure o SRA usando o gerenciador de arrays nas ferramentas ONTAP

Você pode configurar o Storage Replication Adapter (SRA) usando o assistente Array Manager do VMware Live Site Recovery para habilitar as interações entre o VMware Live Site Recovery e as storage virtual machines (SVMs).

Antes de começar

- Você deveria ter emparelhado os sites protegidos e os sites de recuperação no VMware Live Site Recovery.
- Você deve ter configurado seu storage integrado antes de configurar o gerenciador de arrays.
- Você deve ter configurado e replicado as relações do SnapMirror entre os sites protegidos e os sites de recuperação.
- Você deveria ter habilitado as LIFs de gerenciamento do SVM para permitir a multilocação.

O SRA oferece suporte ao gerenciamento em nível de cluster e em nível de SVM. Se você adicionar armazenamento em nível de cluster, poderá descobrir e executar operações em todas as SVMs do cluster. Se você adicionar armazenamento em nível de SVM, poderá gerenciar apenas essa SVM específica.

Passos

1. No VMware Live Site Recovery, selecione **Gerenciadores de Array > Adicionar Gerenciador de Array**.
2. Insira as seguintes informações para descrever o array no VMware Live Site Recovery:
 - a. Insira um nome para identificar o gerenciador de arrays no campo **Nome de Exibição**.
 - b. No campo **Tipo de SRA**, selecione **NetApp Storage Replication Adapter for ONTAP**.
 - c. Insira as informações para conectar ao cluster ou à SVM:
 - Se você estiver se conectando a um cluster, você deve inserir a LIF de gerenciamento do cluster.
 - Se você estiver se conectando diretamente a uma SVM, você deve inserir o endereço IP da LIF de gerenciamento da SVM.



Ao configurar o gerenciador de arrays, você deve usar a mesma conexão (endereço IP) para o sistema de storage que foi usada para integrar o sistema de storage em ONTAP tools for VMware vSphere. Por exemplo, se a configuração do gerenciador de arrays estiver no escopo SVM, então o storage em ONTAP tools for VMware vSphere deve ser adicionado no nível SVM.

- d. Ao conectar-se a um cluster, especifique o nome da SVM no campo **Nome da SVM** ou deixe-o em branco para gerenciar todas as SVMs no cluster.
- e. Insira os volumes a serem descobertos no campo **Volume include list**.

Você pode inserir o volume de origem no site protegido e o volume de destino replicado no site de recuperação.

Por exemplo, se você quiser descobrir o volume `src_vol1` que está em uma relação do SnapMirror com o volume `dst_vol1`, você deve especificar `src_vol1` no campo de site protegido e `dst_vol1` no campo de site de recuperação.

- f. **(Opcional)** Insira os volumes a serem excluídos da descoberta no campo **Volume exclude list**.

Você pode inserir o volume de origem no site protegido e o volume de destino replicado no site de recuperação.

Por exemplo, se você quiser excluir o volume `src_vol1` que está em uma relação do SnapMirror com o volume `dst_vol1`, você deve especificar `src_vol1` no campo do site protegido e `dst_vol1` no campo do site de recuperação.

3. Selecione **Next**.
4. Verifique se a matriz foi detectada e exibida na parte inferior da janela Add Array Manager e selecione **Finish**.

Você pode seguir os mesmos passos para o site de recuperação usando os endereços IP de gerenciamento SVM e credenciais apropriados. Na tela Habilitar Pares de Arrays do assistente Adicionar Gerenciador de Arrays, você deve verificar se o par de arrays correto está selecionado e se ele aparece como pronto para ser habilitado.

Verifique os sistemas de armazenamento replicados nas ferramentas ONTAP

Você deve verificar se o site protegido e o site de recuperação foram emparelhados com sucesso após configurar o Storage Replication Adapter (SRA). O sistema de storage replicado deve ser detectável tanto pelo site protegido quanto pelo site de recuperação.

Antes de começar

- Você deveria ter configurado seu sistema de storage.
- Você deveria ter emparelhado o site protegido e o site de recuperação usando o gerenciador de arrays do VMware Live Site Recovery.
- Você deve ter habilitado a licença FlexClone e a licença SnapMirror antes de executar a operação de failover de teste e a operação de failover para SRA.
- Você deve ter as mesmas políticas e cronogramas de SnapMirror nos sites de origem e de destino.
- Se você estiver usando políticas personalizadas do SnapMirror com um agendamento personalizado, deverá configurar o mesmo agendamento e a mesma política nos sites protegidos e de recuperação.
- Se você estiver usando políticas personalizadas do SnapMirror (com agendamento padrão ou personalizado), deverá realizar a descoberta de storage a partir das ONTAP tools para que a nova política seja reconhecida. Sem isso, os fluxos de trabalho do SRA, incluindo test failover e failover, falharão. Realize a descoberta de storage nos seguintes pontos:
 - Após criar a política personalizada no site de recuperação.
 - Após uma operação de re proteção, que recria a política no site protegido.

Passos

1. Faça login no seu vCenter Server.
2. Acesse **Recuperação de Site > Replicação Baseada em Array**.
3. Selecione o par de matrizes desejado e verifique os detalhes correspondentes.

Os sistemas de armazenamento devem ser detectados no site protegido e no site de recuperação com o status **Enabled**.

Proteção contra fan-out em ONTAP tools

Em um cenário de proteção fan-out, o grupo de consistência é duplamente protegido com um relacionamento síncrono no primeiro destino ONTAP cluster e com um relacionamento assíncrono no segundo destino ONTAP cluster. Os fluxos de trabalho de criação, edição e exclusão de proteção ativa de SnapMirror mantêm a proteção síncrona. Os fluxos de trabalho de failover e re proteção do appliance VMware Live Site Recovery mantêm a proteção assíncrona.



O recurso Fan-out não é suportado para usuários de SVM.

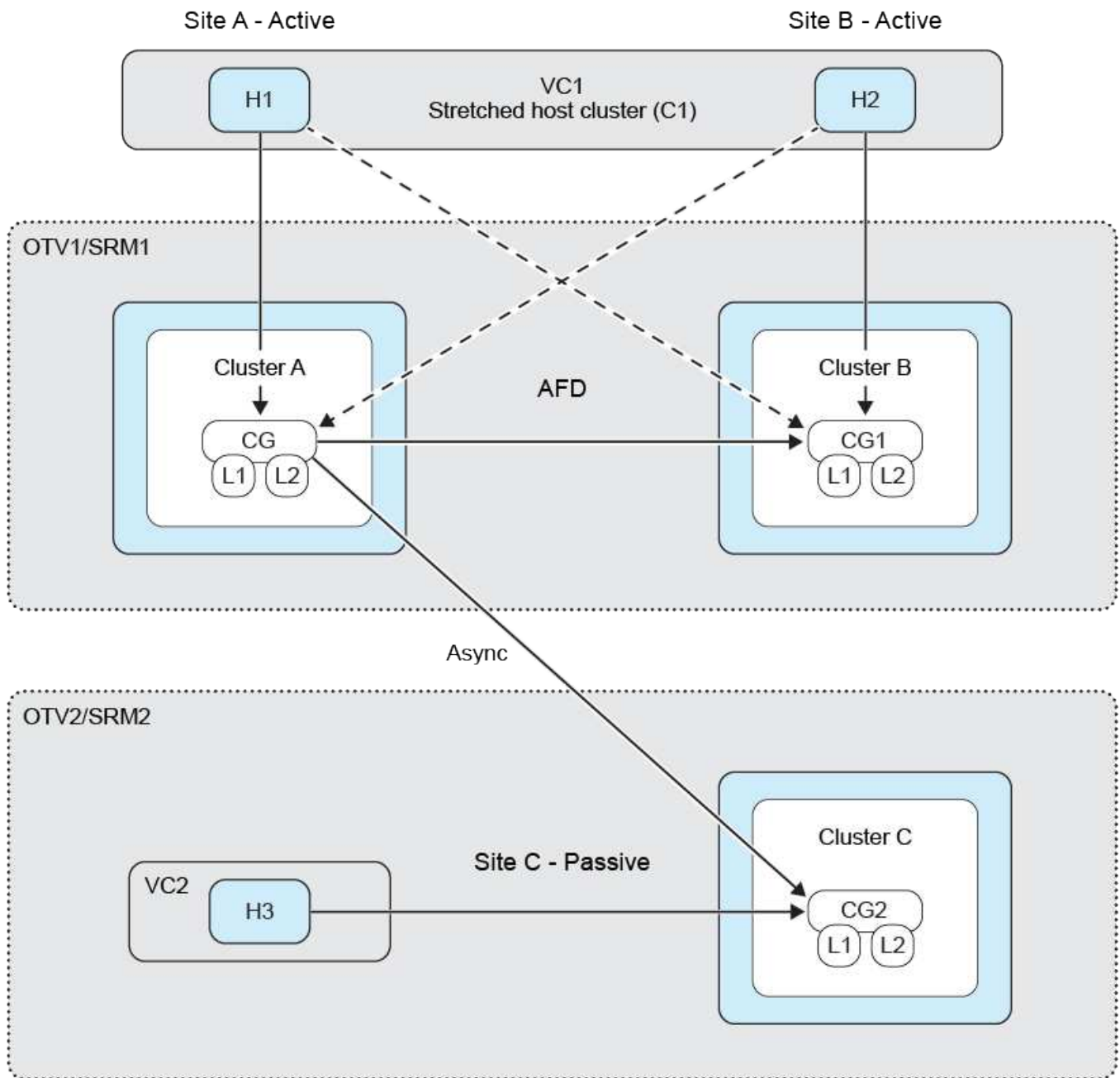
Para configurar a proteção contra dispersão (fan-out), faça o peering dos três clusters do site e das SVMs.

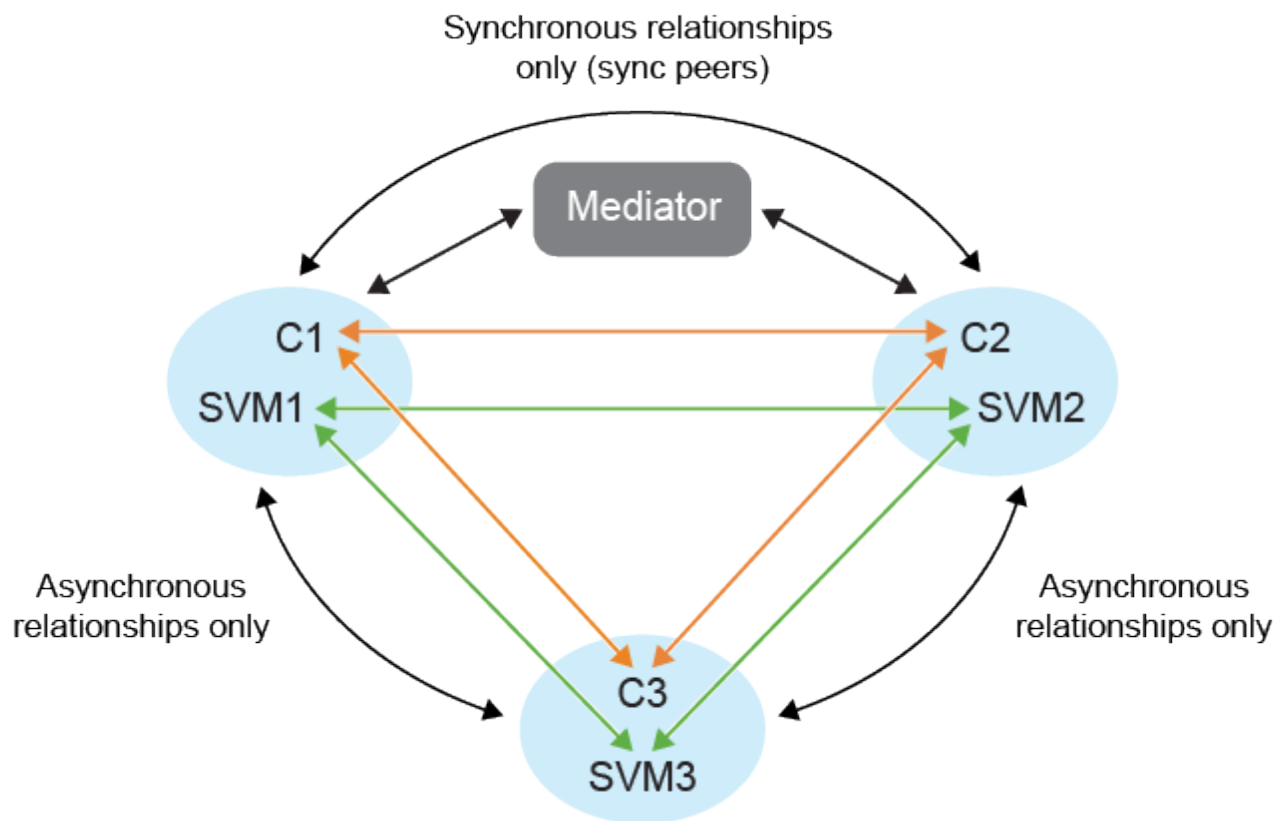
Exemplo:

Se	então
----	-------

• O grupo de consistência de origem está no cluster c1 e SVM svm1 • O primeiro grupo de consistência de destino está no cluster c2 e SVM svm2 e • O segundo grupo de consistência de destino está no cluster c3 e SVM svm3	• O peering de cluster no cluster ONTAP de origem será (C1, C2) e (C1, C3). • O peering de cluster no primeiro cluster ONTAP de destino será (C2, C1) e (C2, C3) e • O peering de cluster no segundo cluster ONTAP de destino será (C3, C1) e (C3, C2). • O peering SVM na SVM de origem será (svm1, svm2) e (svm1, svm3). • O peering SVM no primeiro SVM de destino será (svm2, svm1) e (svm2, svm3) e • O peering SVM no segundo destino svm será (svm3, svm1) e (svm3, svm2).
--	--

O diagrama a seguir mostra a configuração de proteção contra dispersão (fan-out):





Passos

1. Selecione um novo repositório de dados provisório. Os critérios de seleção do repositório de dados provisório para proteção faseada são:
 - Não coloque o datastore placeholder no cluster de hosts que você está protegendo.
 - Se precisar incluir o datastore placeholder no cluster de hosts, adicione-o ao appliance do VMware Live Site Recovery antes de configurar a proteção de sincronização ativa do SnapMirror. Com essa configuração, você pode deixar o datastore placeholder fora da proteção.

Para obter mais informações, consulte ["Selecione um datastore de espaço reservado"](#)

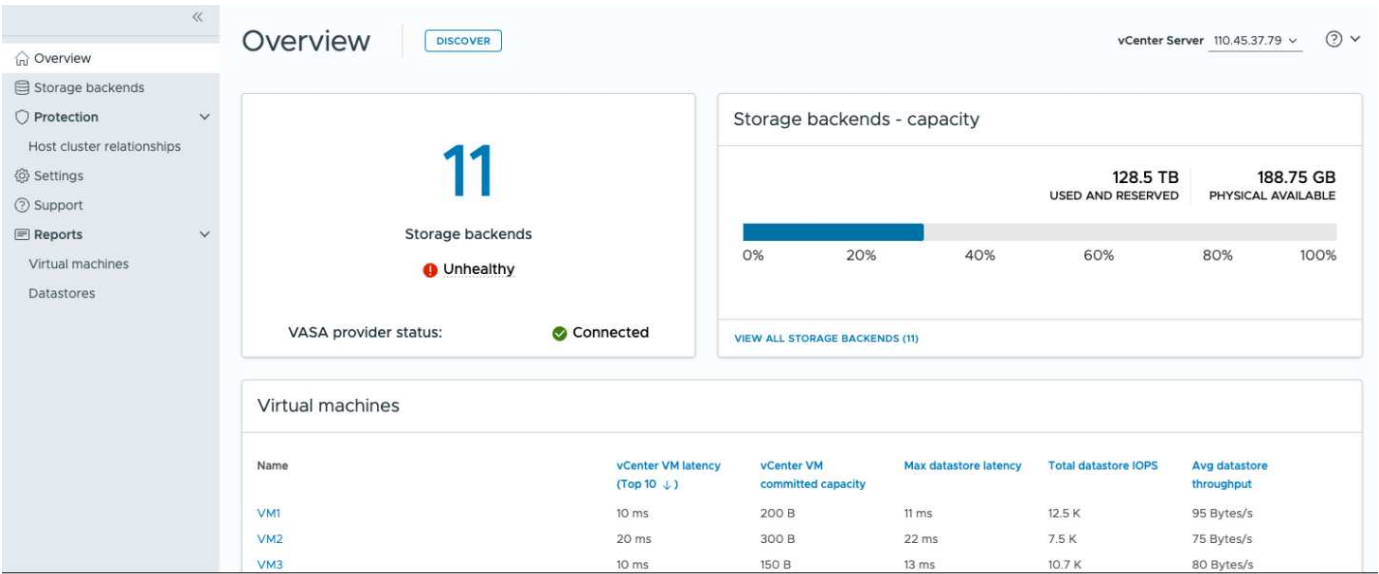
2. Adicione armazenamentos de dados à proteção do cluster de hosts seguindo ["Modificar cluster de hosts protegidos"](#). Adicione tipos de política assíncrona e síncrona.

Gerencie as ferramentas ONTAP para VMware vSphere

Saiba mais sobre o painel de ferramentas do ONTAP

Selecionar o ícone do plug-in ONTAP tools for VMware vSphere na seção de atalhos no cliente vCenter abre a página de visão geral. Este painel fornece um resumo do plug-in ONTAP tools for VMware vSphere.

No Modo Vinculado Avançado (ELM), o menu suspenso do vCenter Server é exibido. Escolha um vCenter Server para visualizar seus dados. O menu suspenso está disponível em todas as visualizações de listagem do plug-in. Quando você seleciona um vCenter Server em uma página, ele permanece o mesmo ao alternar entre as guias do plug-in.



Na página de visão geral, você pode executar a ação **Discovery**. A ação de descoberta detecta back-ends de storage, hosts, datastores e status ou relacionamentos de proteção recém-adicionados ou atualizados no nível do vCenter. Execute a descoberta sob demanda sem esperar pela descoberta agendada.



O botão **Descoberta** só estará habilitado se você tiver o privilégio necessário para realizar a descoberta.

Após o envio da solicitação de descoberta, você pode acompanhar o andamento da ação no painel de tarefas recentes.

O painel de controle possui vários cartões que mostram diferentes elementos do sistema. A tabela a seguir mostra os diferentes cartões e o que eles representam.

Cartão	Descrição
--------	-----------

Status	O cartão de Status exibe o número de storage backends e o status geral de integridade dos storage backends e do VASA Provider. O status dos storage backends é exibido como Íntegro quando todos os storage backends estão com status normal e como Não íntegro se algum storage backend apresentar um problema (status Desconhecido/Inacessível/Degradado). Selecione a dica de ferramenta para abrir os detalhes do status dos storage backends. Você pode selecionar qualquer storage backend para obter mais detalhes. O link Outros estados do VASA Provider exibe o estado atual do VASA Provider registrado no vCenter Server.
Backends de storage - Capacidade	Este cartão mostra a capacidade agregada usada e disponível de todos os backends de armazenamento para a instância de servidor vCenter selecionada. Para sistemas de armazenamento ASA r2, os dados de capacidade não são exibidos porque o armazenamento é desagregado.
Máquinas virtuais	Este cartão exibe as 10 principais máquinas virtuais classificadas por métrica de desempenho. Você pode selecionar o cabeçalho para obter as 10 principais máquinas virtuais para a métrica selecionada, classificadas em ordem crescente ou decrescente. As alterações de classificação e filtragem feitas no cartão permanecem até que você altere ou limpe o cache do navegador.
Datastores	Este cartão exibe os 10 principais datastores classificados por uma métrica de desempenho. Você pode selecionar o cabeçalho para obter os 10 principais datastores para a métrica selecionada, classificados em ordem crescente ou decrescente. As alterações de classificação e filtragem feitas no cartão persistem até que você altere ou limpe o cache do navegador. Há um menu suspenso de tipo de datastore para selecionar o tipo de datastore: NFS, VMFS ou vVols.
Cartão de conformidade do host ESXi	Este cartão mostra se todos os hosts ESXi (para o vCenter selecionado) seguem as configurações de host recomendadas da NetApp por grupo ou categoria. Você pode selecionar o link Aplicar configurações recomendadas para aplicar as configurações recomendadas. Você pode selecionar o status de conformidade dos hosts para ver a lista de hosts.

Como as ONTAP tools gerenciam igroups e políticas de exportação

Os grupos de iniciadores (igroups) são tabelas de nomes de porta World Wide Port

Name (WWPNs) de hosts do protocolo FC ou nomes de nós qualificados de hosts iSCSI. Você pode definir igroups e mapeá-los para LUNs para controlar quais iniciadores têm acesso aos LUNs.

Nas ONTAP tools for VMware vSphere 9.x, os igroups eram criados e gerenciados em uma estrutura plana, onde cada datastore em vCenter estava associado a um único igroup. Esse modelo limitava a flexibilidade e a reutilização de igroups em vários datastores. ONTAP tools for VMware vSphere introduz igroups aninhados, onde cada datastore em vCenter está associado a um igroup pai, enquanto cada host está vinculado a um igroup filho sob esse pai. Você pode definir igroups pai personalizados com nomes definidos pelo usuário para reutilização em vários datastores, facilitando o gerenciamento de igroups. Entenda o fluxo de trabalho de igroup para gerenciar LUNs e datastores nas ONTAP tools for VMware vSphere. Diferentes fluxos de trabalho geram configurações de igroup variadas, como mostrado nos exemplos a seguir:



Os nomes mencionados são apenas para fins ilustrativos e não se referem a nomes reais de igroups. Os igroups gerenciados pelas ONTAP tools usam o prefixo "otv_". Os igroups personalizados podem receber qualquer nome.

Termo	Descrição
DS<number>	Datastore
iqn<number>	IQN do iniciador
host<number>	MoRef do host
lun<number>	ID LUN
<DSName>Igroup<number>	Grupo pai padrão (gerenciado por ONTAP tools)
<Host-Moref>Igroup<number>	Igroup filho
CustomIgroup<number>	Igroup pai personalizado definido pelo usuário
ClassicIgroup<number>	Igroup usado nas versões 9.x das ONTAP tools.

Exemplo 1:

Criar armazenamento de dados em um único host com um iniciador

Fluxo de trabalho: [Criar] DS1 (lun1): host1 (iqn1)

Resultado:

- DS1Igroup:
 - host1Igroup → (iqn1: lun1)

ONTAP cria o igroup pai DS1Igroup para DS1 e mapeia o igroup filho host1Igroup para lun1. O sistema sempre mapeia LUNs para igroups filhos.

Exemplo 2:

Montar o datastore existente em um host adicional

Fluxo de trabalho: [Mount] DS1 (lun1): host2 (iqn2)

Resultado:

- DS1Igroup:

- host1lgroup → (iqn1: lun1)
- host2lgroup → (iqn2: lun1)

ONTAP tools for VMware vSphere criam um igroup filho host2lgroup e o adicionam ao igroup pai existente DS1lgroup.

Exemplo 3:

Desmontar um datastore de um host

Fluxo de trabalho: [Desmontar] DS1 (lun1): host1 (iqn1)

Resultado:

- DS1lgroup:
 - host2lgroup → (iqn2: lun1)

ONTAP tools for VMware vSphere removem o host1lgroup da hierarquia. O sistema não exclui explicitamente os igroups filhos. Ele os exclui sob estas duas condições:

- Se nenhum LUN estiver mapeado, o sistema ONTAP exclui o igroup filho.
- Uma tarefa de limpeza agendada remove os igroups filhos órfãos sem mapeamento de LUN. Esses cenários se aplicam somente aos igroups gerenciados pelas ONTAP tools, não aos criados pelo usuário.

Exemplo 4:

Excluir datastore

Fluxo de trabalho: [Excluir] DS1 (lun1): host2 (iqn2)

Resultado:

- DS1lgroup:
 - host2lgroup → (iqn2: lun1)

Os igroups pai e filho são removidos, a menos que outro datastore reutilize o igroup pai. Os igroups filho não são excluídos explicitamente

Exemplo 5:

Crie vários datastores sob um igroup pai personalizado

Fluxo de trabalho:

- [Criar] DS2 (lun2): host1 (iqn1), host2 (iqn2)
- [Criar] DS3 (lun3): host1 (iqn1), host3 (iqn3)

Resultado:

- Customlgroup1:
 - host1lgroup → (iqn1: lun2, lun3)
 - host2lgroup → (iqn2: lun2)
 - host3lgroup → (iqn3: lun3)

CustomIgroup1 é criado para o DS2 e reutilizado para o DS3. Os igroups filhos são criados ou atualizados sob o pai compartilhado, com cada igroup filho mapeando para seus respectivos LUNs.

Exemplo 6:

Exclua um datastore em um igroup pai personalizado.

Fluxo de trabalho: [Excluir] DS2 (lun2): host1 (iqn1), host2 (iqn2)

Resultado:

- CustomIgroup1:
 - host1Igroup → (iqn1: lun3)
 - host3Igroup → (iqn3: lun3)
- Embora o CustomIgroup1 não seja reutilizado, ele não é excluído.
- Se nenhum LUN estiver mapeado, o sistema ONTAP exclui o host2Igroup.
- host1Igroup não é excluído porque está mapeado para o lun3 do DS3. Custom igroups nunca são excluídos, independentemente do status de reutilização.

Exemplo 7:

Expandir vVols datastore (Adicionar volume)

Fluxo de trabalho:

Antes da expansão:

[Expandir] DS4 (lun4): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4)

Após a expansão:

[Expandir] DS4 (lun4, lun5): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4, lun5)

Um novo LUN é criado e mapeado para o igroup filho existente host4Igroup.

Exemplo 8:

Reduzir datastore vVols (Remover Volume)

Fluxo de trabalho:

Antes de encolher:

[Encolher] DS4 (lun4, lun5): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4, lun5)

Após a redução:

[Encolher] DS4 (lun4): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4)

O LUN especificado (lun5) foi desassociado do igroup filho. O igroup permanece ativo enquanto tiver pelo menos um LUN mapeado.

Exemplo 9:

Migração das ferramentas ONTAP 9 para 10 (normalização de igroup)

Fluxo de trabalho

ONTAP tools for VMware vSphere versões 9.x não suportam igroups hierárquicos. Durante a migração para versões 10.3 ou superiores, os igroups devem ser normalizados na estrutura hierárquica.

Antes da migração:

[Migração] DS6 (lun6, lun7): host6 (iqn6), host7 (iqn7) → Classicigroup1 (iqn6 & iqn7 : lun6, lun7)

A lógica das ONTAP tools 9.x permite múltiplos iniciadores por igroup sem impor um mapeamento de host um para um.

Após a migração:

[Migração] DS6 (lun6, lun7): host6 (iqn6), host7 (iqn7) → Classicigroup1: otv_Classicigroup1 (iqn6 & iqn7 : lun6, lun7)

Durante a migração:

- Um novo igroup pai (Classicigroup1) é criado.
- O igroup original é renomeado com o prefixo otv_ e torna-se um igroup filho.

Isso garante a conformidade com o modelo hierárquico.

A partir do ONTAP tools 10.5P2, os igroups migrados são excluídos quando deixam de ser utilizados. Em versões anteriores, os igroups migrados nunca eram removidos. Observe o seguinte:

- Os igroups migrados não podem ser reutilizados em diferentes datastores.
- Igroups personalizados (definidos pelo usuário) nunca são excluídos e ainda podem ser reutilizados.

Tópicos relacionados

["Sobre igroups"](#)

Políticas de exportação

As políticas de exportação controlam o acesso ao datastore NFS e as permissões do cliente em ONTAP tools for VMware vSphere. As políticas de exportação são criadas e gerenciadas em sistemas ONTAP e podem ser usadas com datastores NFS para impor o controle de acesso. Cada política de exportação consiste em regras que especificam os clientes (endereços IP ou sub-redes) que têm permissão de acesso e as permissões concedidas (somente leitura ou leitura e gravação).

Ao criar um datastore NFS nas ONTAP tools for VMware vSphere, você pode selecionar uma política de exportação existente ou criar uma nova. A política de exportação é então aplicada ao datastore, garantindo que apenas clientes autorizados possam acessá-lo.

Ao montar um datastore NFS em um novo host ESXi, ONTAP tools for VMware vSphere adiciona o endereço IP do host à política de exportação existente associada ao datastore. Isso permite que o novo host acesse o datastore sem criar uma nova política de exportação.

Ao excluir ou desmontar um NFS datastore de um host ESXi, ONTAP tools for VMware vSphere remove o endereço IP do host da política de exportação. Se nenhum outro host estiver usando essa política de exportação, ela será excluída. Ao excluir um NFS datastore, ONTAP tools for VMware vSphere remove a política de exportação associada a esse datastore, caso ela não seja reutilizada por nenhum outro datastore. Se a política de exportação for reutilizada, ela mantém o endereço IP do host e não é alterada. Ao excluir os datastores, a política de exportação desatribui o endereço IP do host e atribui uma política de exportação padrão, para que os sistemas ONTAP possam acessá-los, se necessário.

A atribuição da política de exportação difere quando ela é reutilizada em diferentes datastores. Ao reutilizar a política de exportação, você pode adicionar o novo endereço IP do host à política. Quando você exclui ou desmonta um datastore que usa uma política de exportação compartilhada, a política não será excluída. Ela permanece inalterada e o endereço IP do host não é removido, pois é compartilhado com os outros datastores. A reutilização de políticas de exportação não é recomendada, pois pode causar problemas de acesso e latência.

Tópicos relacionados

["Criar uma política de exportação"](#)

Como as ONTAP tools gerenciam igroups

Se você gerencia tanto as VMs do ONTAP tools quanto os sistemas de storage ONTAP, é importante entender como os igroups se comportam, especialmente ao mover datastores de ambientes não gerenciados pelo ONTAP tools para aqueles que são. Esta página explica como o ONTAP tools para VMware vSphere representa e gerencia igroups. Trata-se de informação conceitual para entender as diferenças de comportamento entre versões anteriores e o modelo atual de igroup aninhado.

A partir do ONTAP tools for VMware vSphere 10.4, ONTAP tools cria e mantém automaticamente objetos ONTAP e vCenter, simplificando o gerenciamento de datastores em ambientes de datacenter VMware. A partir do ONTAP tools for VMware vSphere 10.5 P2, os igroups migrados também são excluídos automaticamente quando não estão mais em uso.

Resumo rápido do comportamento

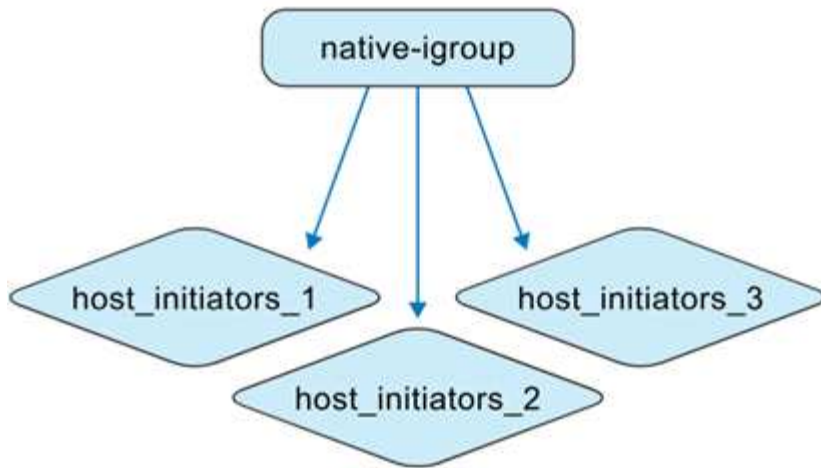
- Os datastores VMFS gerenciados pelas ONTAP tools usam igroups aninhados: um igroup pai por contexto de datastore e igroups filhos por host.
- Os mapeamentos de LUN são aplicados aos igroups filhos.
- Grupos de instâncias (igroups) pais personalizados podem ser reutilizados em diferentes datastores.
- Os igroups migrados das ONTAP tools 9.x não podem ser reutilizados.

Contextos de igroup

ONTAP tools for VMware vSphere lidam com igroups em dois contextos.

Grupos de igroups gerenciados por ferramentas não-ONTAP

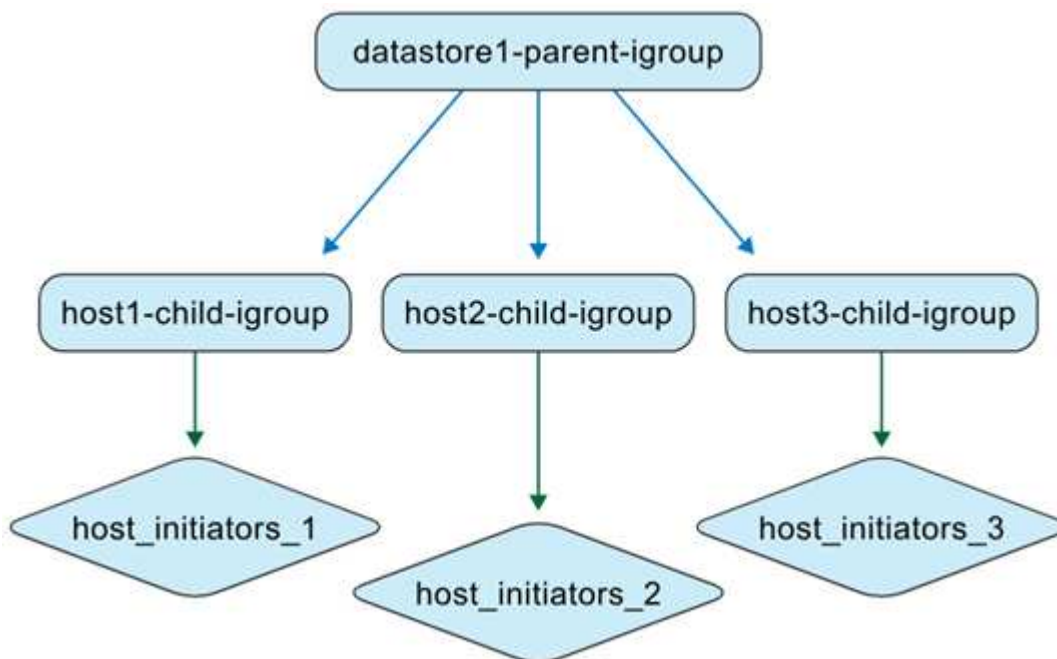
Como administrador de storage, você pode criar igroups no sistema ONTAP como estruturas planas ou aninhadas. A ilustração a seguir mostra um igroup plano criado diretamente no ONTAP.

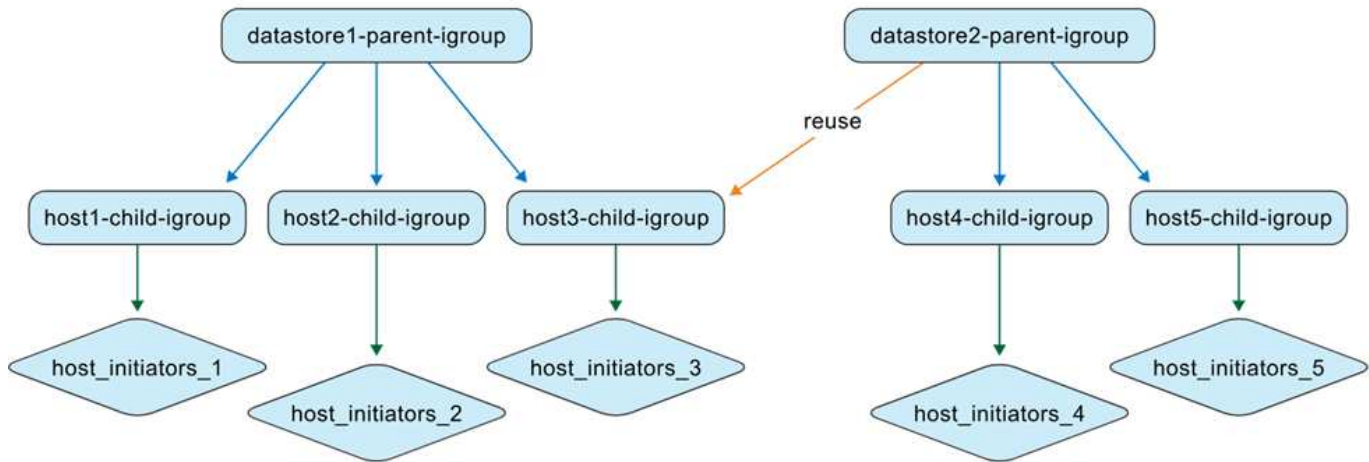


Igroups gerenciados pelo ONTAP tools

Ao criar datastores, ONTAP tools for VMware vSphere cria igroups em uma estrutura aninhada.

Por exemplo, quando o datastore1 é criado e montado nos hosts 1, 2 e 3, e um novo datastore (datastore2) é criado e montado nos hosts 3, 4 e 5, ONTAP tools reutiliza o igroup em nível de host para um gerenciamento eficiente.





Comportamento de nomeação

Ao criar um datastore e deixar o campo igroup em branco, ONTAP tools cria uma estrutura de igroup aninhada padrão.

- Padrão de nomenclatura do grupo pai:
`otv_<vcguid>_<host_parent_datacenterMoref>_<datastore_name>`
- Padrão de nomenclatura do grupo filho: `otv_<hostMoref>_<vcguid>`

A interface ONTAP mostra a relação entre os igroups pai e filho no campo **Parent Initiator Group**.

Comportamento por cenário

Cenário	Comportamento do igroup parental	Comportamento do igroup filho	Mapeamento e visibilidade de LUN
Repositório de dados criado com a configuração padrão do igroup	Um igroup pai padrão gerenciado pelas ONTAP tools é criado.	Grupos de interface (igroups) filhos no nível do host são criados conforme necessário.	Os LUNs são mapeados para igroups filhos. O datastore aparece no inventário do servidor vCenter.
Repositório de dados criado com nome de igroup personalizado	Um igroup pai personalizado é criado com o nome especificado.	Os grupos de instâncias (igroups) filhos existentes no nível do host são reutilizados quando os hosts se sobrepõem.	O novo LUN do datastore é mapeado para o igroup filho reutilizado ou recém-criado. O datastore aparece no vCenter Server.
Grupo de igroup personalizado existente reutilizado durante a criação do datastore	Um igroup pai personalizado existente é selecionado e reutilizado.	Os grupos filhos são reutilizados ou estendidos com base na associação do host.	O novo LUN do datastore é mapeado através do igroup filho associado. O datastore aparece no vCenter Server.

Cenário	Comportamento do igroup parental	Comportamento do igroup filho	Mapeamento e visibilidade de LUN
Datastore e igroup criados nativamente no ONTAP e vCenter, depois descobertos pelas ONTAP tools	ONTAP tools cria um igroup pai em seu contexto de gerenciamento e mantém o nome original do igroup.	ONTAP tools renomeia o igroup original com o `otv_` prefixo e o representa como um igroup filho na hierarquia.	Os mapeamentos de iniciadores permanecem inalterados. Somente os igroups mapeados para datastores são convertidos durante a descoberta.

Reutilização de igroup personalizado e comportamento da API

Na interface de usuário do ONTAP tools, você pode reutilizar um igroup pai personalizado existente na lista suspensa ao criar um datastore.

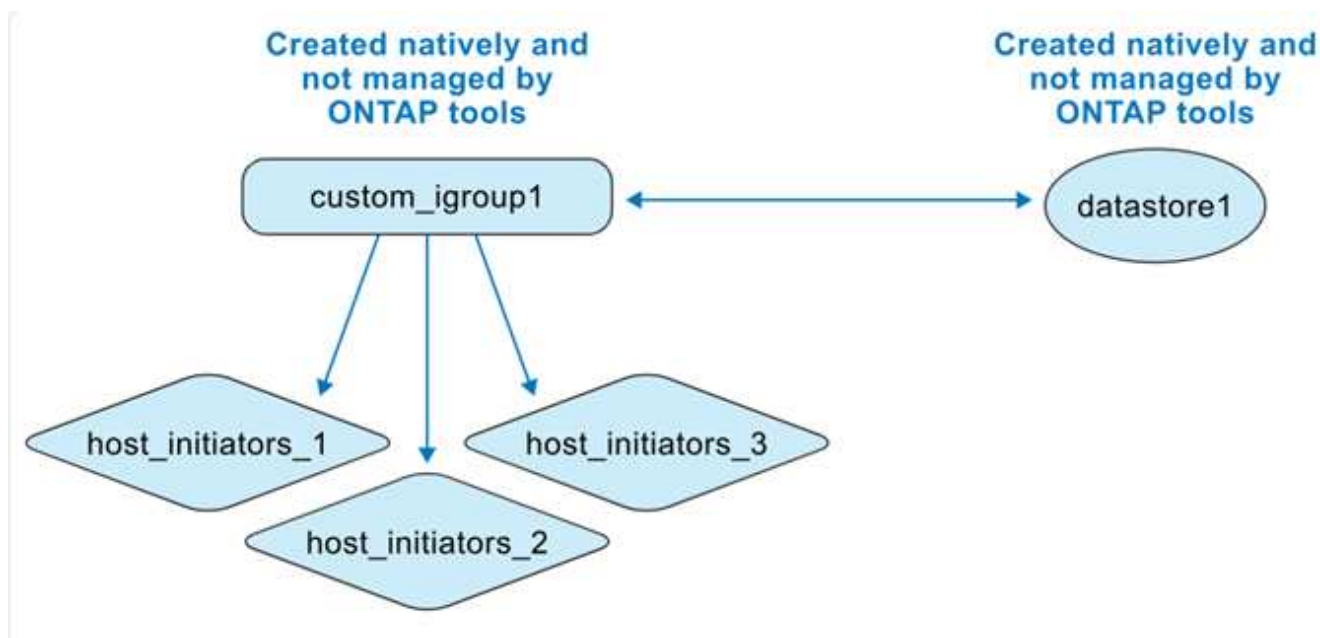
O mesmo comportamento é suportado pela API. Para reutilizar um igroup existente durante a criação do datastore, forneça o UUID do igroup na carga da solicitação da API.



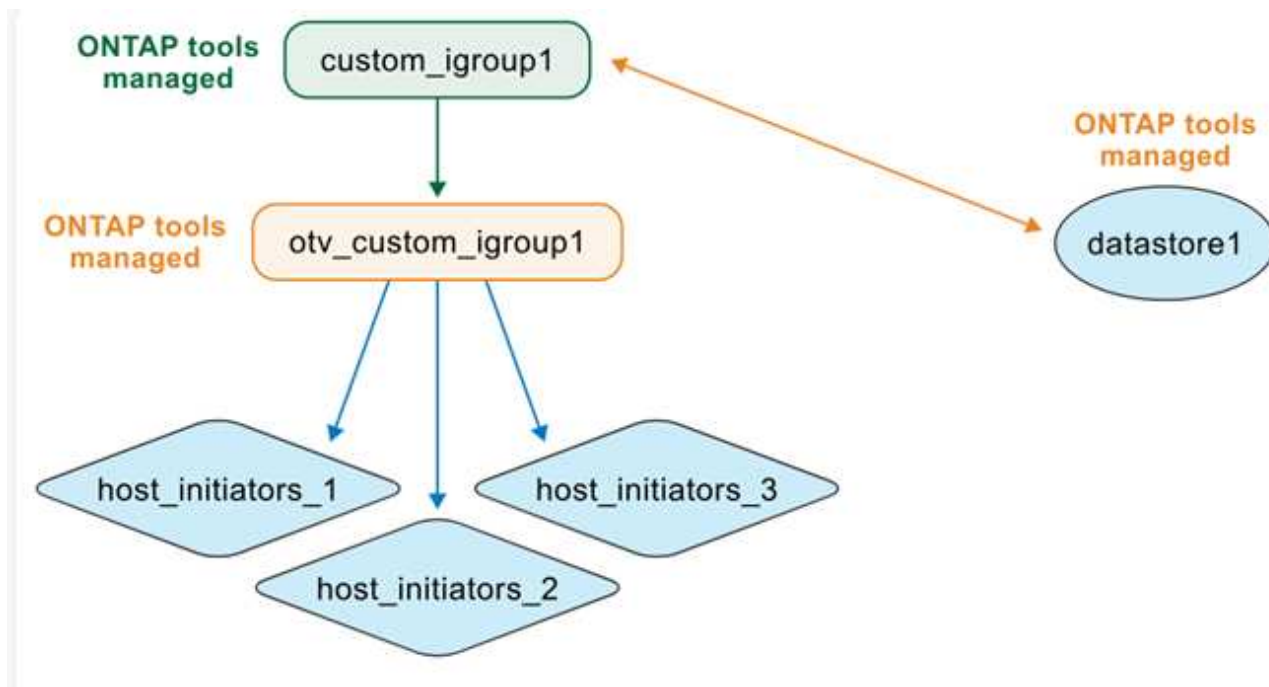
Somente igroups personalizados podem ser reutilizados. Igroups migrados do ONTAP tools 9.x não podem ser reutilizados e, a partir do ONTAP tools 10.5 P2, são excluídos automaticamente quando não estão mais em uso.

Visão de conversão de nativo para gerenciado

Se você criar o igroup e o datastore diretamente em sistemas ONTAP e ambientes VMware, ONTAP tools não gerencia esses objetos inicialmente. Isso resulta em uma estrutura de igroup plana.



Após a descoberta do datastore, ONTAP tools identifica e registra os igroups mapeados para o datastore e, em seguida, os representa em um modelo aninhado. O igroup pai é representado no nível do datastore, o igroup existente é renomeado com o `otv_` prefixo como um igroup filho, e os mapeamentos de iniciadores permanecem inalterados.



ONTAP tools for VMware vSphere não detecta nem gerencia igroups que são criados em sistemas ONTAP mas não estão mapeados para um datastore ou vinculados ao ONTAP tools. Durante a descoberta, ONTAP tools converte apenas os igroups que estão mapeados para datastores descobertos; outros igroups permanecem não gerenciados.

Reutilização de igroups nativos descobertos

Após as ferramentas ONTAP gerenciarem um igroup nativo descoberto, esse igroup ficará disponível na lista suspensão de nomes de grupos de iniciadores personalizados para a criação de datastore.

O novo LUN do datastore é mapeado para o igroup filho normalizado, por exemplo, `otv_NativeIgroup1`.

ONTAP tools for VMware vSphere não detecta nem utiliza igroups criados em sistemas ONTAP que não são gerenciados pelo ONTAP tools ou que não estão vinculados a um datastore.

Saiba mais sobre a interface de usuário do ONTAP tools Manager

ONTAP tools for VMware vSphere suporta alocação a vários clientes, permitindo o gerenciamento de várias instâncias do vCenter Server.

ONTAP tools Manager é um console baseado na Web para gerenciar ONTAP tools for VMware vSphere, vCenter Server instances, storage backends e configuração do appliance, como alta disponibilidade (HA) e escalonamento de nós.

ONTAP tools Manager oferece os seguintes recursos:

- Gerencie alertas - visualize e filtre alertas gerados pelas ONTAP tools for VMware vSphere.
- Gerencie os backends de armazenamento - Adicione e gerencie clusters de armazenamento ONTAP e mapeie-os para instâncias do vCenter Server globalmente.
- Gerencie instâncias do servidor vCenter - Adicione e gerencie instâncias do servidor vCenter dentro das

ONTAP tools.

- Monitorar tarefas - Monitore e depure tarefas assíncronas iniciadas tanto pela interface do plug-in ONTAP tools quanto pela interface do ONTAP tools Manager. Você pode filtrar as tarefas por período, ajustar o tamanho da página e visualizar detalhes da tarefa, incluindo erros e subtarefas. Clique no status de falha para visualizar os detalhes do erro. Para tarefas com subtarefas, expanda a linha para visualizar as descrições e os status. Para subtarefas, use a opção de detalhamento da tarefa para visualizar os detalhes.
- Baixe pacotes de logs - Colete arquivos de log para solucionar problemas com ONTAP tools for VMware vSphere.
- Gerencie certificados - Substitua o certificado autoassinado por um certificado de CA personalizado e renove ou atualize os certificados para o VASA Provider e ONTAP tools.
- Redefinir senhas - Alterar a senha do VASA Provider e do SRA.
- Gerencie as configurações do appliance - Configure o appliance ONTAP tools, incluindo a ativação de HA e o aumento do tamanho dos nós.

Para acessar o ONTAP tools Manager, inicie `https://<ONTAPtoolsIP>:8443/virtualization/ui/` no navegador e faça login com as credenciais de administrador do ONTAP tools for VMware vSphere que você forneceu durante a implantação.

The screenshot displays the ONTAP tools Manager interface. The top navigation bar includes the ONTAP tools Manager logo, a search icon, a refresh icon, and a user profile icon labeled 'admin'. The left sidebar contains a navigation menu with options: Overview, Alerts, Storage backends, vCenters, Jobs, Log bundles, Certificates, and Settings. The main content area is titled 'Overview' and includes an 'EDIT APPLIANCE SETTINGS' button. The 'Appliance' section shows a 'Healthy' status with a green checkmark and a table of settings: Size (Small), HA (Enabled), VASA Provider (Enabled), and SRA (Enabled). The 'Alerts' section shows 'No alerts' for the last 24 hours. The 'vCenters' section shows '1 Healthy' vCenter. The 'Storage backends' section shows 'No storage backends added'. The 'ONTAP tools nodes' section displays three nodes: vee-lab3-vm41, vee-lab3-vm184, and vee-lab3-vm187, all of which are 'Healthy' and have a 'Deploy_OVA_b29c029_998' deployment status.

Node Name	Status	Deployment
vee-lab3-vm41	Healthy	Deploy_OVA_b29c029_998
vee-lab3-vm184	Healthy	Deploy_OVA_b29c029_9982
vee-lab3-vm187	Healthy	Deploy_OVA_b29c029_9983

Cartão	Descrição
Cartão de appliance	O cartão Appliance exibe o status geral do appliance ONTAP tools, detalhes de configuração e o status dos serviços habilitados. Para visualizar mais informações, selecione o hiperlink Exibir detalhes . Se você alterar uma configuração do appliance, o cartão exibirá o status e os detalhes do job até que a alteração seja concluída.
Cartão de alertas	O cartão de Alertas exibe os alertas das ferramentas ONTAP categorizados por tipo, incluindo alertas de nível de nó HA. Você pode visualizar alertas detalhados clicando no hiperlink de contagem, que leva você à página de alertas filtrada pelo tipo de alerta selecionado.
cartão vCenters	O cartão vCenters exibe o status de integridade de todas as instâncias do vCenter Server gerenciadas pelas ONTAP tools. Você pode visualizar os detalhes de cada vCenter selecionando o link correspondente, que leva a uma página com mais informações sobre a instância selecionada.
Cartão de backends de storage	O cartão Storage backends exibe o status de integridade e conectividade de todos os clusters de armazenamento ONTAP configurados nas ONTAP tools. Você pode visualizar detalhes de cada storage backend selecionando o link correspondente, que leva a uma página com mais informações sobre o cluster selecionado.
Cartão de nós do ONTAP tools	O cartão de nós das ONTAP tools mostra todos os nós no appliance, incluindo nome do nó, nome da VM, status e informações de rede. Selecione Exibir detalhes para ver mais detalhes de um nó específico. [NOTA] Em uma configuração sem HA, apenas um único nó aparece. Em uma configuração com HA, três nós são exibidos.

Gerenciar configurações do ONTAP tools Manager

Editar configurações do AutoSupport das ferramentas ONTAP

Ao configurar ONTAP tools for VMware vSphere pela primeira vez, AutoSupport é ativado por padrão. Ele envia mensagens para suporte técnico 24 horas após ser ativado.

Desativar AutoSupport

Ao desativar AutoSupport, você deixará de receber suporte e monitoramento proativos.



Recomenda-se manter AutoSupport ativado, pois isso ajuda a acelerar a detecção e a resolução de problemas. Mesmo quando AutoSupport está desativado, o sistema continua coletando e armazenando informações localmente, mas não envia relatórios pela rede.

Passos

1. Inicie o ONTAP tools Manager a partir de um navegador da web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as credenciais de administrador das ONTAP tools for VMware vSphere que você forneceu durante a implantação.
3. Selecione a opção **Configurações > Telemetria > Editar**.
4. Desmarque a opção **AutoSupport** e salve as alterações.

Atualizar URL do proxy AutoSupport

Atualize a URL do proxy do AutoSupport para que o recurso AutoSupport encaminhe os dados através do servidor proxy para transmissão segura.

Passos

1. Inicie o ONTAP tools Manager a partir de um navegador da web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as credenciais de administrador das ONTAP tools for VMware vSphere que você forneceu durante a implantação.
3. Selecione **Configurações** na barra lateral.
4. Selecione a opção **Configurações > Telemetria > Editar**.
5. Insira um **Proxy URL** válido e salve as alterações.

Se você desativar AutoSupport, o URL do proxy também será desativado.

Adicionar servidores NTP às ferramentas ONTAP

Insira os detalhes do servidor NTP para sincronizar os relógios do tempo do appliance ONTAP tools.

Passos

1. Inicie o ONTAP tools Manager a partir de um navegador da web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as credenciais de administrador das ONTAP tools for VMware vSphere que você forneceu durante a implantação.
3. Selecione a opção **Configurações > Servidor NTP > Editar**.
4. Insira o domínio totalmente qualificado (FQDN), os endereços IPv4 ou IPv6, separados por vírgulas.

Atualize a tela para ver os valores atualizados.

Redefina as credenciais do VASA Provider e do SRA nas ONTAP tools

Se você esquecer suas credenciais do VASA Provider ou SRA, pode redefini-las para

uma nova senha usando a interface do ONTAP tools Manager. A nova senha deve ter entre 8 e 256 caracteres.

Passos

1. Inicie o ONTAP tools Manager a partir de um navegador da web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as credenciais de administrador das ONTAP tools for VMware vSphere que você forneceu durante a implantação.
3. Selecione a opção **Configurações > VASA Provider / SRA credentials > Redefinir senha**.
4. Digite a nova senha e confirme-a.
5. Selecione **Salvar** para aplicar as alterações.

Editar configurações de backup das ferramentas ONTAP

A partir do ONTAP tools for VMware vSphere 10.5, o recurso de backup está ativado por padrão e um backup é criado a cada 10 minutos. Você pode desativar o backup ou editar a frequência do backup.

Não desative o backup porque isso impede que as ONTAP tools mantenham um RPO baixo. Desativar o backup não exclui os arquivos de backup existentes. Você pode alterar a frequência do backup para um valor entre 10 e 60 minutos.

Passos

1. Inicie o ONTAP tools Manager a partir de um navegador da web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as credenciais de administrador das ONTAP tools for VMware vSphere que você forneceu durante a implantação.
3. Selecione a opção **Configurações > Backup > Editar**.
4. Na janela de edição, você pode desativar o backup ou editar a frequência do backup.

Habilitar os serviços do ONTAP tools

Você pode alterar a senha do administrador usando ONTAP tools Manager para habilitar serviços como VASA Provider, importação da configuração de vVols e recuperação de desastres (SRA) usando ONTAP tools Manager.

Passos

1. Inicie o ONTAP tools Manager a partir de um navegador da web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as credenciais de administrador das ONTAP tools for VMware vSphere que você forneceu durante a implantação.
3. Selecione **Editar configurações do aparelho** na seção de visão geral.
4. Na seção **Serviços**, você pode habilitar serviços opcionais como VASA Provider, importação de configuração de vVols e recuperação de desastres (SRA), conforme necessário.

Ao ativar os serviços pela primeira vez, você deve criar as credenciais do VASA Provider e do SRA. Essas

credenciais são usadas para registrar ou ativar os serviços do VASA Provider e do SRA no vCenter Server. O nome de usuário pode conter apenas letras, números e sublinhados. A senha deve ter entre 8 e 256 caracteres.



Antes de desativar quaisquer serviços opcionais, certifique-se de que os servidores vCenter gerenciados pelas ONTAP tools não os estejam utilizando.

A opção **Permitir importação da configuração de vVols** é exibida somente quando o serviço VASA Provider está ativado. Essa opção permite a migração de dados de vVols do ONTAP tools 9.xx para ONTAP tools 10.5.

Alterar as configurações do appliance ONTAP tools

Use o ONTAP tools Manager para expandir a configuração do ONTAP tools for VMware vSphere, seja aumentando o número de nós ou habilitando a High Availability (HA). Por padrão, o appliance ONTAP tools for VMware vSphere é implantado como uma configuração de nó único, sem HA.

Antes de começar

- Certifique-se de que seu modelo OVA tenha a mesma versão OVA que o Node 1. O Node 1 é o nó padrão onde o OVA do ONTAP tools for VMware vSphere é implantado inicialmente.
- Certifique-se de que o adicionar sem desligamento da CPU e o hot plug da memória estejam ativados.
- No vCenter Server, defina o nível de automação do Disaster Recovery Service (DRS) como parcialmente automatizado. Após implantar o HA, reverta para totalmente automatizado.
- Os nomes de host dos nós na configuração de alta disponibilidade devem estar em letras minúsculas.

Passos

1. Inicie o ONTAP tools Manager a partir de um navegador da web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as credenciais de administrador das ONTAP tools for VMware vSphere que você forneceu durante a implantação.
3. Selecione **Editar configurações do aparelho** na seção de visão geral.
4. Na seção **Configuração**, aumente o tamanho do nó e habilite a configuração de HA. Use as credenciais do vCenter Server para fazer alterações.

Na configuração de alta disponibilidade (HA), você pode alterar os detalhes da biblioteca de conteúdo. Forneça a senha para cada edição.



No ONTAP tools for VMware vSphere, você só pode aumentar o tamanho do nó; não é possível reduzir o tamanho do nó. Em uma configuração sem HA, apenas a configuração de tamanho médio é suportada. Em uma configuração com HA, as configurações de tamanho médio e grande são suportadas.

5. Use o botão de alternância HA para ativar a configuração de HA. Na página **Configurações de HA**, certifique-se de que:
 - A biblioteca de conteúdo pertence ao mesmo vCenter Server onde as máquinas virtuais dos nós das ONTAP tools são executadas. As credenciais do vCenter Server são usadas para validar e baixar o template OVA para alterações no appliance.

- A máquina virtual que hospeda o ONTAP tools não é implantada diretamente em um host ESXi. A VM deve ser implantada em um cluster ou em um pool de recursos.



Após a ativação da configuração de HA, você não pode reverter para uma configuração de nó único sem HA.

6. Na seção **Configurações de HA** da janela **Editar configurações do dispositivo**, você pode inserir os detalhes dos nós 2 e 3. ONTAP tools for VMware vSphere suporta três nós em uma configuração de HA.



As ONTAP tools preenchem automaticamente a maioria das opções de entrada com os detalhes de rede do Node 1 para simplificar o fluxo de trabalho. Você pode editar os dados de entrada antes de ir para a última página do assistente. Você pode inserir os detalhes de endereço IPv6 para os outros dois nodes somente quando o endereço IPv6 estiver habilitado no nó de gerenciamento das ONTAP tools.

Certifique-se de que cada host ESXi contenha apenas uma VM do ONTAP tools. As entradas são validadas sempre que você avança para a próxima janela.

7. Confira os detalhes na seção **Resumo** e **Salve** as alterações.

Qual é o próximo passo?

A página **Visão geral** mostra o status da implantação. Você também pode acompanhar o status do trabalho de edição das configurações do appliance na visualização de trabalhos, usando o ID do trabalho.

Se a implementação do HA falhar e o status do novo nó for "Novo", exclua a nova VM em vCenter antes de tentar ativar o HA novamente.

A aba **Alertas** no painel esquerdo lista os alertas para ONTAP tools for VMware vSphere.

Adicionar hosts VMware vSphere às ONTAP tools

Adicione novos hosts VMware vSphere às ONTAP tools for VMware vSphere para gerenciar e proteger os datastores nesses hosts.

Passos

1. Adicione um host ao seu cluster VMware vSphere seguindo o fluxo de trabalho na página: "[Como adicionar um host ESX ao seu cluster vSphere usando o fluxo de trabalho de início rápido](#)"
2. Após adicionar o host, vá ao menu principal do ONTAP tools e selecione **Descobrir** no painel de visão geral. Aguarde a conclusão do processo de descoberta. Como alternativa, você pode aguardar a conclusão da descoberta de host agendada.

Resultado

O novo host agora foi detectado e está sendo gerenciado pelo ONTAP tools for VMware vSphere. Você pode prosseguir para gerenciar o datastore no novo host.

Tópicos relacionados

- "[Montar um datastore vVols](#)" em novos hosts.
- "[Montar datastore NFS e VMFS](#)" em novos hosts.

Gerenciar datastores

Montar datastores NFS e VMFS nas ONTAP tools

A montagem de um datastore fornece acesso ao storage em hosts adicionais. Você pode montar o datastore nos hosts adicionais depois de adicioná-los ao seu ambiente VMware.



Ao adicionar um novo host ESXi usando o ["Adicionar um host ESX ao seu fluxo de trabalho de cluster vSphere"](#), aguarde a conclusão da descoberta agendada do host antes que ele apareça nas ONTAP tools. Como alternativa, você pode executar a descoberta manualmente na tela de visão geral do NetApp ONTAP tools.

Sobre esta tarefa

- Algumas ações do botão direito do mouse estão desativadas ou indisponíveis dependendo da versão do cliente vSphere e do tipo de datastore selecionado.
 - Se você estiver usando o cliente vSphere 8.0 ou versões posteriores, algumas das opções acessíveis pelo botão direito do mouse ficam ocultas.
 - Da versão vSphere 7.0U3 à vSphere 8.0, mesmo que as opções apareçam, a ação estará desativada.
- vSphere desativa a opção de montagem do datastore quando o cluster de hosts está protegido com configurações uniformes.

Passos

1. Na página inicial do vSphere Client, selecione **Hosts and Clusters**.
2. No painel de navegação à esquerda, selecione os data centers que contêm os hosts.
3. Para montar datastores NFS/VMFS em um host ou cluster de hosts, clique com o botão direito e selecione **NetApp ONTAP tools > Mount Datastores**.
4. Selecione os datastores que você deseja montar e selecione **Montar**.

Qual é o próximo passo?

Você pode acompanhar o progresso no painel de tarefas recentes.

Tópico relacionado

["Adicionar novos hosts VMware vSphere"](#)

Desmontar datastores NFS e VMFS nas ONTAP tools

A ação Desmontar armazenamento de dados remove um datastore NFS ou VMFS de hosts ESXi. Ela está disponível para datastores descobertos ou gerenciados por ONTAP tools for VMware vSphere.

Passos

1. Faça login no cliente vSphere.
2. Clique com o botão direito do mouse em um objeto de datastore NFS ou VMFS e selecione **Desmontar datastore**.

O vSphere client abre uma caixa de diálogo e lista os hosts ESXi que montam o datastore. Quando a

operação é realizada em um datastore protegido, uma mensagem de aviso é exibida na tela.

3. Selecione um ou mais hosts ESXi para desmontar o datastore.

Não é possível desmontar o datastore de todos os hosts. A interface de usuário sugere que você use a operação de excluir datastore.

4. Selecione o botão **Desmontar**.

Se o datastore fizer parte de um cluster de hosts protegido, uma mensagem de aviso será exibida.



Se o datastore protegido for desmontado, a configuração de proteção existente pode resultar em proteção parcial. Consulte ["Modificar cluster de hosts protegidos"](#) para ativar a proteção completa.

Qual é o próximo passo?

Você pode acompanhar o progresso no painel de tarefas recentes.

Montar um datastore vVols nas ONTAP tools

Você pode montar um datastore do VMware Virtual Volumes (vVols) em um ou mais hosts adicionais para fornecer acesso ao storage a hosts adicionais. Você pode desmontar o datastore vVols apenas por meio das APIs.



Ao adicionar um novo host ESXi usando o ["Adicionar um host ESX ao seu fluxo de trabalho de cluster vSphere"](#), aguarde a conclusão da descoberta agendada do host antes que ele apareça nas ONTAP tools. Como alternativa, você pode executar a descoberta manualmente na tela de visão geral do NetApp ONTAP tools.

Passos

1. Na página inicial do vSphere Client, selecione **Hosts and Clusters**.
2. No painel de navegação, selecione o data center que contém o datastore.
3. Clique com o botão direito do mouse no datastore e selecione **NetApp ONTAP tools > Montar datastore**.
4. Na caixa de diálogo **Montar datastores em hosts**, selecione os hosts nos quais você deseja montar o datastore e, em seguida, selecione **Montar**.

O painel de tarefas recentes exibe o progresso.

Tópico relacionado

["Adicionar novos hosts VMware vSphere"](#)

Redimensionar datastores NFS e VMFS nas ONTAP tools

Redimensionar um datastore permite que você aumente o storage para os arquivos da sua máquina virtual. Você pode alterar o tamanho de um datastore conforme as necessidades da sua infraestrutura mudam.

Sobre esta tarefa

Você pode aumentar o tamanho dos datastores NFS e VMFS. Um volume FlexVol nesses datastores não

pode ser reduzido abaixo do seu tamanho atual, mas pode crescer até 120%.

Passos

1. Na página inicial do vSphere Client, selecione **Hosts and Clusters**.
2. No painel de navegação, selecione o data center que contém o datastore.
3. Clique com o botão direito do mouse no datastore NFS ou VMFS e selecione **NetApp ONTAP tools > Redimensionar datastore**.
4. Na caixa de diálogo Redimensionar, insira um novo tamanho para o datastore e selecione **OK**.

Expandir vVols datastores nas ONTAP tools

Ao clicar com o botão direito do mouse no objeto datastore na visualização de objetos do vCenter, a seção do plug-in exibe as ações compatíveis para ONTAP tools for VMware vSphere. Ações específicas são habilitadas dependendo do tipo de datastore e dos privilégios do usuário atual.



A operação de expansão do datastore vVols não se aplica a datastores vVols baseados em sistema ASA r2.

Passos

1. Na página inicial do vSphere Client, selecione **Hosts and Clusters**.
2. No painel de navegação, selecione o data center que contém o datastore.
3. Clique com o botão direito do mouse no datastore e selecione **NetApp ONTAP tools > Adicionar storage ao datastore**.
4. Na janela **Criar ou Selecionar Volumes**, você pode criar novos volumes ou escolher entre os volumes existentes. Siga as instruções na tela para fazer sua seleção.
5. Na janela **Resumo**, revise as seleções e selecione **Expandir**. Você pode acompanhar o progresso no painel de tarefas recentes.

Reduzir um datastore vVols nas ONTAP tools

Esta página explica como remover volumes de um vVols datastore.

Utilize a ação "remover storage do datastore" em qualquer datastore vVols gerenciado pelas ONTAP tools no vCenter Server.

Você não pode remover storage de um volume se ele contiver vVols; a opção de remoção será desativada para esses volumes. Ao remover volumes do datastore, você também tem a opção de excluir os volumes selecionados do storage ONTAP.



A operação de redução do datastore vVols não é suportada para datastores vVols baseados em sistemas ASA r2.

Passos

1. Na página inicial do vSphere Client, selecione **Hosts and Clusters**.
2. No painel de navegação, selecione o data center que contém o datastore.
3. Clique com o botão direito do mouse no datastore vVol e selecione **NetApp ONTAP tools > Remover**

storage do datastore.

4. Selecione os volumes que não possuem vVols e selecione **Remover**.



A opção para selecionar o volume em que vVols está instalado está desativada.

5. Na janela pop-up **Remover armazenamento**, selecione a caixa de seleção **Excluir volumes do cluster ONTAP** para excluir os volumes do datastore e do storage ONTAP e selecione **Excluir**.

Excluir datastores nas ONTAP tools

Esta página descreve como excluir datastores NFS, VMFS ou vVols usando ONTAP tools no vCenter Server.

Ao excluir um datastore, as seguintes ações são executadas dependendo do tipo de datastore:

- O vVol container está desmontado.
- Se o igroup não estiver em uso, seus iniciadores serão removidos do igroup.
- O vVol container foi excluído.
- Os volumes FlexVol permanecem no array de storage.

Você só pode excluir o datastore se não houver vVols presentes no datastore selecionado.

Passos

1. Faça login no cliente vSphere.
2. Clique com o botão direito do mouse em um sistema host, um cluster host ou um data center e selecione **NetApp ONTAP tools > Delete datastore**.



Não é possível excluir um datastore usado por máquinas virtuais. Mova as máquinas virtuais para outro datastore antes de excluir. Não é possível excluir o volume se ele fizer parte de um cluster de hosts protegido.

- a. No caso de um datastore NFS ou VMFS, uma caixa de diálogo é exibida com a lista de máquinas virtuais que utilizam o datastore.
 - b. Se nenhuma máquina virtual estiver associada a um datastore VMFS, você verá uma caixa de diálogo de confirmação. Se a proteção de cluster do host estiver habilitada e existir um relacionamento AFD, você pode limpar os elementos de storage secundário.
 - c. Para datastores VMFS protegidos em sistemas ASA r2, remova a proteção antes de excluí-los. A partir do ONTAP 9.17.1 e ONTAP tools for VMware vSphere 10.5, você pode excluir um datastore protegido. Se for o único datastore no grupo de proteção, a proteção do cluster de hosts é removida automaticamente.
 - d. Para datastores vVols, você só pode excluir o datastore se não houver vVols presentes. A caixa de diálogo **Excluir datastore** inclui uma opção para remover volumes do cluster ONTAP.
 - e. Para datastores vVols em sistemas ASA r2, você não pode excluir os volumes de suporte do ONTAP usando a opção **Excluir datastore**.
3. Para excluir os volumes de suporte no storage ONTAP, selecione **Excluir volumes no ONTAP cluster**.



Para datastores VMFS em storage ONTAP unificado que fazem parte de um cluster de hosts protegido, você não pode excluir o volume do cluster ONTAP.

Ao excluir um datastore NFS, VMFS ou vVols, os igroups pai permanecem no sistema ONTAP. Os igroups filho que não estão mapeados para nenhum LUN são excluídos automaticamente. As ONTAP tools realizam uma limpeza diária para remover os igroups pai padrão não mapeados. Exclua manualmente os igroups pai personalizados no ONTAP. As ONTAP tools não podem reutilizar igroups pai obsoletos.

Visualizações de armazenamento ONTAP para datastores em ONTAP tools

ONTAP tools for VMware vSphere exibe a visão do lado do storage ONTAP dos datastores e seus volumes na guia configurar.

Passos

1. No cliente vSphere, vá para o datastore.
2. Selecione a guia **Configurar** no painel direito.
3. Selecione **NetApp ONTAP tools > ONTAP Storage**. A visualização muda de acordo com o tipo de datastore. Veja a tabela abaixo:

Tipo de datastore	Informações disponíveis
Datastore NFS	A página Detalhes do armazenamento contém backends de storage, informações sobre agregados e volumes. A página Detalhes do NFS contém dados relacionados ao datastore NFS.
Datastores VMFS	A página Detalhes do armazenamento contém informações sobre o backend de armazenamento, o agregado, o volume e a zona de disponibilidade de storage (SAZ). A página Detalhes da unidade de armazenamento contém detalhes da unidade de armazenamento.
datastores vVols	Lista todos os volumes. Você pode expandir ou remover storage no painel de storage do ONTAP. ONTAP tools não oferecem suporte a essa visualização para datastores vVols baseados em sistema ASA r2.

Visualização do armazenamento da máquina virtual nas ferramentas ONTAP

A visualização de armazenamento mostra a lista de vVols que a máquina virtual cria.



Esta visualização se aplica a VMs com pelo menos um disco de um datastore vVols gerenciado pelo ONTAP tools for VMware vSphere.

Passos

1. No vSphere Client, acesse a máquina virtual.
2. Selecione a guia **Monitor** no painel direito.
3. Selecione **NetApp ONTAP tools > Storage**. Os detalhes de **Storage** aparecem no painel direito. Você pode ver a lista de vVols que estão presentes na máquina virtual.

Você pode usar a opção "Gerenciar colunas" para ocultar ou exibir diferentes colunas.

Gerencie os limites de armazenamento nas ONTAP tools

Você pode definir o limite para receber notificações no vCenter Server quando o volume e a capacidade agregada atingirem determinados níveis.

Etapas:

1. Faça login no cliente vSphere.
2. Na página de atalhos, selecione **NetApp ONTAP tools** na seção de plug-ins.
3. No painel esquerdo das ONTAP tools, vá para **Configurações > Configurações de Limiar > Editar**.
4. Na janela **Editar Limite**, insira os valores desejados nos campos **Quase Cheio** e **Cheio** e selecione **Salvar**. Você pode restaurar os valores de limite para os padrões recomendados: 80 para Quase Cheio e 90 para Cheio.

Gerencie back-ends de armazenamento nas ONTAP tools

Os backends de armazenamento são sistemas que os hosts ESXi usam para storage.

Descubra o storage

Você pode executar a descoberta de um backend de storage sob demanda, sem precisar esperar que uma descoberta agendada atualize os detalhes do storage imediatamente. Para configurações MetroCluster, execute a descoberta das ONTAP tools manualmente após um switchover.

Siga os passos abaixo para descobrir os storage backends.

Passos

1. Faça login no cliente vSphere.
2. Na página de atalhos, selecione **NetApp ONTAP tools** na seção de plug-ins.
3. No painel esquerdo das ONTAP tools, acesse **Storage Backends** e selecione um storage backend.
4. Selecione o menu de reticências verticais e selecione **Discover storage**

Você pode acompanhar o progresso no painel de tarefas recentes.

Modificar os storage backends

Você pode modificar as credenciais do backend de armazenamento ou o nome da porta. Você também pode modificar o backend de armazenamento para clusters ONTAP globais usando o ONTAP tools Manager. Se o certificado expirar em 30 dias ou menos, o ONTAP tools exibirá um aviso. Modifique o backend de armazenamento e faça upload do novo certificado a partir do administrador do ONTAP.

Ao modificar o backend de armazenamento, ONTAP tools for VMware vSphere realiza uma descoberta do backend de armazenamento para atualizar os detalhes do armazenamento.

Siga os passos desta seção para modificar um backend de storage.

1. Faça login no cliente vSphere.
2. Na página de atalhos, selecione **NetApp ONTAP tools** na seção de plug-ins.
3. No painel esquerdo das ONTAP tools, acesse **Storage Backends** e selecione um storage backend.

4. Selecione o menu de reticências verticais e selecione **Modificar** para modificar as credenciais ou o nome da porta. Você pode acompanhar o progresso no painel de tarefas recentes.

Modifique os clusters ONTAP globais com o ONTAP tools Manager da seguinte forma.

1. Inicie o ONTAP tools Manager a partir de um navegador da web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as credenciais de administrador das ONTAP tools for VMware vSphere que você forneceu durante a implantação.
3. Selecione os storage backends na barra lateral.
4. Selecione o backend de armazenamento que você deseja modificar.
5. Selecione o menu de reticências verticais e selecione **Modificar**.
6. Você pode modificar as credenciais ou a porta. Insira o **Nome de usuário** e a **Senha** para modificar o backend de armazenamento.

Remover backends de storage

Você deve remover todos os armazenamentos de dados associados ao backend de armazenamento antes de removê-lo. Siga os passos abaixo para remover um backend de armazenamento.

1. Faça login no cliente vSphere.
2. Na página de atalhos, selecione **NetApp ONTAP tools** na seção de plug-ins.
3. No painel esquerdo das ONTAP tools, acesse **Storage Backends** e selecione um storage backend.
4. Selecione o menu de reticências verticais e selecione **Remover**. Certifique-se de que o storage backend não contenha nenhum datastore. Você pode acompanhar o progresso no painel de tarefas recentes.

Você pode remover clusters ONTAP globais usando ONTAP tools Manager.

1. Inicie o ONTAP tools Manager a partir de um navegador da web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as credenciais de administrador das ONTAP tools for VMware vSphere que você forneceu durante a implantação.
3. Selecione **Storage Backends** na barra lateral.
4. Selecione o backend de armazenamento que você deseja remover
5. Selecione o menu de reticências verticais e selecione **Remover**.

Visão detalhada do storage backend

A página de backend de armazenamento lista todos os backends de armazenamento. Você pode realizar as operações de descobrir storage, modificar e remover nos backends de armazenamento que você adicionou, mas não nas SVMs filhas individuais do cluster.

Selecione o cluster pai ou filho para visualizar o resumo dos componentes. Para o cluster pai, use o menu suspenso de ações para descobrir storage, modificar ou remover o backend de storage.

A página de resumo fornece os seguintes detalhes:

- Status do backend de armazenamento

- Informações sobre capacidade
- Informações básicas sobre a VM
- Detalhes do certificado, como o status do certificado e a data de validade.
- Informações de rede, como o endereço IP e a porta da rede. Para a SVM filha, as informações são as mesmas do storage backend pai.
- Privileges permitidos e restritos para o backend de armazenamento. Para o SVM filho, as informações são as mesmas do backend de armazenamento pai. ONTAP tools exibe privilégios apenas em backends de armazenamento baseados em cluster. Se você adicionar SVM como backend de armazenamento, as informações de privilégios não serão exibidas.
- A visualização detalhada do cluster do sistema ASA r2 não inclui a guia de camadas locais quando a propriedade desagregada está definida como "true" para o SVM ou o cluster.
- Para sistemas ASA r2 SVM, o portlet de capacidade não é exibido. O portal de capacidade é necessário apenas quando a propriedade desagregada está definida como "true" para o SVM ou o cluster.
- Para sistemas ASA r2 SVM, a seção de informações básicas mostra o tipo de plataforma.

A guia de interface fornece informações detalhadas sobre a interface.

A aba de níveis locais fornece informações detalhadas sobre a lista de agregados.

Gerencie instâncias do servidor vCenter nas ONTAP tools

Instâncias do vCenter Server são plataformas de gerenciamento central que permitem que você controle hosts, máquinas virtuais e backends de storage.

Desassocie os backends de armazenamento da instância do servidor vCenter

A página de listagem do servidor vCenter mostra o número de backends de armazenamento associados. Cada instância do servidor vCenter tem a opção de se associar ou desassociar de um backend de armazenamento.

Passos

1. Inicie o ONTAP tools Manager a partir de um navegador da web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as credenciais de administrador das ONTAP tools for VMware vSphere que você forneceu durante a implantação.
3. Selecione a instância de servidor vCenter desejada na barra lateral.
4. Selecione as elipses verticais ao lado do vCenter Server que você deseja associar ou desassociar dos storage backends.
5. Selecione **Desassociar storage backend**.

Modificar uma instância do servidor vCenter

Siga os passos abaixo para modificar uma instância do servidor vCenter.

1. Inicie o ONTAP tools Manager a partir de um navegador da web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as credenciais de administrador das ONTAP tools for VMware vSphere que você forneceu

durante a implantação.

3. Selecione a instância de servidor vCenter aplicável na barra lateral
4. Selecione as reticências verticais ao lado do vCenter Server que você deseja modificar e selecione **Modificar**.
5. Na janela **Modificar vCenter**, insira o nome de usuário, a senha e os detalhes da porta.
6. Faça o upload do certificado e selecione **Modificar**.

Remover uma instância do servidor vCenter

Remova todos os storage backends do vCenter Server antes de removê-lo.

1. Inicie o ONTAP tools Manager a partir de um navegador da web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as credenciais de administrador das ONTAP tools for VMware vSphere que você forneceu durante a implantação.
3. Selecione as instâncias de vCenter Server aplicáveis na barra lateral
4. Selecione as reticências verticais ao lado do vCenter Server que você deseja remover e selecione **Remover**.



Após remover as instâncias do servidor vCenter, elas não serão mais mantidas pelo aplicativo.

Ao remover instâncias do servidor vCenter nas ONTAP tools, as seguintes ações são executadas automaticamente:

- O plug-in não está registrado.
- Os privilégios de plug-in e as funções de plug-in são removidos.

Renovar certificado do servidor vCenter

ONTAP tools notifica você quando o certificado do vCenter está perto de expirar ou já expirou. Após renovar o certificado do vCenter, faça o upload do novo certificado para o ONTAP tools usando as etapas a seguir:

1. Faça login no shell de diagnóstico remoto das ONTAP tools.
2. Obtenha o certificado renovado do vCenter no shell de diagnóstico:

```
echo | openssl s_client connect <vcenter>:443 2>&1 | sed -n '/-BEGIN
CERTIFICATE/,/END CERTIFICATE/p'
```

3. Certifique-se de que o certificado esteja no formato ASCII Base 64 e inclua as linhas inicial e final, por exemplo:


```

---{}BEGIN CERTIFICATE{}---
MIIFUzCCA7ugAwIBAgIJANOGlapcl5oSMA0GCSqGSIb3DQEBCwUAMIGJMQwwCgYD
VQDDAN2YzExFDASBgoJkiaJk/IsZAEZFgRkZW1vMRUwEwYKCZImiZPyLQBGRYF
bG9jYVWwxCzAJBgNVBAYTA1VTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRwwGgYDVQQK
DBN2YzEuZGVtby5uZXRhcHAuY29tMQwwCgYDVQQLDANMT0QwHhcNMjQwNDA1MTgw
NTE4WhcNMjYwNDA1MTgwNTE4WjBzMRwwGgYDVQQDDBN2YzEuZGVtby5uZXRhcHAu
Y29tMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcn5pYTESMBAGA1UEBwwJ
UGFsbyBBbHRvMQ8wDQYDVQQKDAZOZXRhbnRvMRwwGgYDVQQDAzA2ZGVIC/OTw/7xucvPVuM+b8
DhzvNpQ2phjfr6ctEhbntPpqPdu+t2CKK7l0mzg3D9cJ/rvMvdDDXr0tgaDloi2u
ZDW0CaF0QhLopNfRXMoogBZ66csEhViAy3CHTcOse770mA/PyoHgrCPZngVLZiIQ
TIWpdQMbEEzFIkrLfc70UW2MzfublrsH7Dn/kOu/iCSlVJWixKf7SmZtVQ5ZxBTD
UlJSiqoXleRXGyunArEvrIpOY9kkKXUElm3hGnk/ZmiuBJ+HqUYqYW+H+7vE3lKa
6NEqDX+tZotxTx2bXMjeiIWU30ZbshgeXlIG9qc49clBoC9iGjavhctOcaXg/W3h
dLKK5ds3rpRERgMg6VMkrfiqAJuiq+b3sTvXMAul/3hL7hz5QABAE/hP4ZvIHV02
WWDQRLiuVFAcDAyvCrO9Irx0GklRyRShKYakdWxZ3hhMdLuGq0yvRXqolIb94zwO
JfBJHjFTOA/GqwromZgiTzJkKq5xbN8MFwIDAQABo4HSMIHPMAsGA1UdDwQEAwIF
4DA7BgNVHREENDAYgRVlbWFpbEBkZW1vLm5ldGFwcC5jb22HBMC0AB+CE3ZjMS5k
ZW1vLm5ldGFwcC5jb20wHQYDVRO0BBYEFJ0V0zY+JRpFrEt3lovAY4BLFXmAMB8G
A1UdIwQYMBAAAFENf6fRxWF3OJQNTPIdUpK6kjA78MEMGCCsGAQUFBwEBBDcwNTAz
BggrBgEFBQcwAoYnaHR0cHM6Ly92YzEuZGVtby5uZXRhcHAuY29tL2FmZC92ZWZl
L2NhMA0GCSqGSIb3DQEBCwUAA4IBgQBaDfK7GBM4vmhzYCqGrr6KB+h3qeTJ+Y0Y
5nIPRP1HucawDQ8QTay605ddJ8gFGoxkOQDn9tdXWXGjnTRFOT8R+Hw/nUfVSiDP
sYienbl6copzUNwtqh+m9Ifow74Gf+ulRzEC0EAV01X/nTEYH6NKM6Wy7y7F8g5J
lrpM3JY90ZChMqHO3Av/88rbErfQ/gU1brJ3u9Gks4e20Z7Ff312ZKhWRuJDln2Z
0tc/gp90N9GxaVvELovq/pdjaZ8xiXCxa6piicrJd9WnqMHlgmXP2PIBDxMDBWBG
gwsfs5H7VG9MJYks6lViNsGclo0EwEdF0MfoB3JtsWpPWq6+jBua0Jm7/aFCU+Ht
mykr0gaV7muegoiBQuDma4EkAI3lD7ZlUgJQaw157NTk4RW3TFcbtViBHJkM54Hr
iVm0cl+2BZni/QTMh/MkWV2dYXJ3NuNlqqfzFY+bUfkzkR4SneMk0HX3joNNYDJv
siO7bL+k/Pxql27NVIhuCoVJAAlCI7ak=
---{}END CERTIFICATE{}---

```

4. Copie o resultado e salve-o como um arquivo de texto com a .pem extensão na sua desktop.
5. Inicie o ONTAP tools Manager a partir de um navegador da web:
<https://<ONTAPtoolsIP>:8443/virtualization/ui/>
6. Faça login com as credenciais de administrador das ONTAP tools for VMware vSphere que você forneceu durante a implantação.
7. Selecione a instância de servidor vCenter aplicável na barra lateral
8. Selecione as reticências verticais ao lado do vCenter Server que você deseja modificar e selecione **Modificar**.
9. Na janela **Modificar vCenter**, insira o nome de usuário, a senha e os detalhes da porta.
10. Faça o upload do certificado e selecione **Modificar**.

Informações relacionadas

Gerenciar certificados das ferramentas ONTAP

Um certificado autoassinado é gerado para as ferramentas ONTAP e o VASA Provider por padrão durante a implantação. Você pode usar a interface do ONTAP tools Manager para renovar esse certificado ou substituí-lo por um certificado de CA personalizado. Em implantações com vários vCenter, o uso de certificados de CA personalizados é obrigatório.

Antes de começar

Você deve ter o seguinte antes de começar:

- O nome de domínio mapeado para o endereço IP virtual.
- Consulta nslookup bem-sucedida do nome de domínio, confirmando que ele resolve para o endereço IP correto.
- Certificados criados com o nome de domínio e o endereço IP das ONTAP tools.



O endereço IP do ONTAP tools deve ser mapeado para um nome de domínio totalmente qualificado (FQDN). Os certificados devem conter o mesmo FQDN mapeado para o endereço IP do ONTAP tools no campo de assunto ou nos nomes alternativos de assunto.



Não é possível trocar de um certificado assinado por uma CA para um certificado autoassinado.

Atualizar certificado do ONTAP tools

A aba ONTAP tools exibe detalhes como o tipo de certificado (autoassinado/assinado por CA) e nome de domínio. Durante a implantação, um certificado autoassinado é gerado por padrão. Você pode renovar o certificado ou atualizá-lo para um certificado de CA.

Passos

1. Inicie o ONTAP tools Manager a partir de um navegador da web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as credenciais de administrador das ONTAP tools for VMware vSphere que você forneceu durante a implantação.
3. Selecione **Certificates > ONTAP tools > Renew** para renovar os certificados.

Você pode renovar o certificado se ele tiver expirado ou estiver próximo da data de expiração. A opção de renovação está disponível quando o tipo de certificado é CA-signed. Na janela pop-up, forneça os detalhes do certificado do servidor, da chave privada, da root CA e do certificado intermediário.



O sistema ficará offline até que o certificado seja renovado e você será desconectado da interface do ONTAP tools Manager.

4. Para atualizar o certificado autoassinado para um certificado de CA personalizado, selecione **Certificates > ONTAP tools > opção Upgrade to CA**.
 - a. Na janela pop-up, faça o upload do certificado do servidor, da chave privada do certificado do servidor, do certificado da autoridade certificadora raiz e dos arquivos de certificado intermediário.
 - b. Insira o FQDN do endereço IP do balanceador de carga para o qual você gerou este certificado e atualize o certificado.



O sistema ficará offline até que a atualização seja concluída e você será desconectado da interface do ONTAP tools Manager.

Atualizar certificado do VASA Provider

ONTAP tools for VMware vSphere é implantado com um certificado autoassinado para o VASA Provider. Com isso, apenas uma instância do servidor vCenter pode ser gerenciada para datastores vVols. Quando você gerencia várias instâncias do servidor vCenter e deseja habilitar o recurso vVols nelas, é necessário alterar o certificado autoassinado para um certificado CA personalizado.

Passos

1. Inicie o ONTAP tools Manager a partir de um navegador da web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as credenciais de administrador das ONTAP tools for VMware vSphere que você forneceu durante a implantação.
3. Selecione **Certificados > VASA Provider** ou **ONTAP tools > Renovar** para renovar os certificados.
4. Selecione **Certificados > VASA Provider** ou **ONTAP tools > Atualizar para CA** para atualizar o certificado autoassinado para um certificado de CA personalizado.
 - a. Na janela pop-up, faça o upload do certificado do servidor, da chave privada do certificado do servidor, do certificado da autoridade certificadora raiz e dos arquivos de certificado intermediário.
 - b. Insira o FQDN do endereço IP do balanceador de carga para o qual você gerou este certificado e

atualize o certificado.



O sistema ficará offline até que a atualização seja concluída e você será desconectado da interface do ONTAP tools Manager.

Acesse o console de manutenção do ONTAP tools for VMware vSphere

Saiba mais sobre o console de manutenção das ONTAP tools

O console de manutenção para ONTAP tools for VMware vSphere permite que você gerencie configurações de aplicativo, sistema e rede. Você pode atualizar senhas de administrador e de manutenção, gerar pacotes de suporte, configurar níveis de log, gerenciar configurações de TLS e habilitar diagnósticos remotos.

Após implantar ONTAP tools for VMware vSphere, se o console de manutenção não estiver acessível, instale o VMware tools a partir do vCenter Server. Faça login usando o `maint` nome de usuário e a senha definidos durante a implantação. Use o `nano` para editar arquivos no console de manutenção ou no console de login root.



Você deve definir uma senha para o usuário `diag` ao ativar o diagnóstico remoto.

Você deve usar a guia **Resumo** das suas ONTAP tools for VMware vSphere implantadas para acessar o console de manutenção. Ao selecionar , o console de manutenção é iniciado.

Menu do Console	Opções
Configuração do aplicativo	1. Exibir resumo do status do servidor 2. Alterar o nível de LOG para os serviços do ONTAP tools 3. Alterar sinalizador de validação de certificado
Configuração do sistema	1. Reiniciar máquina virtual 2. Desligar máquina virtual 3. Alterar a senha do usuário 'maint' 4. Alterar fuso horário 5. Aumentar o tamanho do disco da jail (/jail) 6. Atualizar 7. Instalar o VMware Tools

Configuração de rede	1. Exibir configurações de endereço IP 2. Exibir configurações de pesquisa de nome de domínio 3. Alterar configurações de pesquisa de nome de domínio 4. Exibir rotas estáticas 5. Alterar rotas estáticas 6. Confirmar alterações 7. Ping em um host 8. Restaurar configurações padrão
Suporte e diagnóstico	1. Acesse o shell de diagnóstico 2. Habilitar acesso remoto para diagnóstico 3. Forneça as credenciais do vCenter para backup 4. Faça backup

Configure o acesso remoto para diagnóstico das ONTAP tools

Você pode configurar ONTAP tools for VMware vSphere para habilitar o acesso SSH para o usuário diag.

Antes de começar

Ative a extensão VASA Provider para sua instância do servidor vCenter.

Sobre esta tarefa

O uso de SSH para acessar a conta de usuário diag apresenta as seguintes limitações:

- Você só tem permissão para uma conta de login por ativação de SSH.
- O acesso SSH à conta de usuário diag é desativado quando ocorre uma das seguintes situações:
 - O tempo expirou.

A sessão de login expira à meia-noite do dia seguinte.

- Você faz login novamente como usuário diag usando SSH.

Passos

1. No vCenter Server, abra um console para o VASA Provider.
2. Faça login como usuário de manutenção.
3. Digite 4 para selecionar **Suporte e Diagnóstico**.
4. Digite 2 para selecionar **Ativar acesso remoto ao diagnóstico**.
5. Digite y na caixa de diálogo de Confirmação para ativar o acesso remoto para diagnóstico.
6. Digite uma senha para acesso remoto ao diagnóstico.

Inicie o SSH em outros nós do ONTAP tools

Você precisa iniciar o SSH em outros nós antes de atualizar.

Antes de começar

Ative a extensão VASA Provider para sua instância do servidor vCenter.

Sobre esta tarefa

Repita este procedimento em cada nó antes de atualizar.

Passos

1. No vCenter Server, abra um console para o VASA Provider.
2. Faça login como usuário de manutenção.
3. Pressione Enter 4 para selecionar Suporte e Diagnóstico.
4. Pressione Enter 1 para selecionar acessar o shell de diagnóstico.
5. Digite `y` para prosseguir.
6. Execute o comando `sudo systemctl restart ssh`.

Atualizar as credenciais do servidor vCenter nas ONTAP tools

Você pode atualizar as credenciais da instância do servidor vCenter usando o console de manutenção.

Antes de começar

Você precisa ter as credenciais de login do usuário de manutenção.

Sobre esta tarefa

Se você alterou as credenciais do vCenter Server após a implantação, atualize-as usando este procedimento.

Passos

1. No vCenter Server, abra um console para o VASA Provider.
2. Faça login como usuário de manutenção.
3. Pressione Enter 2 para selecionar o Menu de Configuração do Sistema.
4. Insira 8 para alterar as credenciais do vCenter.

Alterar o indicador de validação do certificado nas ONTAP tools

Por padrão, o sinalizador de validação de certificado está habilitado (definido como true). Você pode definir o sinalizador de validação de certificado do backend de armazenamento ONTAP como false se precisar ignorar as verificações de certificado SAN. Essa configuração não se aplica a certificados do vCenter Server.

Antes de começar

Você precisa ter as credenciais de login do usuário de manutenção.

Passos

1. No vCenter Server, abra um console para ONTAP tools.
2. Faça login como usuário de manutenção.
3. Pressione 1 Enter para selecionar o menu **Configuração do Aplicativo**.
4. Digite 3 para alterar o sinalizador de validação do certificado.

O console de manutenção exibe o status do sinalizador de validação do certificado e solicita que você o altere.

5. Digite 'y' para alternar a sinalização ou 'n' para cancelar.

Ao habilitar a opção de validação de certificado (definida como true), ONTAP tools verifica se todos os backends de storage utilizam certificados com um Subject Alternative Name (SAN). Se algum backend utilizar um certificado sem um SAN, você não poderá habilitar a validação de certificado. Antes de habilitar essa opção, verifique se todos os backends de storage utilizam certificados baseados em SAN. Se você desabilitar a opção de validação de certificado (definida como false), ONTAP tools ignora a validação de certificado para todos os backends de storage configurados.

Verifique certificados baseados em SAN para backends de armazenamento

Para garantir uma comunicação segura e a validação adequada, verifique se todos os storage backends utilizam certificados baseados em SAN:

1. Verifique se o certificado de gerenciamento do ONTAP inclui uma entrada de Nome Alternativo do Assunto (SAN).
2. Confirme se as entradas SAN correspondem ao endereço IP de gerenciamento do ONTAP ou ao nome DNS, ou a ambos.
3. Certifique-se de que os detalhes usados para integrar o ONTAP correspondam ao endereço IP ou nome DNS na entrada SAN do certificado.

Seguir esses passos ajuda a evitar problemas de validação de certificados e garante que o sistema ONTAP esteja integrado de forma segura.

O seguinte certificado de exemplo mostra as informações decodificadas:

```
HG8u6GK r2JJonWe/kjoKTUnkjwW7feDI747RUuFrthcvTDqhBNWL76jihNp1VX7
v0SDWMaVdecTeU1X/1X3qMxiL+tU4p9SbKVpQw6hjM/zi0LNC784EYIOSQ7qVob
6f21mfPOJHbqs5fLim9NFFUu2DQIDAQA8oQw0jBABgNVHREEEOT43hwShsSHdKXsgi9z
dGkyMjAtdnNpbS1zcjA1MWUtY2OuY2Rs LmdkbC5lbmdsYWJuZKThcPHauY29nt
BgkqhkiG9wQBAQsFAAOCQAEEagptz11RN7PLuJUo-SSQExBsF5/3JHr0+sSIMZDzm
4P24kbxQZbfryy68itKGF4LeAid0hgyxc3y9iv4zKlx85fLNgiTnVqAe8'KYNoYD6
IEWppDUE0eVNZIZQjrz9QjUAAF9ifjq8+SKr'lphoXnYYUiM6utvobPMG8cR8Gca
jiLibiMM01K6rD7Ng+7+ydUCAwBQwMDDwdn8+7RIRdKgwqX9QDLegcC5IL5WFLwbMc
2GBv8VM839m0KUAKXSDGwJBZ5nSHQdNi7MU3AES7Nzkv63kGEQJT/5Wr1DmOwlf
os14qeeeMRigrAbFL6EHMsOMSP0521rtTrJrjBooB22r0tyDA--
-----END CERTIFICATE-----
```

Certificate Information:

- ✓ Common Name: **test.xyz.com**
- ✓ Subject Alternative Names: IP Address: **xxx.xx.xxx.xxx**, **test.xyz.com**
- ✓ Organization: Self-signed-certificate
- ✓ Organization Unit:
- ✓ Locality: N/A
- ✓ State: N/A
- ✓ Country: XX
- ✓ Valid From: March 8, 2026
- ✓ Valid To: March 7, 2028
- ✓ Issuer: **test.xyz.com**, Self-signed-certificate
- ✓ Serial Number: 640c2752bd2c972c5775180070cfdd2120809ee

Relatórios das ferramentas ONTAP

O plug-in ONTAP tools for VMware vSphere fornece relatórios para máquinas virtuais e datastores. Ao selecionar o ícone do plug-in NetApp ONTAP tools for VMware vSphere na seção de atalhos no cliente vCenter, a interface de usuário navega para a página Visão geral. Selecione a guia Relatórios para visualizar o relatório de máquinas virtuais e datastores.

O relatório de máquinas virtuais exibe a lista de máquinas virtuais detectadas (que devem ter pelo menos um disco de storage baseado em ONTAP) com métricas de desempenho. Ao expandir o registro da VM, a interface exibe todas as informações do datastore relacionadas ao disco.

O relatório de datastores lista os datastores descobertos ou reconhecidos pelas ONTAP tools for VMware vSphere que usam qualquer storage ONTAP, com métricas de desempenho.

Você pode usar a opção Gerenciar Colunas para ocultar ou exibir diferentes colunas.

Gerenciar máquinas virtuais

Considerações sobre migração e clonagem de máquinas virtuais para ONTAP tools

ONTAP tools for VMware vSphere suportam todos os principais tipos de migração de máquina virtual, incluindo somente computação (vMotion), somente armazenamento (Storage vMotion) e migração combinada de computação e armazenamento em todos os datastores. Este tópico descreve as principais considerações e práticas recomendadas para garantir a migração e clonagem bem-sucedidas de máquinas virtuais, independentemente do tipo de datastore subjacente.

Migrar máquinas virtuais protegidas

Você pode migrar máquinas virtuais protegidas para:

- O mesmo armazenamento de dados em um host ESXi diferente
- Um armazenamento de dados compatível diferente no mesmo host ESXi
- Um armazenamento de dados compatível diferente em um host ESXi diferente

Se você migrar a máquina virtual para um volume FlexVol diferente, o sistema atualizará o arquivo de metadados desse volume com as informações da máquina virtual. Se uma máquina virtual for migrada para um host ESXi diferente, mas para o mesmo storage, o arquivo de metadados do volume FlexVol subjacente não será modificado.

Para obter informações sobre a migração de máquinas virtuais, consulte a documentação da Broadcom: ["vSphere Migração de Máquinas Virtuais"](#)

Clonar máquinas virtuais protegidas

Você pode clonar máquinas virtuais protegidas para o seguinte:

- O mesmo contêiner do mesmo FlexVol volume usando um grupo de replicação

O arquivo de metadados do mesmo volume FlexVol é atualizado com os detalhes da máquina virtual clonada.

- O mesmo contêiner de um volume FlexVol diferente usando um grupo de replicação

No volume FlexVol onde a máquina virtual clonada é colocada, o arquivo de metadados é atualizado com os detalhes da máquina virtual clonada.

- Um contêiner ou vVols datastore diferente

No volume FlexVol onde a máquina virtual clonada é colocada, o arquivo de metadados é atualizado com os detalhes da máquina virtual.

Atualmente, a VMware não oferece suporte a máquinas virtuais clonadas para um modelo de máquina virtual.

É possível criar um clone de um clone de uma máquina virtual protegida.

Consulte a documentação da Broadcom: ["Criando uma máquina virtual para clonagem"](#) para obter mais detalhes.

Instantâneos de máquinas virtuais

ONTAP tools suporta snapshots de máquinas virtuais por meio de fluxos de trabalho padrão da VMware. Snapshots são pontos de reversão de curto prazo destinados a casos de uso como testes e preparação de patches. Eles não substituem backup ou proteção de dados baseada em replicação. Executar uma máquina virtual em um snapshot por períodos prolongados pode causar instabilidade e perda de dados.

Você pode tirar snapshots consistentes com falhas (snapshots sem o estado da memória, que podem ser usados para reiniciar a máquina virtual em um estado consistente) em todos os tipos de datastore compatíveis. Snapshots quiesced, que usam o VMware Tools para gravar os dados em memória no disco antes da captura, também são compatíveis. Para obter uma visão geral dos tipos e comportamentos de snapshots, consulte "[Visão geral dos snapshots de máquina virtual em vSphere](#)".



Os snapshots de memória capturam o estado da memória em execução e interrompem temporariamente a máquina virtual. Eles não são suportados nos fluxos de trabalho das ONTAP tools. Se uma máquina virtual tiver um snapshot de memória, você deve excluí-lo antes que a máquina virtual possa ser incluída em um grupo de consistência ou em um relacionamento de cluster de hosts gerenciado pelas ONTAP tools.

Nos sistemas de storage ASA r2, o comportamento dos snapshots de máquina virtual difere de outros tipos de storage. Os snapshots são somente leitura. Ao ligar a máquina virtual, o VASA Provider cria um LUN a partir do snapshot somente leitura e habilita as IOPS. Ao desligar a máquina virtual, o VASA Provider exclui o LUN e desabilita as IOPS.

Para obter informações sobre como gerenciar snapshots de máquinas virtuais, consulte a documentação da Broadcom "[Gerencie máquinas virtuais com snapshots](#)".

Migrar máquinas virtuais para datastores vVols nas ONTAP tools

Você pode migrar máquinas virtuais de datastores NFS e VMFS para datastores Virtual Volumes (vVols) para aproveitar o gerenciamento de máquinas virtuais baseado em políticas e outros recursos de vVols. Os datastores vVols permitem que você atenda a requisitos crescentes de carga de trabalho.

Antes de começar

Certifique-se de que o VASA Provider não esteja em execução em nenhuma das máquinas virtuais que você planeja migrar. Se você migrar uma máquina virtual que esteja executando o VASA Provider para um vVols datastore, você não poderá realizar nenhuma operação de gerenciamento, incluindo ligar as máquinas virtuais que estão em vVols datastores.

Sobre esta tarefa

Ao migrar de um datastore NFS e VMFS para um datastore vVols, o servidor vCenter usa as APIs vStorage para integração de arrays (VAAI) ao mover dados de datastores VMFS, mas não de um arquivo VMDK NFS. As descarregas VAAI normalmente reduzem a carga no host.

Passos

1. Clique com o botão direito do mouse na máquina virtual que você deseja migrar e selecione **Migrar**.
2. Selecione **Alterar apenas o armazenamento** e, em seguida, selecione **Avançar**.
3. Selecione um formato de disco virtual, uma política de armazenamento de VM e um vVol datastore que corresponda aos recursos do datastore que você está migrando.
4. Revise as configurações e selecione **Concluir**.

Limpe as configurações do VASA nas ferramentas ONTAP

Para concluir o processo de limpeza do VASA, siga estas etapas.



Recomenda-se remover todos os datastores vVols antes de iniciar a limpeza do VASA.

Passos

1. Cancele o registro do plug-in acessando https://OTV_IP:8143/Register.html
2. Verifique se o plug-in não está mais disponível no vCenter Server.
3. Desligue as ONTAP tools for VMware vSphere máquina virtual.
4. Exclua a máquina virtual ONTAP tools for VMware vSphere.

Anexar ou desanexar um disco de dados de uma VM nas ONTAP tools

Siga estes passos para conectar ou desconectar discos de dados de máquinas virtuais no vSphere e gerenciar seus recursos de storage.

Anexe um disco de dados a uma máquina virtual

Anexe um disco de dados a uma máquina virtual para adicionar mais storage.

Passos

1. Faça login no cliente vSphere.
2. Clique com o botão direito do mouse em uma máquina virtual no inventário e selecione **Editar configurações**.
3. Na aba **Hardware Virtual**, selecione **disco rígido existente**.
4. Selecione a máquina virtual onde o disco existe.
5. Selecione o disco que você deseja conectar e selecione o botão **OK**.

Resultado

O disco rígido aparece na lista de dispositivos de hardware virtual.

Desconecte um disco de dados da máquina virtual

Desconecte um disco de dados de uma máquina virtual quando você não precisar mais dele. O disco não é excluído; ele permanece no sistema de storage ONTAP.

Passos

1. Faça login no cliente vSphere.
2. Clique com o botão direito do mouse em uma máquina virtual no inventário e selecione **Editar configurações**.
3. Mova o cursor sobre o disco e selecione **Remover**.



O disco é removido da máquina virtual. Se outras máquinas virtuais compartilharem o disco, os arquivos do disco não são excluídos.

Informações relacionadas

"Adicionar um novo disco rígido a uma máquina virtual"

"Adicionar um disco rígido existente a uma máquina virtual"

Descubra sistemas de armazenamento e hosts nas ferramentas ONTAP

Quando ONTAP tools for VMware vSphere é iniciado no vSphere Client pela primeira vez, ele descobre automaticamente os hosts ESXi, seus LUNs e exportações NFS associados, assim como os sistemas de storage NetApp que possuem esses recursos.

Antes de começar

- Certifique-se de que todos os hosts ESXi estejam ligados e conectados.
- Certifique-se de que todas as máquinas virtuais de armazenamento (SVMs) a serem descobertas estejam em execução e que cada nó de cluster tenha pelo menos uma LIF de dados configurada para o protocolo de storage em uso (NFS ou iSCSI).

Sobre esta tarefa

Você pode descobrir novos sistemas de storage ou atualizar os existentes para obter os detalhes mais recentes de capacidade e configuração. Você também pode alterar as credenciais do ONTAP tools for VMware vSphere para acesso ao sistema de storage.

Ao descobrir os sistemas de storage, ONTAP tools for VMware vSphere coleta informações dos hosts ESXi gerenciados pela instância do vCenter Server.

Passos

1. Na página inicial do vSphere Client, selecione **Hosts and Clusters**.
2. Clique com o botão direito do mouse no data center necessário e selecione **NetApp ONTAP tools > Atualizar dados do host**.

Na caixa de diálogo **Confirmar**, confirme sua escolha.

3. Selecione os controladores de armazenamento descobertos que possuem o status **Authentication Failure** e selecione **Ações > Modificar**.
4. Preencha as informações necessárias na caixa de diálogo **Modificar Storage System**.
5. Repita os passos 4 e 5 para todos os controladores de armazenamento com **Authentication Failure** status.

Após a conclusão do processo de descoberta, execute as seguintes ações:

- Use ONTAP tools for VMware vSphere para configurar as configurações do host ESXi para hosts que exibem o ícone de alerta na coluna de configurações do adaptador, na coluna de configurações MPIO ou na coluna de configurações NFS.
- Forneça as credenciais do sistema de storage.

Modifique as configurações do host ESXi usando as ferramentas ONTAP

Use o painel de ferramentas do ONTAP no VMware vSphere para identificar problemas de configuração, selecionar hosts ESXi, revisar as configurações recomendadas da NetApp e aplicá-las.

Antes de começar

O portlet de sistemas host ESXi exibe problemas com as configurações do host ESXi. Selecione um problema para visualizar o nome do host ou endereço IP.

Passos

1. Faça login no cliente vSphere.
2. Na página de atalhos, selecione **NetApp ONTAP tools** na seção de plug-ins.
3. Acesse o portlet **Conformidade do host ESXi** na Visão geral (painel de controle) do ONTAP tools for VMware vSphere plug-in.
4. Selecione o link **Aplicar configurações recomendadas**.
5. Na janela **Aplicar configurações de host recomendadas**, selecione os hosts para os quais você deseja usar as configurações de host recomendadas da NetApp e selecione **Avançar**.



Você pode expandir o host ESXi para ver os valores atuais.

6. Na página de configurações, selecione os valores recomendados conforme necessário.
7. No painel de resumo, verifique os valores e selecione **Concluir**. Você pode acompanhar o progresso no painel de tarefas recentes.

Informações relacionadas

["Configurar as configurações do host ESXi"](#)

Gerenciar senhas

Alterar a senha do ONTAP tools Manager

Você pode alterar a senha do administrador usando ONTAP tools Manager.

Passos

1. Inicie o ONTAP tools Manager a partir de um navegador da web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com suas credenciais de administrador das ONTAP tools for VMware vSphere.
3. Selecione o ícone de **administrador** no canto superior direito da tela e selecione **Alterar senha**.
4. Na janela pop-up de alteração de senha, insira a senha antiga e a nova senha. A interface de usuário mostra os requisitos da senha.
5. Selecione **Alterar** para aplicar as alterações.

Redefinir a senha do ONTAP tools Manager

Se você esquecer a senha do ONTAP tools Manager, pode restaurar o acesso de administrador usando um token de redefinição gerado no console de manutenção do ONTAP tools for VMware vSphere.

Passos

1. Abra um navegador da web e navegue até <https://<ONTAPtoolsIP>:8443/virtualization/ui/> para acessar o Gerenciador de ferramentas ONTAP.
2. Na página de login, selecione **Redefinir senha**.
3. Gere um token de redefinição de senha usando o console de manutenção do ONTAP tools for VMware vSphere:
 - a. Faça login no vCenter Server e abra o console de manutenção.
 - b. Pressione 2 Enter para selecionar **Configuração do Sistema**.
 - c. Pressione 3 para selecionar **Alterar a senha do usuário 'maint'**.
4. Na caixa de diálogo de redefinição de senha, insira o token de redefinição, o nome de usuário e a nova senha.
5. Selecione **Redefinir** para atualizar as credenciais.
6. Faça login no ONTAP tools Manager com a nova senha.

Redefinir senha de usuário do aplicativo nas ONTAP tools

Siga estas etapas para redefinir a senha do usuário do aplicativo necessária para o registro do SRA e do VASA Provider no vCenter Server usando ONTAP tools for VMware vSphere.

Passos

1. Abra um navegador da web e acesse: <https://<ONTAPtoolsIP>:8443/virtualization/ui/>
2. Faça login usando as credenciais de administrador configuradas durante a implantação das ONTAP tools.
3. Na barra lateral, selecione **Configurações**.
4. Na página **Credenciais VASA/SRA**, selecione **Redefinir senha**.
5. Digite e confirme a nova senha.
6. Selecione **Redefinir** para aplicar a nova senha.

Redefina a senha do console de manutenção das ONTAP tools

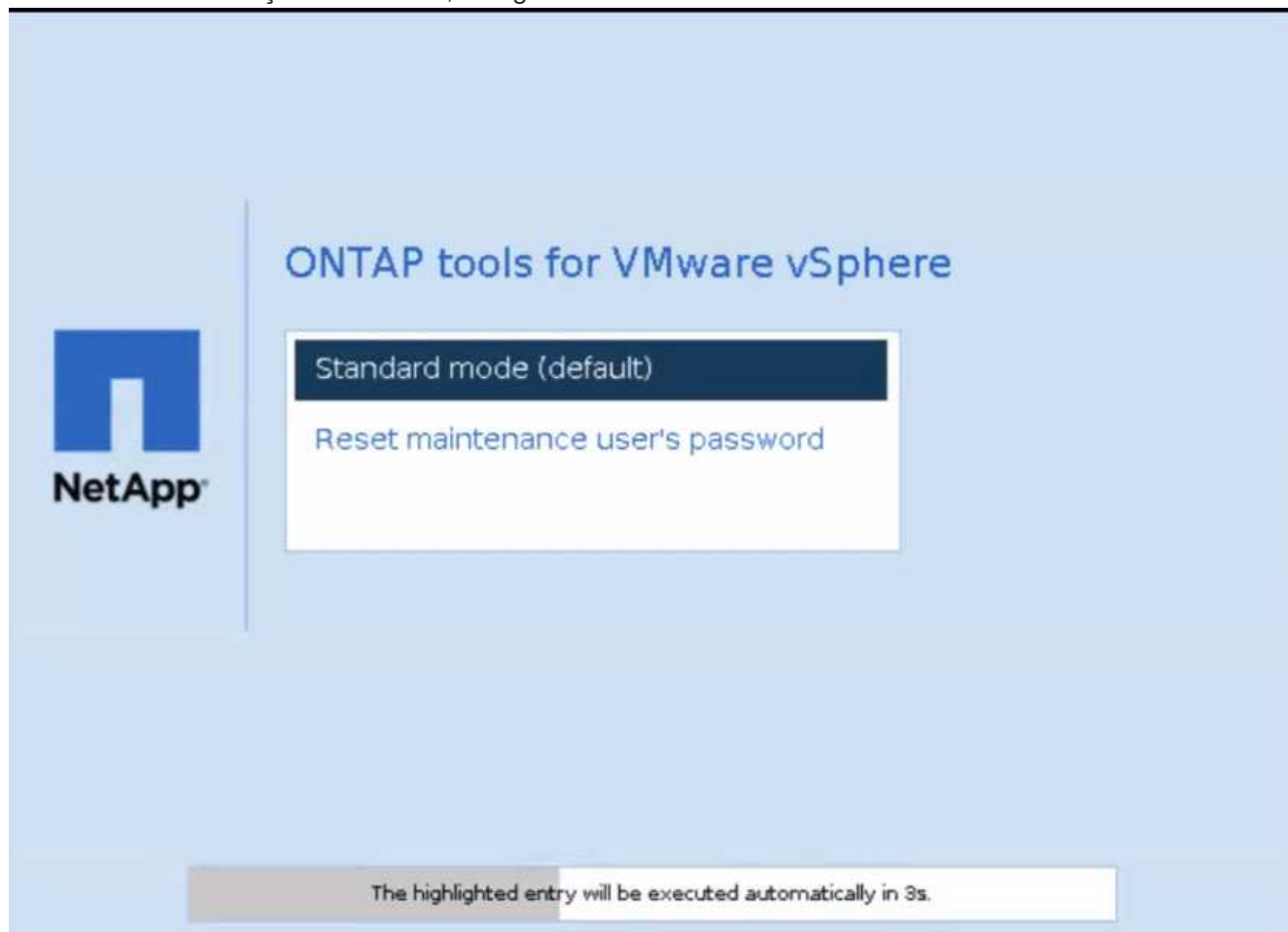
Durante uma operação de reinicialização do sistema operacional convidado, o menu GRUB exibe uma opção para redefinir a senha do usuário do console de manutenção. Use essa opção para atualizar a senha do usuário do console de manutenção na máquina virtual. Após redefinir a senha, a máquina virtual reinicia para definir a nova senha. Em um cenário de implantação em HA, após a reinicialização da máquina virtual, a senha é atualizada automaticamente nas outras duas máquinas virtuais.



Para a implantação de alta disponibilidade (HA) do ONTAP tools for VMware vSphere, você deve alterar a senha do usuário do console de manutenção no nó de gerenciamento do ONTAP tools, que é o node1.

Passos

1. Faça login no seu vCenter Server
2. Clique com o botão direito do mouse na máquina virtual e selecione **Energia > Reiniciar SO convidado**. Durante a reinicialização do sistema, a seguinte tela será exibida:



Você tem 5 segundos para escolher sua opção. Pressione qualquer tecla para interromper o progresso e congelar o menu GRUB.

3. Selecione a opção **Redefinir senha do usuário de manutenção**. O console de manutenção é aberto.
4. No console, digite e confirme a nova senha. Você tem três tentativas. O sistema reinicia após você inserir corretamente a nova senha.
5. Pressione **Enter** para continuar. O sistema atualiza a senha na máquina virtual.



O mesmo menu GRUB aparece quando você liga a máquina virtual. No entanto, você deve usar a opção de redefinição de senha somente com a opção **Reiniciar SO convidado**.

Gerenciar a proteção do cluster de hosts

Modificar um cluster de hosts protegido nas ferramentas ONTAP

Você pode alterar as configurações de proteção de um cluster de hosts em um único fluxo de trabalho. As seguintes alterações são suportadas:

- Adicione novos datastores ou hosts ao cluster protegido.
- Adicione novos SnapMirror relacionamentos às configurações de proteção.
- Exclua os relacionamentos SnapMirror existentes das configurações de proteção.
- Modificar uma relação do SnapMirror existente.



Você precisa executar a descoberta de armazenamento após criar, editar ou excluir a proteção para um cluster de hosts para refletir as alterações. Se você não executar a descoberta de armazenamento, as alterações serão refletidas após a descoberta periódica de armazenamento ser acionada.

Monitorar a proteção do cluster de hosts

Monitore o status de proteção, os relacionamentos SnapMirror, os datastores e o status SnapMirror de cada cluster de hosts protegido.

Passos

1. Faça login no cliente vSphere.
2. Acesse **NetApp ONTAP tools > Proteção > Relações de cluster de hosts**.

A coluna de proteção exibe um ícone que mostra o status da proteção.

3. Passe o cursor sobre o ícone para ver mais detalhes.

Adicione novos datastores ou hosts

Adicione hosts ou crie datastores no cluster protegido usando a interface de usuário do vCenter.

Passos

1. Faça login no cliente vSphere.
2. Para editar as propriedades de um cluster protegido, você pode
 - a. Acesse **NetApp ONTAP tools > Proteção > Relacionamentos de cluster de hosts**, selecione o menu de reticências ao lado do cluster e selecione **Editar** ou
 - b. Clique com o botão direito do mouse em um cluster de hosts e selecione **NetApp ONTAP tools > Proteger Cluster**.
3. Se você criar um datastore na interface de usuário do vCenter, ele aparecerá como desprotegido. Você pode visualizar todos os datastores no cluster e seus status de proteção em uma caixa de diálogo. Selecione o botão **Proteger** para habilitar a proteção.



Após criar um datastore na interface de usuário do vCenter Server, selecione **Discover** na página de visão geral para exibir o datastore como um candidato à proteção no cluster de hosts. O status de proteção é atualizado para protegido após a próxima descoberta periódica de proteção.

4. Ao adicionar um novo host ESXi, o status de proteção é exibido como parcialmente protegido. Selecione o

menu de reticências em SnapMirror e selecione **Editar** para definir a proximidade do host ESXi recém-adicionado.



Para relações assíncronas, a edição não é suportada nas ONTAP tools porque o SVM de destino para um site terciário não pode ser adicionado à mesma instância. Para modificar a configuração da relação, use o System Manager ou a CLI no SVM de destino.

5. Após efetuar as alterações, selecione **Salvar**.
6. Você pode ver as alterações na janela **Protect Cluster**.

As ferramentas ONTAP criam uma tarefa do vCenter e você pode acompanhar o progresso dela no painel **Tarefas recentes**.

Adicionar uma nova SnapMirror relationship

Passos

1. Faça login no cliente vSphere.
2. Para editar as propriedades de um cluster protegido, você pode
 - a. Acesse **NetApp ONTAP tools > Proteção > Relações de cluster de hosts**, selecione o menu de reticências ao lado do cluster e selecione **Editar** ou
 - b. Clique com o botão direito do mouse em um cluster de hosts e selecione **NetApp ONTAP tools > Proteger Cluster**.
3. Selecione **Adicionar relação**.
4. Adicione um novo relacionamento como tipo de política **Assíncrono** ou **AutomatedFailOverDuplex**.
5. Selecione **Protect**.

Você pode ver as alterações na janela **Protect Cluster**.

As ferramentas ONTAP criam uma tarefa do vCenter e você pode acompanhar o progresso dela no painel **Tarefas recentes**.

Excluir uma relação do SnapMirror existente

Para excluir uma relação assíncrona do SnapMirror, certifique-se de que o SVM ou cluster do site secundário esteja adicionado como um backend de armazenamento em ONTAP tools for VMware vSphere. Você não pode excluir todas as relações do SnapMirror de uma só vez. Excluir uma relação também remove a relação correspondente do cluster ONTAP. Ao excluir uma relação Automated Failover Duplex do SnapMirror, o sistema desmapeia os datastores de destino e exclui o grupo de consistência, LUNs, volumes e igroups do cluster ONTAP de destino.

Ao excluir a relação do SnapMirror, o sistema verifica novamente o site secundário para remover o LUN não mapeado como um caminho ativo dos hosts.

Passos

1. Faça login no cliente vSphere.
2. Para editar as propriedades de um cluster protegido, você pode
 - a. Acesse **NetApp ONTAP tools > Proteção > Relações de cluster de hosts**, selecione o menu de reticências ao lado do cluster e selecione **Editar** ou

- b. Clique com o botão direito do mouse em um cluster de hosts e selecione **NetApp ONTAP tools > Proteger Cluster**.

3. Selecione o menu de reticências em SnapMirror configurações e selecione **Excluir**.

- Se você excluir um relacionamento baseado em tipo de política assíncrona de um cluster de hosts protegido, deverá remover manualmente os elementos de armazenamento do storage terciário. Os elementos de armazenamento incluem grupos de consistência, volumes (para sistemas ONTAP), unidades de armazenamento (LUNs/Namespaces) e snapshots.
- Se você excluir uma relação do SnapMirror baseada em políticas de Failover Duplex Automatizado (AFD) de um cluster de hosts protegido, poderá optar por remover os elementos de armazenamento associados no storage secundário diretamente da interface.
- Se você excluir uma relação do SnapMirror baseada em políticas de Failover Duplex Automatizado (AFD) e o grupo de consistência agora for hierárquico para backups em nível de aplicativo, um aviso sobre o impacto no backup será exibido. Confirme para prosseguir. Após a confirmação, exclua os elementos de armazenamento associados no storage secundário. Se você não os remover, eles permanecerão no site secundário.

As ferramentas ONTAP criam uma tarefa do vCenter e você pode acompanhar o progresso dela no painel **Tarefas recentes**.

Modificar uma relação do SnapMirror existente

Para modificar uma relação assíncrona do SnapMirror, certifique-se de que o SVM ou cluster do site secundário seja adicionado como backend de armazenamento em ONTAP tools for VMware vSphere. Para relações Automated Failover Duplex do SnapMirror, você pode atualizar a proximidade do host para configurações uniformes ou o acesso ao host para configurações não uniformes. Não é suportada a alteração entre os tipos de política Assíncrono e Automated Failover Duplex. Você pode configurar as definições de proximidade ou acesso para hosts recém-descobertos no cluster.



Você não pode editar uma relação do SnapMirror assíncrona existente.

Passos

1. Faça login no cliente vSphere.
2. Para editar as propriedades de um cluster protegido, você pode
 - a. Acesse **NetApp ONTAP tools > Proteção > Relações de cluster de hosts**, selecione o menu de reticências ao lado do cluster e selecione **Editar** ou
 - b. Clique com o botão direito do mouse em um cluster de hosts e selecione **NetApp ONTAP tools > Proteger Cluster**.
3. Se o tipo de política AutomatedFailOverDuplex for selecionado, adicione detalhes de proximidade do host ou de acesso ao host.
4. Selecione o botão **Proteger**.

ONTAP tools criam uma tarefa do vCenter. Acompanhe o progresso dela no painel **Tarefas recentes**.

Remover a proteção de cluster de hosts nas ONTAP tools

Ao remover a proteção do cluster de hosts, os datastores ficam desprotegidos.

Passos

1. Para visualizar a lista de clusters de hosts protegidos, acesse **NetApp ONTAP tools > Proteção >**

Relacionamentos de clusters de hosts.

Nesta página, você pode monitorar clusters de hosts protegidos, estado de proteção, SnapMirror relacionamento e status. Selecione grupos de consistência para visualizar a capacidade, os datastores associados e os grupos filhos.

2. Na janela **Proteção do cluster de hosts**, selecione o menu de reticências ao lado do cluster e selecione **Remover proteção**.
 - Se você remover a proteção de um cluster de hosts com apenas um SnapMirror relacionamento assíncrono, deverá excluir manualmente os elementos de armazenamento. Os elementos de armazenamento incluem grupos de consistência, volumes (para sistema ONTAP), unidades de armazenamento (LUNs) e snapshots.
 - Se você remover a proteção de um cluster de hosts que possui apenas uma relação de política de SnapMirror baseada em failover automatizado duplex e um grupo de consistência não hierárquico, poderá excluir os elementos de armazenamento associados no storage secundário diretamente da mesma tela.
 - Se você remover a proteção de um cluster de hosts com políticas SnapMirror e um grupo de consistência hierárquico para backups, um aviso sobre os impactos no backup será exibido. Confirme para prosseguir. Após a confirmação, exclua os elementos de armazenamento associados no storage secundário. Se você não fizer a limpeza, os elementos de armazenamento permanecerão no site secundário.

Recupere a configuração das ONTAP tools

A partir do ONTAP tools for VMware vSphere 10.5, o recurso de backup está ativado por padrão.

O datastore onde você implanta as ONTAP tools for VMware vSphere virtual machines armazena os arquivos de backup. Uma pasta nomeada com o endereço IP das ONTAP tools (os pontos são substituídos por sublinhados e com o sufixo *OTV_backup*) mantém os dois arquivos de backup mais recentes (*OTV_backup_1.tar.enc* e *OTV_backup_2.tar.enc*) e um arquivo de informações (*OTV_backup_info.txt*) que contém o nome do backup mais recente.

Certifique-se de que a nova máquina virtual utilize o mesmo endereço IP das ferramentas ONTAP e corresponda à configuração inicial do sistema, incluindo serviços habilitados, tamanho do nó e modo HA.

Passos

1. Faça o download dos arquivos de backup do datastore da máquina virtual original para o seu sistema local.
 - a. Acesse a seção de storage e escolha o datastore que contém os arquivos de backup da máquina virtual.
 - b. Selecione a seção **Arquivos**.
 - c. Baixe o diretório de backup necessário.
2. Desligue a máquina virtual existente. Em seguida, implante uma nova máquina virtual usando o mesmo arquivo OVA da implantação original.
3. No vCenter Server, abra o console de manutenção.
4. Faça login como usuário de manutenção.
5. Digite 4 para selecionar **Suporte e Diagnóstico**.

6. Pressione 2 Enter para selecionar a opção **Ativar acesso remoto para diagnóstico** e crie uma nova senha para o acesso de diagnóstico.
7. Escolha um arquivo de backup no diretório baixado. Consulte o arquivo *OTV_backup_info.txt* para identificar o backup mais recente.
8. Utilize o seguinte comando para transferir o arquivo de backup para a nova máquina virtual. Quando solicitado, insira a senha de diagnóstico.

```
scp <OTV_backup_X.tar.enc>  
diag@<node_ip>:/home/diag/system_recovery.tar.enc
```



Não altere o caminho de destino e o nome do arquivo (/home/diag/system_recovery.tar.enc) mencionados no comando.

9. Após a transferência do arquivo de backup, faça login no shell de diagnóstico e execute o seguinte comando:

```
sudo perl /home/maint/scripts/post-deploy-upgrade.pl -recovery
```

Os registros são gravados no arquivo */var/log/post-deploy-upgrade.log*.

Após a conclusão da recuperação, as ONTAP tools restauram os serviços e os objetos do vCenter.

Desinstalar ONTAP tools

Desinstalar o ONTAP tools for VMware vSphere exclui todos os dados nas ferramentas.

Passos

1. Remova ou mova todas as máquinas virtuais dos datastores gerenciados pelas ONTAP tools for VMware vSphere.
 - Para remover as máquinas virtuais, consulte ["Remova e registre novamente as VMs e os modelos de VM"](#)
 - Para movê-los para um armazenamento de dados não gerenciado, consulte ["Como migrar sua máquina virtual com storage vMotion"](#)
2. ["Excluir datastores"](#) criado em ONTAP tools for VMware vSphere.
3. Se você habilitou o provedor VASA, selecione **Configurações > Configurações do provedor VASA > Cancelar registro** em ONTAP tools para cancelar o registro dos provedores VASA de todos os servidores vCenter.
4. Desassocie todos os backends de armazenamento da instância do servidor vCenter. Consulte ["Desassocie os backends de armazenamento da instância do servidor vCenter"](#).
5. Exclua todos os backends de armazenamento. Consulte ["Gerenciar back-ends de armazenamento"](#).
6. Remova o adaptador SRA do VMware Live Site Recovery:
 - a. Faça login como admin na interface de gerenciamento do appliance VMware Live Site Recovery usando a porta 5480.

- b. Selecione **Storage Replication Adapters**.
- c. Selecione o cartão SRA apropriado e, no menu suspenso, selecione **Excluir**.
- d. Confirme que você sabe os resultados de excluir o adaptador e selecione **Excluir**.
7. Exclua as instâncias de servidor vCenter integradas às ONTAP tools for VMware vSphere. Consulte ["Gerenciar instâncias do servidor vCenter"](#).
8. Desligue as máquinas virtuais ONTAP tools for VMware vSphere a partir do vCenter Server e exclua as VMs.

Qual o próximo passo?

["Remover volumes FlexVol"](#)

Remova os volumes FlexVol após desinstalar as ONTAP tools

Quando você usa um ONTAP cluster dedicado para a implantação do ONTAP tools for VMware, muitos volumes FlexVol não utilizados são criados. Após remover o ONTAP tools for VMware vSphere, você deve remover os volumes FlexVol para evitar possíveis impactos no desempenho.

Passos

1. Descubra o tipo de implantação das ONTAP tools for VMware vSphere a partir da VM do nó de gerenciamento das ONTAP tools. Execute o seguinte comando para verificar o tipo de implantação: `cat /opt/netapp/meta/ansible_vars.yaml | grep -i protocol`

Se for uma implementação iSCSI, exclua também os igroups.
2. Obtenha a lista de volumes FlexVol. `kubectl describe persistentvolumes | grep internalName | awk -F=' '{print $2}'`
3. Remova as VMs do vCenter Server. Consulte ["Remova e registre novamente as VMs e os modelos de VM"](#).
4. Exclua volumes FlexVol. Consulte ["Excluir um volume FlexVol"](#). Digite o nome exato do volume FlexVol no comando da CLI para excluí-lo.
5. Exclua os igroups SAN do sistema de storage ONTAP em caso de implantação iSCSI. Consulte ["Visualize e gerencie iniciadores SAN e igroups"](#).

Atualize as ONTAP tools for VMware vSphere

Atualize das ONTAP tools for VMware vSphere 10.x para 10.5

Você pode atualizar de ONTAP tools for VMware vSphere 10.3 ou 10.4 para 10.5. No entanto, para atualizar de ONTAP tools 10.0, 10.1 ou 10.2 para 10.5, você deve primeiro atualizar para 10.3 ou 10.4 antes de prosseguir para 10.5.



- Para sistemas ASA r2, certifique-se de atualizar ONTAP tools for VMware vSphere para 10.5 e ONTAP para 9.16.1 antes de configurar mais storage availability zones (SAZs).
- Se a atualização do ONTAP tools for VMware vSphere 10.3 ou 10.4 para 10.5 falhar, você não poderá reverter. Use RPO baixo ou recuperação por snapshot para restaurar a configuração. Para ONTAP tools for VMware vSphere 10.2 e anteriores, use RPO zero para restaurar a configuração.

Antes de começar

- Certifique-se de que todos os nós estejam ativos.
- Certifique-se de que o certificado do sistema ONTAP e os certificados integrados do vCenter sejam válidos por pelo menos 5 dias. Se os certificados expirarem antes desse prazo, a atualização falhará.
- Certifique-se de ter um quinto disco com capacidade de 100 GB em todos os nós.
- Verifique se a configuração do nó corresponde às especificações na tabela abaixo.

Tipo de implantação	CPU (núcleo) por nó	Memória (GB) por nó	Espaço em disco (GB) por nó	CPU total (núcleos)	Memória (GB)	Espaço total em disco (GB)
Não-HA pequenos	9	18	350	9	18	350
Médio não HA	13	26	350	13	26	350
HA pequeno	9	18	350	27	54	1050
HA Médio	13	26	350	39	78	1050
HA Grande	17	34	350	51	102	1050

- Certifique-se de que o hot plug-in para CPU e RAM está habilitado.
- Habilite backup com baixo RPO e certifique-se de que um backup esteja visível na interface do Cliente vCenter. Baixe a pasta de backup antes da atualização.
- Recomenda-se um backup com RPO baixo. No entanto, em implantações sem HA, você pode criar um snapshot quiescente da máquina virtual ONTAP tools antes de atualizar.

Consulte ["Editar configurações de backup"](#) e ["Recupere a configuração das ONTAP tools"](#) para obter mais informações sobre backup e recuperação.

Passos

1. Faça upload do ISO de atualização do ONTAP tools for VMware vSphere na biblioteca de conteúdo.

2. Na página da VM primária, selecione **Ações > Editar configurações**. Para identificar o nome da VM primária:
 - a. Ative o shell de diagnóstico em qualquer nó
 - b. Execute o seguinte comando:

```
grep sourceHost /opt/netapp/meta/ansible_vars.yaml
```
3. Selecione o **arquivo ISO da biblioteca de conteúdo** na janela de edição de configurações, no campo **unidade de CD/DVD**.
4. Selecione o arquivo ISO, marque a caixa **Conectado** no campo **CD/DVD drive** e clique em **OK**.
5. No vCenter Server, abra um console para ONTAP tools.
6. Faça login como usuário de manutenção.
7. Digite **2** para selecionar o menu **Configuração do Sistema**.
8. Digite **6** para selecionar a opção **Upgrade**.
9. Forneça as credenciais do vCenter quando solicitado. Esta é a instância do vCenter onde o ONTAP tools está hospedado.

Se você estiver usando as ferramentas ONTAP em uma topologia de dois vCenter Server—onde o appliance está hospedado em uma instância vCenter e gerencia outra, você pode atribuir uma função restrita para a instância vCenter que hospeda as ferramentas ONTAP. Você pode criar um usuário e uma função dedicados vCenter com apenas as permissões necessárias para a implantação do template OVF. Para obter detalhes, consulte as funções listadas em ["Funções incluídas nas ONTAP tools for VMware vSphere 10"](#).

Para a instância do vCenter que será gerenciada pelas ONTAP tools, certifique-se de que a conta de usuário do vCenter tenha privilégios de administrador.

Durante a atualização, se algum certificado de backend de armazenamento integrado estiver sem entradas de Nome Alternativo do Assunto (SAN), você receberá uma mensagem indicando o SAN ausente. Se você optar por prosseguir sem validar o SAN, a atualização continuará, mas isso não é recomendado devido a potenciais riscos de segurança.

10. Ao atualizar, as seguintes ações são executadas automaticamente:
 - a. O certificado do gateway é renovado com um período de validade de 1 ano. Ao remover o adaptador SRA anterior e carregar o novo adaptador 10.5, a validade do certificado SRA muda de 10 anos para 1 ano.
 - b. Plug-in remoto foi atualizado
 - c. Os certificados do ONTAP e do servidor vCenter são validados e adicionados às ONTAP tools
 - d. O backup está ativado

O que vem a seguir

Após a atualização para ONTAP tools for VMware vSphere 10.5:

- Monitore os alertas do sistema e planeje renovar o certificado do gateway antes que ele expire em um ano.
- Remova o adaptador SRA das ONTAP tools 10.4 ou 10.3 e carregue o arquivo tar do adaptador SRA 10.5.
- Execute o comando de instalação após carregar o arquivo tar do adaptador SRA. Em seguida, verifique novamente os adaptadores SRA para atualizar a página de Storage Replication Adapters do VMware Site Recovery.

Após a atualização, você pode:

- Desative os serviços na interface de usuário do gerente
- Migrar de uma configuração sem alta disponibilidade (HA) para uma configuração com alta disponibilidade (HA)
- Aumente uma configuração pequena não HA para uma configuração média não HA, ou para uma configuração média ou grande HA.

Informações relacionadas

["Migrar das ONTAP tools for VMware vSphere 9.xx para 10.5"](#)

Códigos de erro de atualização das ONTAP tools

Você pode encontrar códigos de erro durante a operação de atualização das ONTAP tools for VMware vSphere. Os códigos de erro têm cinco dígitos, onde os dois primeiros dígitos representam o script que apresentou o problema e os três últimos dígitos representam o fluxo de trabalho específico dentro desse script.

Todos os registros de erros são armazenados no arquivo `ansible-perl-errors.log` para facilitar o rastreamento e a resolução de problemas. Este arquivo de log contém o código de erro e a tarefa Ansible que falhou.



Os códigos de erro fornecidos nesta página são apenas para referência. Entre em contato com a equipe de suporte se o erro persistir ou se não houver resolução mencionada.

A tabela a seguir lista os códigos de erro e os nomes de arquivo correspondentes.

Código de erro	Nome do script
00	firstboot-network-config.pl, modo deploy
01	firstboot-network-config.pl, modo upgrade
02	firstboot-inputs-validation.pl
03	firstboot-deploy-otv-ng.pl, implantar, HA
04	firstboot-deploy-otv-ng.pl, deploy, non-HA
05	firstboot-deploy-otv-ng.pl, reinicializar
06	firstboot-deploy-otv-ng.pl, upgrade, HA
07	firstboot-deploy-otv-ng.pl, atualização, não HA
08	firstboot-otv-recovery.pl
09	post-deploy-upgrade.pl

Os três últimos dígitos do código de erro indicam o erro específico no fluxo de trabalho dentro do script:

Código de erro de upgrade	Fluxo de trabalho	Resolução
052	A ISO pode ser a mesma da versão atual ou duas versões acima da versão atual.	Utilize uma versão ISO compatível para atualizar a partir da sua versão atual.

Código de erro de upgrade	Fluxo de trabalho	Resolução
068	Falha ao reverter pacotes Debian	Use recuperação baseada em RPO zero ou em snapshots e tente atualizar novamente.
069	Falha ao restaurar arquivos	Use recuperação baseada em RPO zero ou em snapshots e tente atualizar novamente.
070	Falha ao excluir backup	-
071	O cluster Kubernetes não estava saudável	-
074	A montagem ISO falhou	Verifique o arquivo /var/log/upgrade-run.log e tente atualizar novamente.
075	As verificações prévias da atualização falharam	Tente atualizar novamente.
076	A atualização do registro falhou	Use recuperação baseada em RPO zero ou em snapshots e tente atualizar novamente.
077	Falha ao reverter o registro	Use recuperação baseada em RPO zero ou em snapshots e tente atualizar novamente.
078	A atualização do operador falhou	Use recuperação baseada em RPO zero ou em snapshots e tente atualizar novamente.
079	Falha ao reverter operador	Use recuperação baseada em RPO zero ou em snapshots e tente atualizar novamente.
080	A atualização dos serviços falhou	Use recuperação baseada em RPO zero ou em snapshots e tente atualizar novamente.
081	Falha ao reverter serviços	Use recuperação baseada em RPO zero ou em snapshots e tente atualizar novamente.
082	A exclusão de imagens antigas do contêiner falhou	Use recuperação baseada em RPO zero ou em snapshots e tente atualizar novamente.
083	A exclusão do backup falhou	Use recuperação baseada em RPO zero ou em snapshots e tente atualizar novamente.

Código de erro de upgrade	Fluxo de trabalho	Resolução
084	A reversão do JobManager para produção falhou	Execute os seguintes passos para recuperar/concluir a atualização. 1. Habilite o Diagnostic Shell 2. Execute o comando: <i>sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade</i> 3. Verifique os logs em /var/log/post-deploy-upgrade.log
087	As etapas pós-upgrade falharam.	Execute os seguintes passos para recuperar/concluir a atualização. 1. Habilite o Diagnostic Shell 2. Execute o comando <i>sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade</i> 3. Verifique os logs em /var/log/post-deploy-upgrade.log
088	A configuração de rotação de logs para o journald falhou	Verifique as configurações de rede da máquina virtual (VM) compatíveis com o host em que a VM está hospedada. Você pode tentar migrar a VM para outro host e reiniciar.
089	A alteração da propriedade do arquivo de configuração de rotação do log de resumo falhou	Tente atualizar novamente.
095	A atualização do sistema operacional falhou	Não há recuperação para a atualização do sistema operacional. Os serviços do ONTAP tools são atualizados e novos pods serão executados.
096	Instale o provisionador de armazenamento dinâmico	Verifique os registros de upgrade e tente atualizar novamente.
097	A desinstalação dos serviços para upgrade falhou	Use RPO zero ou recuperação baseada em snapshot e tente atualizar novamente.
098	Falha ao copiar o segredo dockercred do ntv-system para o namespace do provisionador de storage dinâmico	Verifique os registros de upgrade e tente atualizar novamente.
099	Falha ao validar a nova adição de HDD	Adicione o novo HDD a todos os nós em caso de HA e a um nó em caso de implantação sem HA.
109	O backup dos dados de volume persistente falhou	Verifique os registros de upgrade e tente atualizar novamente.

Código de erro de upgrade	Fluxo de trabalho	Resolução
110	A restauração dos dados de volume persistente falhou	Use recuperação baseada em RPO zero ou em snapshots e tente atualizar novamente.
111	Falha ao atualizar os parâmetros de tempo limite do etcd para RKE2	Verifique os registros de upgrade e tente atualizar novamente.
112	A desinstalação do provisionador de armazenamento dinâmico falhou	-
113	A atualização dos recursos nos nós secundários falhou	Verifique os registros de upgrade e tente atualizar novamente.
104	A reinicialização do nó secundário falhou	Reinicie os nós manualmente, um por um.
100	a reversão do kernel falhou	-
051	A atualização do provisionador de armazenamento dinâmico falhou	Verifique os registros de atualização e tente atualizar novamente.
056	A exclusão do backup de migração falhou	N/A
090	Falha na validação de certificado para backends de armazenamento e vCenter	Verifique os registros de atualização e o arquivo de log em <code>/var/log/cert_validation_error.log</code> e tente a atualização novamente.

Código de erro de upgrade	Fluxo de trabalho	Resolução
114	A atualização do certificado interno na coleção do MongoDB falhou	Se a atualização falhar com o código de erro 114, execute os seguintes passos: 1. Conecte-se à ISO de atualização no nó primário e habilite o shell de diagnóstico. 2. Monte a imagem ISO a partir da sessão SSH no nó primário: <pre> sudo mount /dev/cdrom sudo mount -o loop,ro /dev/cdrom/APPLIANCE_UPGRADE.bin /upgrade </pre> 3. Instalar pacotes Debian: <pre> sudo dpkg -iE /upgrade/dists/squeeze/main/binary-amd64/vplatform.deb sudo dpkg -iE /upgrade/dists/squeeze/main/binary-amd64/vpupgrader.deb sudo dpkg -iE /upgrade/dists/squeeze/main/binary-amd64/vmware-tools.deb </pre> 4. Copie o arquivo de informações de compilação: <pre> sudo cp /upgrade/APPLIANCE_BUILD / </pre> 5. Adicione certificados à coleção ativando o shell de diagnóstico e executando:



A partir do ONTAP tools for VMware vSphere 10.3, o RPO zero não é suportado.

Saiba mais sobre ["Como restaurar ONTAP tools for VMware vSphere se a atualização da versão 10.0 para 10.1 falhar"](#)

```
sudo perl
/home/maint/scripts
/post-deploy-
upgrade.pl
--internal_cert_upd
ate_collection
```

Verifique os registros em
/var/log/otvng/post-
deploy-upgrade.log.

6. Reinicie os nós:

```
sudo bash
/home/maint/scripts
/vault_decrypt.sh
cd
/home/maint/rke2-pb
sudo ansible-
playbook site.yaml
--tags
restart_nodes
--skip-tags
debian_upgrade,kern
el_upgrade,rescan_s
csi_bus,source_iso,
eject_upgrade,mount
Iso,upgradeNodes,re
gistryUpg,deleteOld
Images,wait,checkRe
achability,delete_o
tv_cr,uninstall_tri
dent,del_trident_im
ages,refresh_resour
ces,ntp_configure,n
tpd_uninstall
```

7. Execute as etapas pós-atualização:

```
sudo perl
/home/maint/scripts
/post-deploy-
upgrade.pl
--postupgrade
```

Migrar ONTAP tools for VMware vSphere 9.xx para 10.5

Migrar das ONTAP tools for VMware vSphere 9.xx para 10.5

Mover a configuração das NetApp ONTAP tools for VMware vSphere da versão 9.xx para a 10.5 requer um processo de migração devido às significativas atualizações e melhorias do produto entre as versões.

Você pode migrar das versões ONTAP tools for VMware vSphere 9.12D1, 9.13D2 e 9.13P2 para ONTAP tools for VMware vSphere 10.5.

Se você possui datastores NFS e VMFS e não possui vVols datastores em sua configuração, basta desinstalar ONTAP tools 9.xx e implantar ONTAP tools 10.5. No entanto, se sua configuração contém vVols datastores, você deve realizar um processo de migração do VASA Provider e do SRA.

A tabela a seguir descreve o processo de migração nesses dois cenários diferentes.

Se a configuração tiver datastores vVols	Se a configuração contiver apenas datastores NFS e VMFS
Etapas: 1. "Migrar o provedor VASA" 2. "Criar políticas de storage de VM"	Etapas: 1. Remova ONTAP tools 9.xx do seu ambiente. Consulte o "Como remover OTV 9.xx do seu ambiente" NetApp artigo da Knowledge Base. 2. "Implantar e configurar ONTAP tools for VMware vSphere 10.5" 3. "Atualize o SRA" 4. "Criar políticas de storage de VM"



Após migrar das ONTAP tools for VMware vSphere 9.xx para 10.5, os datastores vVols que utilizam o protocolo NVMe/FC se tornam não operacionais porque as ONTAP tools 10.5 suportam o protocolo NVMe-oF apenas com datastores VMFS.

Migre o provedor VASA e atualize o SRA nas ONTAP tools

Siga os passos desta seção para migrar o VASA Provider do ONTAP tools for VMware vSphere 9.xx para o ONTAP tools for VMware vSphere 10.5 e atualizar o Storage Replication Adapter (SRA) no appliance VMware Live Site Recovery.

Etapas para migrar o provedor VASA

1. Para habilitar a porta 1527 do Derby nas ONTAP tools for VMware vSphere existentes, habilite o usuário raiz e faça login na CLI via SSH. Em seguida, execute o seguinte comando:

```
iptables -I INPUT 1 -p tcp --dport 1527 -j ACCEPT
```

2. Implantar OVA para ONTAP tools for VMware vSphere 10.5.
3. Adicione a instância do servidor vCenter que você deseja migrar para ONTAP tools for VMware vSphere

versão 10.5. Consulte ["Adicionar uma instância do servidor vCenter"](#) para mais informações.

4. ["Habilitar provedor VASA"](#) serviço em ONTAP tools for VMware vSphere 10.5.
5. Integre o backend de armazenamento localmente a partir das APIs do servidor vCenter para o plug-in ONTAP tools. Consulte ["Adicione um backend de armazenamento usando o console do cliente vSphere"](#) para mais informações.
6. Obtenha um token de acesso para autenticar solicitações à API REST. Use o exemplo a seguir, substituindo as variáveis por valores específicos do seu ambiente.

8. Verifique se a operação foi concluída com sucesso.

```
tail -f  
/var/log/post-
```

```
curl --request POST \  
  --location "https://$FQDN_IP_PORT/virtualization/api/v1/auth/vcenter-  
login" \  
  --header "Content-Type: application/json" \  
  --header "Accept: */*" \  
  -d '{"username": "$MYUSER", "password": "$MYPASSWORD", "vcenter  
hostname": "$MYVCENTER"}'
```

Copie e salve o token de acesso retornado na resposta.

7. Emita a seguinte API a partir do Swagger ou Postman para migrar.

```
sudo umount -l -f  
/upgrade  
sudo umount -l -f  
/dev/cdrom
```

```
curl -X POST  
`https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/{vcguid}/migra  
tion-jobs`
```

Você pode acessar o Swagger através deste URL: [https://\\$FQDN_IP_PORT/](https://$FQDN_IP_PORT/), por exemplo:
<https://10.67.25.33:8443/>.

```
sudo reboot -f
```

Método HTTP e endpoint

Esta chamada à API REST utiliza o seguinte método e endpoint.

Método HTTP	Caminho
POST	/api/v1

Tipo de processamento

Assíncrono

Exemplo de curl

```
curl -X POST 'https://<OTV-NG-IP>:8443/virtualization/api/v1/vcenters/<vcguid>/migration-jobs' \
--header 'x-auth: <auth_token>' \
--header 'Content-Type: application/json' \
--data '{
  "otv_ip": "xx.xx.xx.xx",
  "vasa_provider_credentials": {
    "username": "xxxxx",
    "password": "*****"
  },
  "database_password": "*****"
}'
```

Corpo da solicitação para migração de outra versão:

```
{
  "otv_ip": "xx.xx.xx.xx",
  "vasa_provider_credentials": {
    "username": "xxxxx",
    "password": "*****"
  }
}
```

Exemplo de saída JSON

O sistema retorna um objeto de tarefa. Salve o identificador da tarefa para usá-lo na próxima etapa.


```
{
  "id": 123,
  "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35",
  "status": "running"
}
```

8. Utilize o seguinte URI no Swagger para verificar o status:

```
curl
`https://xx.xx.xx.xxx:8443/virtualization/api/jobmanager/v2/jobs/<JobId
>?includeSubJobsAndTasks=true`
```

Utilize o valor 'id' retornado pela tarefa de migração na etapa anterior. Após a conclusão da tarefa, revise o relatório de migração na resposta da tarefa.

9. Registre o provedor VASA com ONTAP tools for VMware vSphere. Para obter instruções, consulte ["Registre o provedor VASA"](#).
10. Verifique o registro do VASA Provider:
 - a. No vSphere Client, navegue até o vCenter Server.
 - b. Selecione **Configurar > Provedores de armazenamento**.
 - c. Confirme que o VASA Provider registrado na etapa anterior aparece online.
11. Pare o serviço ONTAP tools for VMware vSphere storage provider 9.10/9.11/9.12/9.13 VASA Provider usando estas etapas:
 - a. Nas ONTAP tools 9.x, abra o console da web.
 - b. Acesse o console de manutenção.
 - c. Pressione 1 Enter para selecionar o menu **Configuração do Aplicativo**.
 - d. Digite 5 para interromper os serviços do provedor VASA e do SRA.
 - e. No vSphere Client, navegue até o vCenter Server e selecione **Configurar > Provedores de armazenamento**.
 - f. Selecione o VASA Provider offline para ONTAP tools 9.x e selecione **Remover**.

Após a interrupção do provedor VASA antigo, o vCenter Server realiza o failover para o ONTAP tools for VMware vSphere. Todos os datastores e VMs tornam-se acessíveis e são servidos pelo ONTAP tools for VMware vSphere.

12. Os datastores NFS e VMFS migrados aparecem em ONTAP tools for VMware vSphere 10.5 após a tarefa de descoberta do datastore, que pode levar até 30 minutos. Verifique a visibilidade deles na página de visão geral.
13. Execute a migração de patches usando a seguinte API no Swagger ou no Postman:

Método HTTP e endpoint

Esta chamada à API REST utiliza o seguinte método e endpoint.

Método HTTP	Caminho
PATCH	/api/v1

Tipo de processamento

Assíncrono

Use o seguinte URI no Swagger:

```
curl -X PATCH
`https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/<vcenter_id>/migration-jobs/<migration_id>`
```

Método HTTP e endpoint

Esta chamada à API REST utiliza o seguinte método e endpoint.

Método HTTP	Caminho
PATCH	/api/v1

Tipo de processamento

Assíncrono

Use o seguinte URI no Swagger:

```
curl -X PATCH
`https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/<vcenter_id>/migration-jobs/<migration_id>`
```

Exemplo de curl

```
curl -X PATCH
`https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/56d373bd-4163-44f9-a872-9adabb008ca9/migration-jobs/d50073ce-35b4-4c51-9d2e-4ce66f802c35`
```

Exemplo de saída JSON

```
{
  "id": 123,
  "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35",
  "status": "running"
}
```



Utilize o valor 'migration_id' retornado na Etapa 7 como <migration_id> na chamada da API PATCH. O corpo da requisição está vazio para a operação de patch.



UUID é o UUID de migração retornado em resposta à API post-migrate.

Após a execução da API de migração de patches, todas as VMs estão em conformidade com a política de armazenamento.

O que vem a seguir

Após concluir a migração e registrar ONTAP tools 10.5 no vCenter Server, siga estas etapas:

- Aguarde a conclusão da **Descoberta** e o sistema atualiza automaticamente os certificados em todos os hosts.
- Aguarde antes de iniciar operações de datastore e máquinas virtuais. O tempo de espera depende do número de hosts, datastores e máquinas virtuais. Se você não esperar, poderá ver falhas ocasionais.

Após a atualização, se o estado de conformidade da máquina virtual estiver desatualizado, reapply a política de armazenamento seguindo os passos abaixo:

1. Acesse o datastore e selecione **Resumo > Políticas de armazenamento de VM**.
2. O sistema mostra o status de conformidade em **Conformidade com a política de armazenamento de VM** como **Desatualizado**.
3. Selecione a política de Storage VM e a VM correspondente.
4. Selecione **Aplicar**.
5. O status de conformidade em **Conformidade com a política de armazenamento de VM** é exibido como em conformidade.

Informações relacionadas

- ["Saiba mais sobre ONTAP tools for VMware vSphere 10 RBAC"](#)
- ["Atualize das ONTAP tools for VMware vSphere 10.x para 10.5"](#)

Etapas para atualizar o adaptador de replicação de armazenamento (SRA)

Antes de começar

No plano de recuperação, o site protegido refere-se ao local onde as VMs estão atualmente em execução, enquanto o site de recuperação é onde as VMs serão recuperadas. A interface do appliance VMware Live Site Recovery exibe o estado do plano de recuperação com detalhes sobre os sites protegido e de recuperação. No plano de recuperação, os botões CLEANUP e REPROTECT estão desativados, enquanto os botões TEST e RUN permanecem ativados. Isso indica que o site está preparado para recuperação de dados. Antes de migrar o SRA, verifique se um site está no estado protegido e o outro no estado de recuperação.



Não inicie a migração se o failover tiver sido concluído, mas a re proteção estiver pendente. Certifique-se de que o processo de re proteção seja concluído antes de prosseguir com a migração. Se um failover de teste estiver em andamento, finalize o failover de teste e inicie a migração.

1. Siga estes passos para excluir o adaptador SRA das ONTAP tools para VMware vSphere 9.xx no VMware Site Recovery:
 - a. Vá para a seção **Storage Replication Adapter**.
 - b. No menu de reticências, selecione **Redefinir configuração**.
 - c. No menu de reticências, selecione **Excluir**.
2. Acesse a página de gerenciamento de configuração do VMware Live Site Recovery.
 - a. Vá para a seção **Storage Replication Adapter**.
 - b. No menu de reticências, selecione **Redefinir configuração**.
 - c. No menu de reticências, selecione **Excluir**.
3. Execute estas etapas tanto nos sites de proteção quanto nos de recuperação.
 - a. ["Habilite os serviços do ONTAP tools for VMware vSphere"](#)
 - b. Configure as ONTAP tools for VMware vSphere 10.5 SRA usando as etapas em ["Configure o SRA no appliance VMware Live Site Recovery"](#).
 - c. Na interface VMware Live Site Recovery, execute **Descobrir Arrays** e **Descobrir Dispositivos**. Confirme se os dispositivos são exibidos como antes da migração.

Automatize usando a API REST

Saiba mais sobre a API REST do ONTAP tools

ONTAP tools for VMware vSphere 10 é um conjunto de ferramentas para gerenciamento de ciclo de vida de máquina virtual. Inclui uma API REST robusta que você pode usar como parte dos seus processos de automação.

Fundamentos de serviços web REST

A Transferência de Estado Representacional (REST) é um estilo para a criação de aplicações web distribuídas, incluindo o design de APIs de serviços web. Ela estabelece um conjunto de tecnologias para expor recursos baseados em servidor e gerenciar seus estados.

Recursos e representação de estado

Os recursos são os componentes fundamentais de uma aplicação de serviços web REST. Existem duas tarefas iniciais importantes ao projetar uma API REST:

- Identifique os recursos do sistema ou do servidor
- Defina os estados dos recursos e as operações de transição de estado associadas

Os aplicativos cliente podem exibir e alterar os estados dos recursos por meio de fluxos de mensagens bem definidos.

Mensagens HTTP

O Protocolo de Transferência de Hipertexto (HTTP) é o protocolo usado pelo cliente e pelo servidor de serviços web para trocar mensagens sobre os recursos. Ele segue o modelo CRUD, baseado nas operações genéricas de criar, ler, atualizar e excluir. O protocolo HTTP inclui cabeçalhos de requisição e resposta, bem como códigos de status de resposta.

Formatação de dados JSON

Embora existam diversos formatos de mensagem disponíveis, a opção mais popular é JavaScript Object Notation (JSON). JSON é um padrão do setor para representar estruturas de dados simples em texto sem formatação e é usado para transferir informações de estado que descrevem os recursos e as ações desejadas.

Segurança

A segurança é um aspecto importante de uma API REST. Além do protocolo Transport Layer Security (TLS) usado para proteger o tráfego HTTP na rede, o ONTAP tools for VMware vSphere 10 API REST também utiliza tokens de acesso para autenticação. Você precisa obter um token de acesso e usá-lo em chamadas de API subsequentes.

Suporte para solicitações assíncronas

As ONTAP tools for VMware vSphere 10 API REST executam a maioria das solicitações de forma síncrona, retornando um código de status quando a operação é concluída. Ela também oferece suporte ao processamento assíncrono para tarefas que exigem mais tempo para serem concluídas.

Ambiente do Gerenciador de ferramentas ONTAP

Existem vários aspectos do ambiente do ONTAP tools Manager que você deve considerar.

Máquina virtual

ONTAP tools for VMware vSphere 10 é implantado usando a arquitetura de plug-in remoto do vSphere. O software, incluindo suporte para a API REST, é executado em uma máquina virtual separada.

Endereço IP do ONTAP tools

ONTAP tools for VMware vSphere 10 expõe um único endereço IP que serve como gateway para os recursos da máquina virtual. Você precisa fornecer o endereço durante a configuração inicial e ele é atribuído a um componente interno de balanceamento de carga. O endereço é usado pela interface de usuário do ONTAP tools Manager, assim como para acessar diretamente a página de documentação do Swagger e a API REST.

Duas APIs REST

Além das ONTAP tools for VMware vSphere 10 API REST, o cluster ONTAP possui sua própria API REST. ONTAP tools Manager utiliza a API REST do ONTAP como cliente para executar tarefas relacionadas ao armazenamento. É importante lembrar que essas duas APIs são separadas e distintas. Para mais informações, consulte "[Automação ONTAP](#)".

Detalhes da implementação da API REST das ferramentas ONTAP

Embora o REST estabeleça um conjunto comum de tecnologias e boas práticas, a implementação exata de cada API pode variar de acordo com as escolhas de design. Você deve se familiarizar com como a API REST do ONTAP tools for VMware vSphere 10 foi projetada antes de usá-la.

A API REST inclui diversas categorias de recursos, como vCenters e agregados. Consulte a documentação "[Referência API](#)" para obter mais informações.

Como acessar a API REST

Você pode acessar as ONTAP tools for VMware vSphere 10 API REST através do endereço IP das ONTAP tools junto com a porta. Há várias partes na URL completa, incluindo:

- Endereço IP e porta das ferramentas ONTAP
- Versão API
- Categoria de recurso
- Recurso específico

Você deve configurar o endereço IP durante a configuração inicial, enquanto a porta permanece fixa em 8443. A primeira parte da URL é consistente para cada instância do ONTAP tools for VMware vSphere 10; apenas a categoria do recurso e o recurso específico mudam entre os endpoints.



Os valores de endereço IP e porta nos exemplos abaixo são apenas para fins ilustrativos. Você precisa alterar esses valores para o seu ambiente.

Exemplo de acesso a serviços de autenticação

```
https://10.61.25.34:8443/virtualization/api/v1/auth/login
```

Esta URL pode ser usada para solicitar um token de acesso usando o método POST.

Exemplo para listar os servidores vCenter

<https://10.61.25.34:8443/virtualization/api/v1/vcenters>

Este URL pode ser usado para solicitar uma lista das instâncias de servidor vCenter definidas usando o método GET.

Detalhes HTTP

As ONTAP tools for VMware vSphere 10 API REST usam HTTP e parâmetros relacionados para agir sobre as instâncias e coleções de recursos. Os detalhes da implementação HTTP são apresentados abaixo.

Métodos HTTP

Os métodos ou verbos HTTP suportados pela API REST são apresentados na tabela abaixo.

Método	CRUD	Descrição
GET	Ler	Recupera as propriedades de um objeto para uma instância de recurso ou coleção. Isso é considerado uma operação de listagem quando usado com uma coleção.
POST	Criar	Cria uma nova instância de recurso com base nos parâmetros de entrada.
PUT	Atualizar	Atualiza toda a instância do recurso com o corpo da solicitação JSON fornecido. Os valores-chave que não podem ser modificados pelo usuário são preservados.
PATCH	Atualizar	Solicita que um conjunto de alterações selecionadas na solicitação seja aplicado à instância do recurso.
EXCLUIR	Excluir	Exclui uma instância de recurso existente.

Cabeçalhos de solicitação e resposta

A tabela a seguir resume os cabeçalhos HTTP mais importantes usados com a API REST.

Cabeçalho	Tipo	Notas de uso
Aceitar	Solicitação	Este é o tipo de conteúdo que o aplicativo cliente pode aceitar. Os valores válidos incluem <code>*/*</code> ou <code>application/json</code> .
x-auth	Solicitação	Contém um token de acesso que identifica o usuário que emitiu a solicitação por meio do aplicativo cliente.
Content-Type	Resposta	Retornado pelo servidor com base no <code>Accept</code> cabeçalho da solicitação.

Códigos de status HTTP

Os códigos de status HTTP usados pela API REST são descritos abaixo.

Código	Significado	Descrição
200	OK	Indica sucesso para chamadas que não criam uma nova instância de recurso.

Código	Significado	Descrição
201	Criado	Um objeto foi criado com sucesso com um identificador exclusivo para a instância do recurso.
202	Aceito	A solicitação foi aceita e uma tarefa em segundo plano foi criada para executá-la.
204	Sem conteúdo	A solicitação foi bem-sucedida, embora nenhum conteúdo tenha sido retornado.
400	Pedido ruim	A entrada solicitada não foi reconhecida ou é inadequada.
401	Não autorizado	O usuário não está autorizado e deve se autenticar.
403	Proibido	O acesso foi negado devido a um erro de autorização.
404	Não encontrado	O recurso mencionado na solicitação não existe.
409	Conflito	A tentativa de criar um objeto falhou porque o objeto já existe.
500	Erro interno	Ocorreu um erro interno geral no servidor.

Autenticação

A autenticação de um cliente na API REST é realizada por meio de um token de acesso. As características relevantes do token e do processo de autenticação incluem:

- O cliente deve solicitar um token usando as credenciais de administrador do ONTAP tools Manager (nome de usuário e senha).
- Os tokens são formatados como um JSON Web Token (JWT).
- Cada token expira após 60 minutos.
- As solicitações de API de um cliente devem incluir o token no `x-auth` cabeçalho da solicitação.

Consulte ["Sua primeira chamada à API REST"](#) para um exemplo de como solicitar e usar um token de acesso.

Requisições síncronas e assíncronas

A maioria das chamadas à API REST é concluída rapidamente e, portanto, executada de forma síncrona. Ou seja, elas retornam um código de status (como 200) após a conclusão da solicitação. As solicitações que levam mais tempo para serem concluídas são executadas de forma assíncrona, utilizando uma tarefa em segundo plano.

Após emitir uma chamada de API que é executada de forma assíncrona, o servidor retorna um código de status HTTP 202. Isso indica que a solicitação foi aceita, mas ainda não foi concluída. Você pode consultar a tarefa em segundo plano para determinar seu status, incluindo sucesso ou falha.

O processamento assíncrono é usado para diversos tipos de operações de longa duração, incluindo operações de datastore e vVol. Consulte a categoria job manager da API REST na página do Swagger para mais informações.

Faça sua primeira chamada à API REST das ONTAP tools

Você pode fazer uma chamada de API usando curl para começar a usar o ONTAP tools for VMware vSphere 10 API REST.

Antes de começar

Você deve revisar as informações e os parâmetros necessários nos exemplos do curl.

Informações necessárias

Você precisa do seguinte:

- ONTAP tools for VMware vSphere 10, endereço IP ou domínio totalmente qualificado, assim como a porta
- Credenciais do administrador do ONTAP tools Manager (nome de usuário e senha)

Parâmetros e variáveis

Os exemplos de curl apresentados abaixo incluem variáveis no estilo Bash. Você pode definir essas variáveis no ambiente Bash ou atualizá-las manualmente antes de executar os comandos. Se você definir as variáveis, o shell substituirá os valores em cada comando antes de executá-lo. As variáveis são descritas na tabela abaixo.

Variável	Descrição
\$FQDN_IP_PORT	O nome de domínio totalmente qualificado ou endereço IP do ONTAP tools Manager, juntamente com o número da porta.
\$MYUSER	Nome de usuário para a conta do Gerenciador de ferramentas ONTAP.
\$MYPASSWORD	Senha associada ao nome de usuário do Gerenciador de ferramentas ONTAP.
\$ACCESS_TOKEN	O token de acesso emitido pelo ONTAP tools Manager.

Os comandos e a respectiva saída na linha de comando do Linux ilustram como uma variável pode ser definida e exibida:

```
FQDN_IP_PORT=172.14.31.224:8443
echo $FQDN_IP
172.14.31.224:8443
```

Etapa 1: obtenha um token de acesso

Você precisa obter um token de acesso para usar a API REST. Um exemplo de como solicitar um token de acesso é apresentado abaixo. Você deve substituir os valores apropriados para o seu ambiente.

```
curl --request POST \
--location "https://$FQDN_IP_PORT/virtualization/api/v1/auth/login" \
--header "Content-Type: application/json" \
--header "Accept: */*" \
-d '{"username": "$MYUSER", "password": "$MYPASSWORD"}'
```

Copie e salve o token de acesso fornecido na resposta.

Etapa 2: faça a chamada à API REST

Após obter um token de acesso, você pode usar o curl para fazer uma chamada à API REST. Inclua o token de acesso obtido na primeira etapa.

Exemplo de curl

```
curl --request GET \
--location "https://$FQDN_IP_PORT/virtualization/api/v1/vcenters" \
--header "Accept: */*" \
--header "x-auth: $ACCESS_TOKEN"
```

A resposta JSON inclui uma lista das instâncias do VMware vCenter configuradas no ONTAP tools Manager.

Referência da API REST das ONTAP tools

A referência da API REST das ferramentas ONTAP para VMware vSphere 10 contém detalhes sobre todas as chamadas da API. Essa referência é útil no desenvolvimento de aplicações de automação.

Você pode acessar a documentação da API REST das ONTAP tools for VMware vSphere 10 online através da interface de usuário Swagger. Você precisa do endereço IP ou do domínio totalmente qualificado (FQDN) do serviço de gateway das ONTAP tools for VMware vSphere 10, assim como da porta.

Passos

1. Digite o seguinte URL no seu navegador, substituindo a combinação apropriada de endereço IP e porta pela variável, e pressione **Enter**.

```
https://$FQDN_IP_PORT/
```

Exemplo

```
https://10.61.25.33:8443/
```

2. Como exemplo de uma chamada de API individual, role para baixo até a categoria **vCenters** e selecione **GET** ao lado do endpoint `/virtualization/api/v1/vcenters`

Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e mais.

Direitos autorais

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marcas registradas

NETAPP, o logotipo da NETAPP e as marcas listadas na página de Marcas Registradas da NetApp são marcas registradas da NetApp, Inc. Outros nomes de empresas e produtos podem ser marcas registradas de seus respectivos proprietários.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Patentes

A lista atual de patentes detidas pela NetApp pode ser encontrada em:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Política de privacidade

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

Código aberto

Os arquivos de notificação fornecem informações sobre direitos autorais e licenças de terceiro usados no software NetApp.

["Aviso para ONTAP tools for VMware vSphere 10.5"](#)

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.