



Ferramentas do ONTAP para documentação do VMware vSphere 10,3

ONTAP tools for VMware vSphere 10

NetApp
November 17, 2025

Índice

Ferramentas do ONTAP para documentação do VMware vSphere 10,3	1
Notas de lançamento	2
Notas de lançamento	2
Novidades nas ferramentas do ONTAP para o VMware vSphere 10,3	2
Comparação de recursos das ferramentas do ONTAP para VMware vSphere 9 e ONTAP Tools para VMware vSphere 10	3
Conceitos	5
Visão geral das ferramentas do ONTAP para VMware vSphere	5
Principais conceitos e termos	5
Controle de acesso baseado em função	8
Saiba mais sobre as ferramentas do ONTAP para VMware vSphere 10 RBAC	8
RBAC com VMware vSphere	9
RBAC com ONTAP	13
Alta disponibilidade para ferramentas ONTAP para VMware vSphere	16
AutoSupport	16
Interface de usuário do Gerenciador de ferramentas do ONTAP	17
Implantar as ferramentas do ONTAP para o VMware vSphere	19
Início rápido das ferramentas do ONTAP para VMware vSphere	19
Fluxo de trabalho de implantação de alta disponibilidade (HA)	21
Pré-requisitos para ferramentas do ONTAP para implantação do VMware vSphere	21
Requisitos do sistema	22
Requisitos mínimos de storage e aplicativos	22
Limites de configuração para implantar as ferramentas do ONTAP para o VMware vSphere	22
Ferramentas do ONTAP para VMware vSphere - adaptador de replicação de armazenamento (SRA) ..	23
Requisitos portuários	23
Antes de começar.....	25
Folha de cálculo de implementação	25
Configuração de firewall de rede	26
Implantar as ferramentas do ONTAP para o VMware vSphere	27
Códigos de erro de implantação	29
Configurar as ferramentas do ONTAP para o VMware vSphere	32
Adicione instâncias do vCenter Server	32
Registre o provedor VASA com uma instância do vCenter Server	32
Instale o plug-in NFS VAAI	33
Configure as configurações do host ESXi	34
Configure as configurações multipath e timeout do servidor ESXi	34
Defina os valores do host ESXi	35
Configurar as funções de usuário do ONTAP e o Privileges	36
Requisitos de mapeamento de agregados da SVM	37
Crie manualmente o usuário e a função do ONTAP	37
Atualize as ferramentas do ONTAP para o usuário do VMware vSphere 10,1 para o usuário 10,3	45
Adicionar um back-end de storage	47
Associar um back-end de storage a uma instância do vCenter Server	48

Configurar o acesso à rede	49
Crie um datastore	49
Proteja armazenamentos de dados e máquinas virtuais	54
Proteger usando a proteção do cluster de host	54
Proteja usando proteção SRA	55
Ative o SRA para proteger datastores	55
Configurar o SRA para ambientes SAN e nas	55
Configure o SRA para ambientes altamente dimensionados	56
Configure o SRA no VMware Live Site Recovery Appliance	58
Atualizar credenciais SRA	59
Configurar sites protegidos e de recuperação	59
Configurar recursos do site protegidos e de recuperação	60
Verificar sistemas de storage replicados	64
Gerenciar as ferramentas do ONTAP para VMware vSphere	65
Visão geral das ferramentas do ONTAP para o painel do VMware vSphere	65
Interface de usuário do Gerenciador de ferramentas do ONTAP	67
Entenda igroups e políticas de exportação em ferramentas ONTAP para VMware vSphere	68
Políticas de exportação	72
Habilite as ferramentas do ONTAP para os serviços do VMware vSphere	73
Alterar as ferramentas do ONTAP para a configuração do VMware vSphere	73
Gerenciar armazenamentos de dados	75
Montar armazenamentos de dados NFS e VMFS	75
Desmonte armazenamentos de dados NFS e VMFS	75
Montar um datastore vVols	76
Redimensione o armazenamento de dados NFS e VMFS	76
Expanda o armazenamento de dados vVols	77
Diminua o armazenamento de dados do vVols	77
Excluir datastores	78
Visualizações de storage do ONTAP para datastores	79
Visualização de armazenamento de máquina virtual	79
Gerenciar limites de storage	80
Gerenciar backends de armazenamento	80
Descubra o armazenamento	80
Modificar backends de armazenamento	80
Remova as extremidades de armazenamento	81
Visualização detalhada do back-end de storage	81
Gerenciar instâncias do vCenter Server	82
Dissociar os backends de armazenamento com a instância do vCenter Server	82
Modifique uma instância do vCenter Server	82
Remova uma instância do vCenter Server	83
Gerenciar certificados	83
Acesse as ferramentas do ONTAP para o console de manutenção do VMware vSphere	85
Visão geral das ferramentas do ONTAP para o console de manutenção do VMware vSphere	85
Configure o acesso de diagnóstico remoto	86
Inicie o SSH em outros nós	87

Atualize as credenciais do vCenter Server e do ONTAP	87
Relatórios de ferramentas do ONTAP	87
Recolha os ficheiros de registo	88
Gerenciar máquinas virtuais	88
Considerações para migrar ou clonar máquinas virtuais	89
Migre máquinas virtuais com datastores NFS e VMFS para armazenamentos de dados vVols	90
Limpeza VASA	90
Descubra sistemas de storage e hosts	91
Modifique as configurações do host ESXi usando as ferramentas do ONTAP	91
Gerenciar senhas	92
Alterar a senha do Gerenciador de ferramentas do ONTAP	92
Redefinir a senha do Gerenciador de ferramentas do ONTAP	92
Repor a palavra-passe do utilizador da aplicação	93
Redefinir a senha do usuário do console de manutenção	93
Gerenciar a proteção do cluster de host	94
Modificar cluster de host protegido	94
Remova a proteção do cluster do host	97
Desative o AutoSupport	97
Atualize o URL do proxy do AutoSupport	98
Crie backup e recupere a configuração	98
Criar cópia de segurança e transferir o ficheiro de cópia de segurança	98
Recuperar	99
Desinstale as ferramentas do ONTAP para o VMware vSphere	99
Remover volumes FlexVol	100
Atualize as ferramentas do ONTAP para o VMware vSphere	101
Atualize das ferramentas do ONTAP para o VMware vSphere 10.x para o 10,3	101
Atualizar códigos de erro	105
Migrar as ferramentas do ONTAP para o VMware vSphere 9.xx para o 10,3	109
Migrar das ferramentas do ONTAP para o VMware vSphere 9.xx para o 10,3	109
Migrar o Provedor VASA e atualizar o SRA	109
Etapas para migrar o provedor VASA	109
Etapas para atualizar o adaptador de replicação de armazenamento (SRA)	112
Automatize usando a API REST	114
Saiba mais sobre as ferramentas do ONTAP para a API REST do VMware vSphere 10	114
Base de serviços web REST	114
Ambiente do Gerenciador de ferramentas do ONTAP	114
Detalhes de implementação das ferramentas do ONTAP para a API REST do VMware vSphere 10	115
Como acessar a API REST	115
Detalhes HTTP	116
Autenticação	117
Solicitações síncronas e assíncronas	117
Suas primeiras ferramentas do ONTAP para chamada de API REST do VMware vSphere 10	118
Antes de começar	118
Passo 1: Adquirir um token de acesso	118
Etapa 2: Emita a chamada da API REST	119

Referência de API para as ferramentas do ONTAP para a API REST do VMware vSphere 10	119
Avisos legais	120
Direitos de autor	120
Marcas comerciais	120
Patentes	120
Política de privacidade	120
Código aberto	120

Ferramentas do ONTAP para documentação do VMware vSphere 10,3

Notas de lançamento

Notas de lançamento

Saiba mais sobre os novos e aprimorados recursos disponíveis nas ferramentas do ONTAP para VMware vSphere 10,3.

Para obter uma lista completa de novos recursos e aprimoramentos, [Novidades nas ferramentas do ONTAP para VMware vSphere 10,3](#) consulte .

Para saber mais sobre se a migração das ferramentas do ONTAP para o VMware vSphere 9 para o ONTAP Tools 10,3 é adequada para sua implantação, [Comparação de recursos das ferramentas do ONTAP para VMware vSphere 9 e ONTAP Tools para VMware vSphere 10](#) consulte . A migração é suportada pelas ferramentas do ONTAP para as versões do VMware vSphere 9,12-D e 9,13-D para as ferramentas do ONTAP para VMware vSphere 10,3.

Para obter mais informações, consulte ["Ferramentas do ONTAP para notas de versão do VMware vSphere 10,3"](#) . Você deve entrar com sua conta do NetApp ou criar uma conta para acessar as Notas de versão.

Novidades nas ferramentas do ONTAP para o VMware vSphere 10,3

Saiba mais sobre os novos recursos disponíveis nas ferramentas do ONTAP para VMware vSphere 10,3.

Atualização	Descrição
Suporte para novas versões de plataforma e aplicativos	As ferramentas do ONTAP para VMware vSphere 10,3 agora oferecem suporte a essas versões de plataforma e aplicativos: • ONTAP 9.16,0 e posterior • VMware vSphere 8,0 U3 • VMware Live Site Recovery 9,0
Facilidade de implantação	Agora você pode implantar as ferramentas do ONTAP para o VMware vSphere 10,3 com requisitos mínimos em um cluster de nó único e atualizá-lo para uma implantação de alta disponibilidade (HA) ou vários nós.
Provisionamento e configuração otimizados	As ferramentas do ONTAP para VMware vSphere 10,3 removem as dependências associadas ao Trident e agora usam provisionador de storage dinâmico para permitir o provisionamento e a configuração aprimorados.
Segurança aprimorada para autenticação de API REST	As ferramentas do ONTAP para VMware vSphere 10,3 agora dependem de certificados assinados pela CA para APIs REST e interface de usuário das ferramentas ONTAP para fornecer maior segurança.

Atualização	Descrição
Suporte para sistemas ASA R2	As ferramentas do ONTAP para o VMware vSphere 10,3 oferecem suporte ao provisionamento de armazenamento de dados VMFS em sistemas ASA R2 para ajudar a proteger armazenamentos de dados VMFS com sincronização ativa do SnapMirror e recuperação de site em tempo real SRA/VMware.
Observabilidade aprimorada	As ferramentas do ONTAP para o VMware vSphere 10,3 estendem o suporte a métricas de observação para datastores VMFS e evolução e suas respectivas VMs.

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

Saiba se a migração das ferramentas do ONTAP para o VMware vSphere 9 para as ferramentas do ONTAP para o VMware vSphere 10,1 ou versões posteriores é ideal para você. Para obter as informações de compatibilidade mais atualizadas, ["Ferramenta de Matriz de interoperabilidade do NetApp"](#) consulte .

Recurso	Ferramentas ONTAP 9,13	Ferramentas ONTAP 10,1	Ferramentas ONTAP a partir do modelo do ano 10,2
Proposta de valor chave	Simplifique e simplifique as operações do dia 0 ao dia 2 com recursos aprimorados de segurança, conformidade e automação	Evolução das ferramentas do ONTAP 10.x em direção à paridade 9.x, estendendo os limites de alta disponibilidade, desempenho e escala	Suporte expandido para incluir FC para VMFS e vVols e NVMe-of/FC, NVMe-of/TCP apenas para VMFS. Facilidade de uso para o NetApp SnapMirror, configuração simples para clusters de armazenamento do vSphere metro e suporte para recuperação de site em tempo real em três locais
Qualificação de lançamento do ONTAP	ONTAP 9.9,1 para ONTAP 9.15,1	ONTAP 9.12,1 para ONTAP 9.14,1	ONTAP 9.12.1 para ONTAP 9.15.1 para ferramentas ONTAP 10,2 ONTAP 9.14.1, 9.15.1 e 9.16.0 para ferramentas ONTAP 10,3.
Suporte ao lançamento 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 VMware Site Recovery Manager (SRM) 8,7 para VMware Live Site Recovery 9,0	VSphere 7.x-8.x VMware Site Recovery Manager (SRM) 8,7 para VMware Live Site Recovery 9,0

Recurso	Ferramentas ONTAP 9,13	Ferramentas ONTAP 10,1	Ferramentas ONTAP a partir do modelo do ano 10,2
Suporte ao protocolo	Armazenamentos de dados NFS e VMFS: Armazenamentos de dados vVols NFS (v3 e v4,1), VMFS (iSCSI e FCP): iSCSI, FCP, NVMe/FC, NFS v3	Armazenamentos de dados NFS e VMFS: Armazenamentos de dados NFS (v3 e v4,1), VMFS (iSCSI) vVols: iSCSI, NFS v3	Armazenamentos de dados NFS e VMFS: Armazenamentos de dados vVols NFS (v3 e v4,1), VMFS (iSCSI/FCP/NVMe-of): iSCSI, FCP, NFS v3
Escalabilidade	Hosts e VMs: 300 hosts, até 10K armazenamentos de dados de VMs: 600 NFS, até 50 VMFS, até 250 vVols vVols: Até 14.000 TB	Hosts e VMs: 600 hosts vVols: Até 140.000	Hosts e VMs: 600 hosts vVols: Até 140.000
Observabilidade	Relatórios dinâmicos de VM e armazenamento de dados, além de dashboards de conformidade de host, capacidade e performance	Relatórios dinâmicos de VM e armazenamento de dados atualizados sobre performance, capacidade e conformidade do host	Relatórios dinâmicos de VM e armazenamento de dados atualizados sobre performance, capacidade e conformidade do host
Proteção de dados	Replicação SRA para replicação baseada em VMFS e NFS FlexVols para integração de VCS vVols e interoperável para backup	Replicação SRA para armazenamentos de dados iSCSI VMFS e NFS v3	A replicação SRA para iSCSI VMFS e NFS v3 armazenamentos de dados de três locais de proteção combinando SMAS e VMware Live Site Recovery.
Suporte ao VASA Provider	VASA 4,0	VASA 3,0	VASA 3,0

Conceitos

Visão geral das ferramentas do ONTAP para VMware vSphere

As ferramentas do ONTAP para VMware vSphere são um conjunto de ferramentas para o gerenciamento do ciclo de vida da máquina virtual. Ele se integra ao ecossistema VMware para ajudar no provisionamento de armazenamento de dados e no fornecimento de proteção básica para máquinas virtuais.

As ferramentas do ONTAP para VMware vSphere são uma coleção de microsserviços horizontalmente escaláveis, orientados a eventos, implantados como um dispositivo virtual aberto (OVA). Esta versão tem integração com API REST com o ONTAP.

As ferramentas do ONTAP para VMware vSphere consistem em:

- Funcionalidade de máquina virtual, como proteção básica e recuperação de desastres
- FORNECEDOR VASA para gerenciamento granular de VM
- Gerenciamento baseado em política de storage
- Adaptador de replicação de armazenamento (SRA)
- SnapMirror ativo Sync (SMAS)

Principais conceitos e termos

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

Sistemas ASA r2

Os novos sistemas NetApp ASA R2 fornecem uma solução unificada de hardware e software que cria uma experiência simplificada específica para as necessidades dos clientes somente de SAN. ["Saiba mais sobre os sistemas de armazenamento ASA R2"](#).

Autoridade de certificação (CA)

A CA é uma entidade confiável que emite certificados SSL (Secure Sockets Layer).

Grupo de consistência

Um grupo de consistência é uma coleção de volumes que são gerenciados como uma única unidade. No ONTAP, os grupos de consistência fornecem gerenciamento fácil e uma garantia de proteção para um workload de aplicações que abrange vários volumes. Saiba mais ["grupo de consistência"](#) sobre o .

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 de cluster são configurados em pares de HA para operações sem interrupções.

Número de unidade lógica (LUN)

Um 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 através do protocolo SCSI (Small Computer System Interface) ou de 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 protocolos FC e iSCSI, e um subsistema NVMe é análogo a um iggroup. Um subsistema NVMe pode ser associado a iniciadores para que os namespaces dentro do subsistema possam ser acessados pelos iniciadores associados.

Gerenciador de ferramentas do ONTAP

O Gerenciador de ferramentas do ONTAP fornece mais controle às ferramentas do ONTAP para o administrador do VMware vSphere sobre as instâncias gerenciadas do vCenter Server e os back-ends de storage integrados. O Gerenciador de ferramentas do ONTAP ajuda no gerenciamento de instâncias do vCenter Server, backends de armazenamento, certificados, senhas e downloads de pacotes de log.

Abrir dispositivo virtual (OVA)

O OVA é um padrão aberto para empacotar e distribuir dispositivos virtuais ou software que deve ser executado em máquinas virtuais.

Objetivo do ponto de recuperação (RPO)

RPO é uma medida da frequência com que o backup ou a replicação dos dados. Ele representa o ponto no tempo para o qual os dados devem ser recuperados após uma interrupção para retomar as operações de negócios. Por exemplo, se uma organização tiver um RPO de 4 horas, poderá tolerar a perda de até 4 horas de dados em caso de desastre.

SnapMirror ativo Sync (SMAS)

O SnapMirror active Sync permite que os serviços empresariais continuem operando mesmo em uma falha completa do local, com suporte ao failover de aplicações de forma transparente, usando uma cópia secundária. A intervenção manual nem o script personalizado são necessários para acionar um failover com a sincronização ativa do SnapMirror. Lear mais sobre ["Sincronização ativa do SnapMirror"](#).

Back-ends de armazenamento

Os backends de armazenamento são a infraestrutura de armazenamento subjacente que o host ESXi usa para armazenar arquivos de máquina virtual, dados e outros recursos. O back-end de armazenamento permite que o host ESXi acesse e gerencie dados persistentes, fornecendo a capacidade de armazenamento e o desempenho necessários para o ambiente virtualizado.

Adaptador de replicação de armazenamento (SRA)

O SRA é o software específico do fornecedor de storage instalado no dispositivo VMware Live Site Recovery. O adaptador permite a comunicação entre o Site Recovery Manager e uma controladora de storage no nível

de Storage Virtual Machine (SVM) e a configuração no nível do cluster.

Máquina virtual de storage (SVM)

Como uma máquina virtual em execução em um hipervisor, a SVM é uma entidade lógica que abstrai recursos físicos. O SVM contém volumes de dados e uma ou mais LIFs por meio dos quais eles fornecem dados aos clientes.

Configuração uniforme e não uniforme

- **Acesso uniforme ao host** significa que os hosts de ambos os sites estão conectados a todos os caminhos para os clusters de armazenamento em ambos os sites. Os caminhos entre os locais são estendidos ao longo da distância.
- **Acesso não uniforme ao host** significa que os hosts em cada site estão conectados apenas ao cluster no mesmo site. Caminhos entre locais e caminhos esticados não estão conectados.



O acesso uniforme de host é compatível com qualquer implantação de sincronização ativa do SnapMirror. O acesso de host não uniforme só é compatível com implantações ativas/ativas simétricas.

Sistema de arquivos de máquina virtual (VMFS)

O VMFS é um sistema de arquivos em cluster projetado especificamente para armazenar arquivos de máquina virtual em ambientes VMware vSphere.

Volumes virtuais (vVols)

Os vVols fornecem uma abstração em nível de volume para armazenamento usado por uma máquina virtual. Ele inclui vários benefícios e fornece uma alternativa ao uso de um LUN tradicional. Um datastore da VVol é normalmente associado a um único LUN que atua como um contêntor para os vVols.

Política de storage da VM

As políticas de armazenamento de VM são criadas no vCenter Server em políticas e perfis. Para vVols, crie um conjunto de regras usando regras do provedor do tipo de storage do NetApp vVols.

Recuperação do VMware Live Site

O VMware Live Site Recovery oferece continuidade dos negócios, recuperação de desastres, migração de sites e recursos de teste sem interrupções para ambientes virtuais VMware.

VMware vSphere APIs for Storage Awareness (VASA)

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

VMware vSphere Storage APIs - Array Integration (VAAI)

O VAAI é um conjunto de APIs que permite a comunicação entre os hosts do VMware vSphere ESXi e os dispositivos de armazenamento. As APIs incluem um conjunto de operações primitivas usadas pelos hosts para descarregar operações de storage para o array. O VAAI pode fornecer melhorias significativas de desempenho para tarefas com uso intenso de storage.

Cluster de armazenamento vSphere Metro

O vSphere Metro Storage Cluster (vmsc) é uma tecnologia que permite e suporta o vSphere em uma implantação de cluster estendida. As soluções vmsc são compatíveis com o NetApp MetroCluster e o SnapMirror ativo Sync (anteriormente SMBC). Essas soluções fornecem continuidade de negócios aprimorada em caso de falha de domínio. O modelo de resiliência é baseado em suas escolhas de configuração específicas. Saiba mais "[Cluster de armazenamento do VMware vSphere Metro](#)" sobre o .

Armazenamento de dados vVols

O datastore vVols é uma representação lógica do datastore de um contentor vVols que é criado e mantido por um provedor VASA.

RPO zero

RPO significa objetivo do ponto de restauração, que é a quantidade de perda de dados considerada aceitável durante um determinado tempo. Zero RPO significa que nenhuma perda de dados é aceitável.

Controle de acesso baseado em função

Saiba mais sobre as ferramentas do ONTAP para VMware vSphere 10 RBAC

O controle de acesso baseado em função (RBAC) é uma estrutura de segurança para controlar o acesso a recursos dentro de uma organização. O RBAC simplifica a administração definindo 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 erros e simplifica o gerenciamento do controle de acesso em toda a organização.

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

Componentes RBAC

Em alto nível, existem vários componentes que geralmente são incluídos em cada implementação do RBAC. Estes componentes estão ligados de diferentes formas como parte da definição dos processos de autorização.

Privileges

Um *privilegio* é uma ação ou capacidade que pode ser permitida ou negada. Pode ser algo simples, como a capacidade de ler um arquivo ou pode ser uma operação mais abstrata específica para um determinado sistema de software. O Privileges também pode ser definido para restringir o acesso a endpoints de API REST e comandos CLI. Cada implementação do RBAC inclui Privileges pré-definido e também pode permitir que os administradores criem Privileges personalizados.

Funções

Um *role* é um contentor que inclui um ou mais Privileges. As funções são geralmente definidas com base em tarefas específicas ou funções de trabalho. Quando uma função é atribuída a um usuário, o usuário recebe todos os Privileges contidos na função. E, como acontece com o Privileges, as implementações incluem funções pré-definidas e geralmente permitem que funções personalizadas sejam criadas.

Objetos

Um *objeto* representa um recurso real ou abstrato identificado no ambiente RBAC. As ações definidas através do Privileges são executadas em ou com os objetos associados. Dependendo da implementação, o Privileges pode ser concedido a um tipo de objeto ou a uma instância de objeto específica.

Usuários e grupos

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

Permissões

A *permission* é uma definição que liga um usuário ou grupo junto com uma função a um objeto. As permissões podem ser úteis com um modelo de objeto hierárquico onde podem ser herdadas opcionalmente pelos filhos na hierarquia.

Dois ambientes RBAC

Há dois ambientes RBAC distintos que você precisa considerar ao trabalhar com as ferramentas do ONTAP para VMware vSphere 10.

VMware vCenter Server

A implementação RBAC no VMware vCenter Server é usada para restringir o acesso a objetos expostos por meio da interface de usuário do vSphere Client. Como parte da instalação das ferramentas do ONTAP para VMware vSphere 10, o ambiente RBAC é estendido para incluir objetos adicionais que representam os recursos das ferramentas do ONTAP. O acesso a esses objetos é fornecido através do plug-in remoto. Consulte "[Ambiente RBAC do vCenter Server](#)" para obter mais informações.

Cluster DE ONTAP

As ferramentas do ONTAP para VMware vSphere 10 se conectam a um cluster do 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 do ONTAP fornecida durante a autenticação. Consulte "[Ambiente RBAC do ONTAP](#)" para obter mais informações.

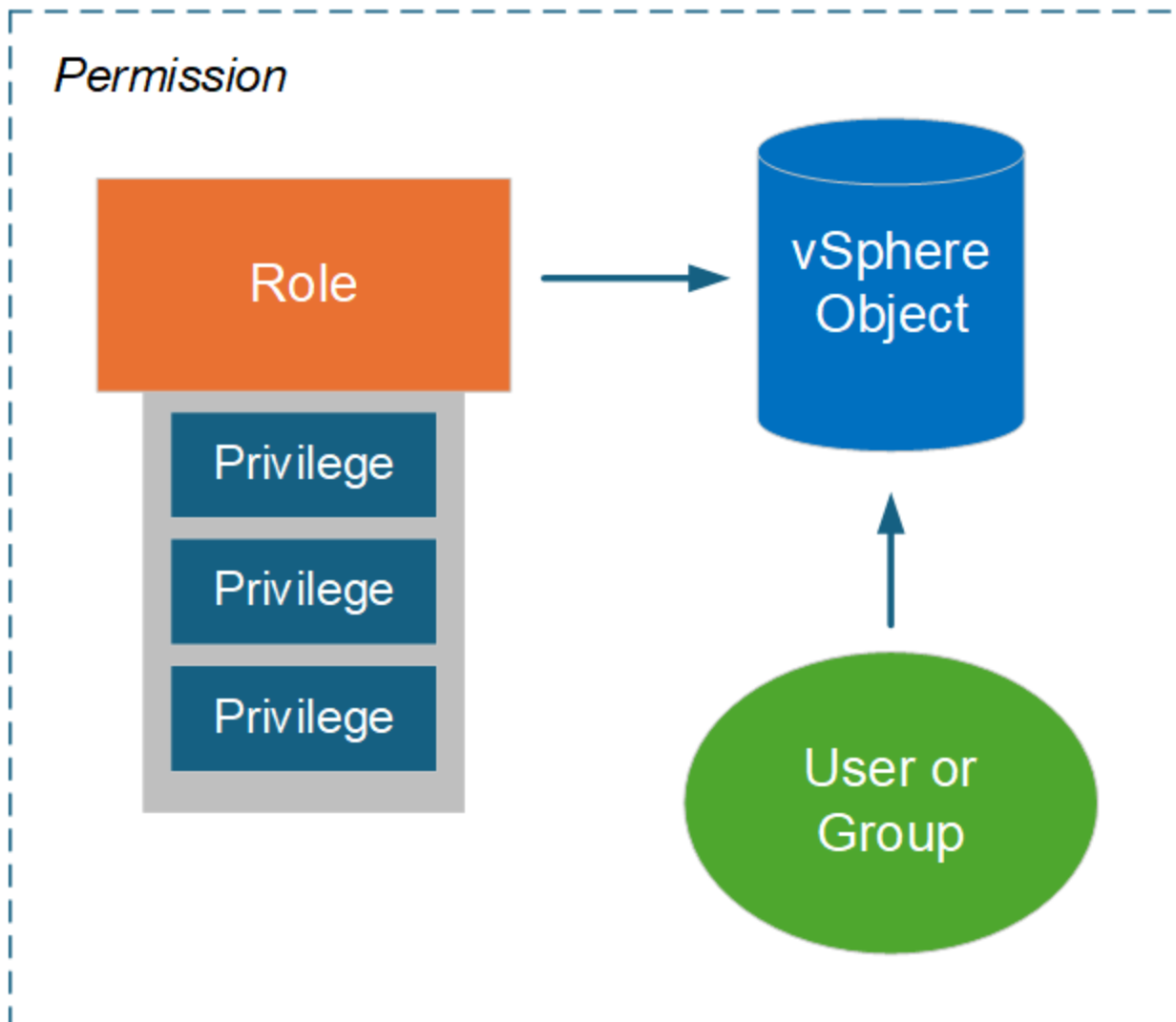
RBAC com VMware vSphere

Ambiente RBAC do vCenter Server com ferramentas do ONTAP para VMware vSphere 10

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

Ilustração de uma permissão do vCenter Server

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



Componentes de uma permissão do vCenter Server

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

Objetos vSphere

As permissões são associadas a objetos vSphere, como 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 ferramentas do ONTAP para VMware vSphere, todas as permissões são atribuídas e validadas no nível da pasta raiz ou raiz do vCenter Server. Consulte ["Use o RBAC com o vCenter Server"](#) para obter mais informações.

Privileges e funções

Há dois tipos de vSphere Privileges usados com as ferramentas do ONTAP para VMware vSphere 10. Para simplificar o trabalho com o RBAC nesse ambiente, as ferramentas do ONTAP fornecem funções que contêm o Privileges personalizado e nativo necessário. Os Privileges incluem:

- Privileges nativo do vCenter Server

Estes são os Privileges fornecidos pelo vCenter Server.

- Privileges específico de ferramentas do ONTAP

Esses são Privileges personalizados exclusivos das ferramentas do ONTAP para 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 no Privilege na função associada. Observe que as funções não são atribuídas diretamente aos usuários isoladamente. Em vez disso, usuários e grupos obtêm acesso a um objeto por meio do Role Privilege como parte da permissão maior do vCenter Server.

Use o RBAC do vCenter Server com as ferramentas do ONTAP para VMware vSphere 10

Há vários aspectos das ferramentas do ONTAP para a implementação do RBAC do VMware vSphere 10 com o vCenter Server que você deve considerar antes de usá-lo em um ambiente de produção.

Funções do vCenter e a conta de administrador

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

Hierarquia de objetos do vSphere

O inventário de objetos do vSphere é organizado em uma hierarquia. Por exemplo, você pode mover para baixo a hierarquia da seguinte forma:

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

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

Funções incluídas nas ferramentas do ONTAP para VMware vSphere 10

Para simplificar o trabalho com o vCenter Server RBAC, as ferramentas do ONTAP para VMware vSphere fornecem funções predefinidas adaptadas a várias tarefas de administração.



Você pode criar novas funções personalizadas, se necessário. Nesse caso, você deve clonar uma das funções existentes das ferramentas do ONTAP e editá-la conforme necessário. Depois de fazer as alterações de configuração, os usuários do cliente vSphere afetados precisam fazer logout e fazer login novamente para ativar as alterações.

Para exibir as ferramentas do ONTAP para as funções do VMware vSphere, selecione **Menu** na parte superior do vSphere Client e clique em **Administration** e depois em **Roles** à esquerda. Existem três funções predefinidas, conforme descrito abaixo.

Ferramentas do NetApp ONTAP para o administrador do VMware vSphere

Fornece todas as ferramentas nativas do vCenter Server Privileges e do ONTAP específicas Privileges necessárias para executar as principais ferramentas do ONTAP para tarefas de administrador do VMware vSphere.

Ferramentas do NetApp ONTAP para VMware vSphere somente leitura

Fornece acesso somente leitura às ferramentas do ONTAP. Esses usuários não podem executar nenhuma ferramenta do ONTAP para ações do VMware vSphere controladas por acesso.

Ferramentas do NetApp ONTAP para o provisionamento do VMware vSphere

Fornece algumas das Privileges nativas específicas das ferramentas do vCenter Server Privileges e do ONTAP necessárias para provisionar o storage. Você pode executar as seguintes tarefas:

- Crie novos datastores
- Gerenciar armazenamentos de dados

Back-ends de armazenamento de objetos vSphere e ONTAP

Os dois ambientes RBAC funcionam em conjunto. Ao executar uma tarefa na interface do cliente vSphere, as funções de ferramentas do ONTAP definidas para o vCenter Server são verificadas primeiro. Se a operação for permitida pelo vSphere, o ONTAP Role Privileges será examinado. Esta segunda etapa é executada com base na função ONTAP atribuída ao usuário quando o back-end de storage foi criado e configurado.

Trabalhando com o vCenter Server RBAC

Há algumas coisas a considerar ao trabalhar com o vCenter Server Privileges e as permissões.

Privileges necessário

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

O nível de atribuição na hierarquia de objetos vSphere determina quais partes da interface de usuário você pode acessar. A atribuição do privilégio *Exibir* ao objeto raiz permite que você acesse as ferramentas do ONTAP para VMware vSphere clicando no ícone NetApp.

Em vez disso, você pode atribuir o privilégio *Exibir* a outro nível de objeto vSphere inferior. No entanto, isso limitará as ferramentas do ONTAP para os menus do VMware vSphere que você pode acessar e usar.

Atribuindo permissões

Você precisa usar as permissões do vCenter Server se quiser limitar o acesso aos objetos e tarefas do vSphere. Quando você atribui permissão na hierarquia de objetos do vSphere determina as ferramentas do ONTAP para 10 as tarefas que 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 as ferramentas do ONTAP para VMware vSphere 10 se aplicam a objetos personalizados que não sejam do vSphere, como sistemas de storage. Se possível, você deve atribuir essas permissões a ferramentas do ONTAP para o objeto raiz do VMware vSphere porque não há nenhum objeto

vSphere ao qual você possa atribuí-lo. Por exemplo, qualquer permissão que inclua um privilégio "Adicionar/Modificar/Remover sistemas de armazenamento" do ONTAP vSphere deve ser atribuída no nível do objeto raiz.

Ao definir uma permissão em um nível mais alto na hierarquia de objetos, você pode configurar a permissão para que ela seja passada e herdada pelos objetos filho. Se necessário, você pode atribuir permissões adicionais aos objetos filho que substituem as permissões herdadas do pai.

Você pode modificar uma permissão a qualquer momento. Se você alterar qualquer um dos Privileges dentro de uma permissão, os usuários associados à permissão precisarão fazer logout do vSphere e fazer login novamente para ativar a alteração.

RBAC com ONTAP

Ambiente RBAC do ONTAP com ferramentas ONTAP para VMware vSphere 10

O ONTAP fornece um ambiente RBAC robusto e extensível. Use a funcionalidade RBAC para controlar o acesso ao storage e às operações do sistema conforme exposto pela API REST e CLI. É útil estar familiarizado com o ambiente antes de usá-lo com as ferramentas do ONTAP para a implantação do VMware vSphere 10.

Visão geral das opções administrativas

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



O ONTAP RBAC é personalizado para um ambiente de storage e é mais simples do que a implementação do RBAC fornecida com o vCenter Server. Com o 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 papéis e Privileges

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

- DESCANSO

As funções REST foram introduzidas com o ONTAP 9.6 e geralmente são aplicadas aos usuários que acessam o ONTAP por meio da API REST. Os Privileges incluídos nessas funções são definidos em termos de acesso aos endpoints da API REST do ONTAP e às ações associadas.

- Tradicional

Estas são as funções herdadas incluídas antes do ONTAP 9.6. Eles continuam sendo um aspecto fundamental da RBAC. Os Privileges são definidos em termos de acesso aos comandos da CLI do ONTAP.

Embora os papéis RESTANTES tenham sido introduzidos mais recentemente, os papéis tradicionais têm algumas vantagens. Por exemplo, parâmetros de consulta adicionais podem ser opcionalmente incluídos para que o Privileges defina com mais precisão os objetos aos quais são aplicados.

Âmbito de aplicação

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

Definições de função

O ONTAP fornece um conjunto de funções pré-definidas no nível do cluster e da SVM. Você também pode definir funções personalizadas.

Trabalhando com as funções REST do ONTAP

Há várias considerações ao usar as funções REST do ONTAP incluídas nas ferramentas do ONTAP para VMware vSphere 10.

Mapeamento de funções

Seja usando uma função tradicional ou REST, todas as decisões de acesso ao ONTAP são tomadas com base no comando CLI subjacente. Mas como os Privileges 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 mapeia para um papel tradicional subjacente. Isso permite que o ONTAP tome decisões de controle de acesso de forma consistente, independentemente do tipo de função. Não é possível modificar as funções mapeadas paralelas.

Definindo uma FUNÇÃO REST usando CLI Privileges

Como o ONTAP sempre usa os comandos CLI para determinar o acesso em um nível básico, é possível expressar uma FUNÇÃO REST usando o comando CLI Privileges 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 e a API REST do ONTAP. No entanto, é mais conveniente usar a interface do Gerenciador do sistema juntamente com o arquivo JSON disponível através do Gerenciador de ferramentas do ONTAP. Consulte ["Use o RBAC do ONTAP com as ferramentas do ONTAP para VMware vSphere 10"](#) para obter mais informações.

Use o RBAC do ONTAP com as ferramentas do ONTAP para VMware vSphere 10

Há vários aspectos das ferramentas do ONTAP para a implementação do RBAC do VMware vSphere 10 com o ONTAP que você deve considerar antes de usá-lo em um ambiente de produção.

Visão geral do processo de configuração

As ferramentas do ONTAP para VMware vSphere 10 incluem suporte para criar um usuário do ONTAP com uma função personalizada. As definições são empacotadas em um arquivo JSON que você pode carregar para o cluster ONTAP. Você pode criar o usuário e adaptar a função para suas necessidades de ambiente e segurança.

Os principais passos de configuração são descritos em um nível alto abaixo. ["Configurar as funções de usuário do ONTAP e o Privileges"](#) Consulte para obter mais detalhes.

1. Prepare-se

Você precisa ter credenciais administrativas para o Gerenciador de ferramentas do ONTAP e para o cluster do ONTAP.

2. Baixe o arquivo de definição JSON

Depois de fazer login na interface de usuário do Gerenciador de ferramentas do ONTAP, você pode baixar o

arquivo JSON contendo as definições RBAC.

3. Crie um usuário do ONTAP com uma função

Depois de iniciar sessão no System Manager, pode criar o utilizador e a função:

1. Selecione **Cluster** à esquerda e, em seguida, **Settings**.
2. Role para baixo até **usuários e funções** e clique `→` em .
3. Selecione **Adicionar** em **usuários** e selecione **Produtos de virtualização**.
4. Selecione o arquivo JSON em sua estação de trabalho local e carregue-o.

4. Configure a função

Como parte da definição do papel, você precisa tomar várias decisões administrativas. [Configure a função usando o System Manager](#) Consulte para obter mais detalhes.

Configure a função usando o System Manager

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

Configuração principal do usuário e da função

As definições RBAC são empacotadas como várias capacidades de produto, incluindo combinações de VSC, VSA Provider e SRA. Você deve selecionar o ambiente ou os ambientes em que precisa de suporte a RBAC. Por exemplo, se você quiser que as funções suportem o recurso de plug-in remoto, selecione VSC. Você também precisa escolher o nome de usuário e a senha associada.

Privileges

As Privileges de função são organizadas em quatro conjuntos com base no nível de acesso necessário ao storage ONTAP. Os Privileges em que as funções são baseadas incluem:

- Detecção

Essa função permite adicionar sistemas de storage.

- Crie armazenamento

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

- Modificar o armazenamento

Essa função permite modificar o armazenamento. Ele também inclui todos os Privileges associados à descoberta e criação de funções de storage.

- Destrua o armazenamento

Esta função permite que você destrua o armazenamento. Ele também inclui todos os Privileges associados à descoberta, criação de storage e modificação de funções de storage.

Gere o usuário com uma função

Depois de selecionar as opções de configuração para o seu ambiente, clique em **Adicionar** e o 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")
- Capacidade do produto selecionada
- 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.

Alta disponibilidade para ferramentas ONTAP para VMware vSphere

As ferramentas do ONTAP para VMware vSphere oferecem suporte a uma configuração de alta disponibilidade (HA) para ajudar a fornecer funcionalidade ininterrupta das ferramentas do ONTAP para VMware vSphere durante a falha.

A solução de alta disponibilidade (HA) oferece recuperação rápida de interrupções causadas por:

- Falha do host



Apenas é suportada uma falha de nó único.

- Falha de rede
- Falha da máquina virtual (falha do sistema operacional convidado)
- Falha na aplicação (ferramentas ONTAP)

Nenhuma configuração adicional é necessária para que as ferramentas do ONTAP para VMware vSphere forneçam alta disponibilidade (HA).



As ferramentas do ONTAP para VMware vSphere não são compatíveis com o vCenter HA.

Para habilitar o recurso HA, o hot add e o hot plug de memória da CPU devem ser ativados durante a implantação ou posteriormente nas ferramentas do ONTAP para as configurações de VM do VMware vSphere.

AutoSupport

O AutoSupport é um mecanismo que monitora proativamente a integridade do sistema e envia mensagens automaticamente para o suporte técnico da NetApp, sua organização de suporte interno e um parceiro de suporte.

O AutoSupport é ativado por padrão quando você configura o sistema de storage pela primeira vez. O AutoSupport começa a enviar mensagens para o suporte técnico 24 horas após a ativação do AutoSupport.

Você pode desativar o AutoSupport usando a opção do console de manutenção **Configuração do aplicativo > Desativar o AutoSupport**. Recomenda-se que o deixe ativado. Ativar o AutoSupport ajuda a acelerar a

deteção de problemas e ajuda a alcançar uma resolução mais rápida. O sistema coleta informações do AutoSupport e as armazena localmente, mesmo quando o AutoSupport está desativado. No entanto, ele não envia o relatório para nenhuma rede. Você precisa fornecer o url do proxy usando o console de manutenção da primeira VM. Use a opção **Configuração do aplicativo > Atualizar URL do proxy AutoSupport** para inserir o URL do proxy.

Interface de usuário do Gerenciador de ferramentas do ONTAP

As ferramentas do ONTAP para VMware vSphere são um sistema de alocação a vários clientes que pode gerenciar várias instâncias do vCenter Server. O Gerenciador de ferramentas do ONTAP fornece mais controle às ferramentas do ONTAP para o administrador do VMware vSphere sobre as instâncias gerenciadas do vCenter Server e os back-ends de storage integrados.

O Gerenciador de ferramentas do ONTAP ajuda a:

- Gerenciamento de instâncias do vCenter Server - Adicione e gerencie instâncias do vCenter Server às ferramentas do ONTAP.
- Gerenciamento de back-end de storage: Adicione e gerencie clusters de storage do ONTAP às ferramentas do ONTAP para VMware vSphere e mapeie-os para instâncias integradas do vCenter Server globalmente.
- Downloads do pacote de log - coletar arquivos de log para as ferramentas do ONTAP para VMware vSphere.
- Gerenciamento de certificados - altere o certificado auto-assinado para um certificado CA personalizado e renove ou atualize todos os certificados do provedor VASA e das ferramentas do ONTAP.
- Gerenciamento de senhas - Redefina a senha do aplicativo OVA do usuário.

Para acessar o Gerenciador de ferramentas do ONTAP, inicie a

<https://<ONTAPtoolsIP>:8443/virtualization/ui/> partir do navegador e faça login com as ferramentas do ONTAP para as credenciais de administrador do VMware vSphere fornecidas durante a implantação.

A seção de visão geral do Gerenciador de ferramentas do ONTAP ajuda a gerenciar a configuração do dispositivo, como gerenciamento de serviços, aumento do tamanho dos nós e capacitação de alta disponibilidade (HA). Você também pode monitorar as informações gerais das ferramentas do ONTAP relacionadas aos nós, como integridade, detalhes da rede e alertas.

ONTAP tools Manager

Administrator

- Overview
- Alerts
- Jobs
- Storage backends
- vCenters
- Log bundles
- Certificates
- Settings

Overview

EDIT APPLIANCE SETTINGS

Appliance

Size: Small
HA: Enabled
VASA provider: Enabled
SRA: Enabled

VIEW DETAILS

Alerts

Last 24 hours

3
Error

2
Warning

5
Info

VIEW ALL ALERTS (43)

ONTAP tools nodes

nodename_01
Online
demo_vm1

VIEW DETAILS

nodename_02
Online
demo_vm2

VIEW DETAILS

nodename_03
Online
demo_vm3

VIEW DETAILS

Cartão	Descrição
Cartão do aparelho	O cartão de dispositivo fornece o status geral do dispositivo ONTAP Tools. Ele mostra os detalhes de configuração do dispositivo e o status dos serviços habilitados. Para obter informações adicionais sobre o dispositivo ONTAP Tools, selecione o link Exibir detalhes . Quando um trabalho de ação de configuração de dispositivo de edição está em andamento, o portlet do dispositivo mostra o status e os detalhes do trabalho.
Cartão de alertas	A placa Alertas lista os alertas das ferramentas do ONTAP por tipo, incluindo os alertas no nível do nó de HA. Pode ver a lista de alertas selecionando no texto de contagem (hiperligação). A ligação encaminha-o para a página de visualização de alertas filtrada pelo tipo selecionado.
Placa de nós de ferramentas do ONTAP	A placa de nós de ferramentas do ONTAP mostra a lista de nós com nome do nó, nome da VM do nó, status e todos os dados relacionados à rede. Você pode selecionar em Exibir detalhes para exibir os detalhes adicionais relacionados ao nó selecionado. [NOTA] em uma configuração que não seja de HA, somente um nó é exibido. Na configuração de HA, três nós são mostrados.

Implantar as ferramentas do ONTAP para o VMware vSphere

Início rápido das ferramentas do ONTAP para VMware vSphere

Os primeiros passos com as ferramentas do ONTAP para VMware vSphere incluem algumas etapas. Esse início rápido leva você pela configuração inicial das ferramentas do ONTAP para o VMware vSphere.

Inicialmente, você implantará as ferramentas do ONTAP para o VMware vSphere como uma configuração de nó único de pequeno porte que fornece serviços essenciais para dar suporte a armazenamentos de dados NFS e VMFS. Se você precisar expandir sua configuração para usar o armazenamento de dados vVols e a alta disponibilidade (HA), você fará isso depois de concluir esse fluxo de trabalho. Para obter mais informações, consulte o ["Fluxo de trabalho DE IMPLANTAÇÃO DE HA"](#).

1

Planeje sua implantação

Verifique se as versões do host vSphere, ONTAP e ESXi são compatíveis com a versão das ferramentas do ONTAP. Alocar CPU, memória e espaço em disco suficientes. Dependendo das suas políticas de segurança, pode ser necessário configurar firewalls ou outros dispositivos de segurança para permitir o tráfego de rede.

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

- ["Ferramenta de Matriz de interoperabilidade"](#)
- ["Pré-requisitos para ferramentas do ONTAP para implantação do VMware vSphere"](#)
- ["Antes de começar"](#)

2

Implantar as ferramentas do ONTAP para o VMware vSphere

Inicialmente, você implantará as ferramentas do ONTAP para o VMware vSphere como uma configuração de nó único de pequeno porte que fornece serviços essenciais para dar suporte a armazenamentos de dados NFS e VMFS. Se você planeja expandir sua configuração para usar armazenamentos de dados vVols e alta disponibilidade (HA), você fará isso depois de concluir esse fluxo de trabalho. Para expandir com êxito para uma configuração de HA, você deve garantir que as opções de hot-add e hot-plug de memória da CPU estejam ativadas.

- ["Implantar as ferramentas do ONTAP para o VMware vSphere"](#)

3

Adicione instâncias do vCenter Server

Adicione uma ou mais instâncias do vCenter Server às ferramentas do ONTAP para o VMware vSphere para configurar, gerenciar e proteger seus datastores virtuais no ambiente do vCenter Server.

- ["Adicione instâncias do vCenter Server"](#)

4

Configurar as funções de usuário do ONTAP e o Privileges

Configure novas funções de usuário e o Privileges para gerenciar backends de storage usando o arquivo JSON fornecido com as ferramentas do ONTAP para VMware vSphere.

- ["Configurar as funções de usuário do ONTAP e o Privileges"](#)

5

Configure os backends de armazenamento

Adicionar um back-end de storage a um cluster do ONTAP. Para configurações de alocação a vários clientes em que o vCenter atua como locatário de um SVM associado, use o Gerenciador de ferramentas do ONTAP para adicionar o cluster. Associe o back-end de storage ao vCenter Server para mapeá-lo globalmente para a instância integrada do vCenter Server.

Adicione os back-ends de storage local com credenciais de cluster ou SVM usando a interface de usuário das ferramentas do ONTAP. Esses backends de armazenamento estão limitados a um único vCenter. Ao usar credenciais de cluster localmente, os SVMs associados mapeiam automaticamente para o vCenter para gerenciar vVols ou VMFS. Para o gerenciamento do VMFS, incluindo SRA, as ferramentas do ONTAP são compatíveis com credenciais SVM sem a necessidade de um cluster global.

- ["Adicionar um back-end de storage"](#)
- ["Associar o back-end de storage a uma instância do vCenter Server"](#)

6

Atualize os certificados se estiver trabalhando com várias instâncias do vCenter Server

Ao trabalhar com várias instâncias do vCenter Server, atualize o certificado autoassinado para um certificado assinado pela autoridade de certificação (CA).

- ["Gerenciar certificados"](#)

7

(Opcional) ative a proteção SRA

Habilite o recurso SRA para configurar a recuperação de desastres e proteger armazenamentos de dados NFS ou VMFS.

- ["Configure o SRA no VMware Live Site Recovery Appliance"](#)

8

(Opcional) ative a proteção de sincronização ativa do SnapMirror

Configure as ferramentas do ONTAP para o VMware vSphere para gerenciar a proteção do cluster de host para a sincronização ativa do SnapMirror. Emparelhe os clusters de origem e destino e o SVM para SnapMirror active Sync. Isso se aplica somente aos datastores VMFS.

- ["Proteger usando a proteção do cluster de host"](#)

9

Configure o backup e a recuperação para suas ferramentas do ONTAP para a implantação do VMware vSphere

Programe backups de suas ferramentas do ONTAP para a configuração do VMware vSphere que você pode

usar para recuperar a configuração em caso de falha.

- ["Crie backup e recupere a configuração das ferramentas do ONTAP"](#)

Fluxo de trabalho de implantação de alta disponibilidade (HA)

Se você estiver usando armazenamentos de dados vVols, será necessário expandir a implantação inicial de ferramentas do ONTAP para uma configuração de alta disponibilidade (HA) e ativar os serviços do provedor VASA.

1

Faça a escalabilidade vertical da implantação

É possível escalar as ferramentas do ONTAP para a configuração do VMware vSphere para aumentar o número de nós na implantação e alterar a configuração para uma configuração de HA.

- ["Alterar as ferramentas do ONTAP para a configuração do VMware vSphere"](#)

2

Ativar serviços

Para configurar o datastore vVols, você deve habilitar o serviço provedor VASA. Registre o provedor VASA no vCenter e garanta que suas políticas de armazenamento atendam aos requisitos de HA, incluindo configurações adequadas de rede e armazenamento.

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

- ["Ative os serviços Vasa Provider e SRA"](#)

3

Atualize os certificados

Se você estiver usando datastores vVol com várias instâncias do vCenter Server, atualize o certificado autoassinado para um certificado assinado pela autoridade de certificação (CA).

- ["Gerenciar certificados"](#)

Pré-requisitos para ferramentas do ONTAP para implantação do VMware vSphere

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

Você pode usar as ferramentas do ONTAP para VMware vSphere com o VMware vCenter Server Virtual Appliance (vCSA). Você deve implantar as ferramentas do ONTAP para o VMware vSphere em um cliente vSphere compatível que inclua o sistema ESXi.

Requisitos do sistema

- * Requisitos de espaço do pacote de instalação por nó*
 - 15 GB para instalações com provisionamento reduzido
 - 348 GB para instalações com provisionamento espesso
- **Requisitos de dimensionamento do sistema anfitrião** a memória recomendada de acordo com o tamanho da implementação é como mostrado na tabela abaixo:

Tipo de implantação	CPUs	Memória (GB)	Espaço em disco (GB) com espessura provisionada
Não-HA pequeno	9	18	350
Meio não-HA	13	26	350
Ha pequena (cumulativa de três nós)	27	54	1050
Meio HA (cumulativo de três nós)	39	78	1050
Ha grande (cumulativo de três nós)	51	102	1050

Requisitos mínimos de storage e aplicativos

Storage, host e aplicações	Requisitos mínimos de versão
ONTAP	9.14.1, 9.15.1 e 9.16.0. FAS, ASA A-Series, ASA C-Series, AFF A-Series, AFF C-Series e ASA R2.
Hosts ESXi	ESXi 7.0.3
Servidor vCenter	VCenter 7.0U3
Fornecedor VASA	3,0
Aplicação OVA	10,3

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

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

Limites de configuração para implantar as ferramentas do ONTAP para o VMware vSphere

Você pode usar a tabela a seguir como um guia para configurar as ferramentas do ONTAP para o VMware vSphere.

Implantação	Tipo	Número de vVols	Número de hosts
Não HA	Pequeno (S)	12K	32
Não HA	Médio (M)	24K	64

Alta disponibilidade	Pequeno (S)	24K	64
Alta disponibilidade	Médio (M)	50k	128
Alta disponibilidade	Grande (L)	100k	256 [NOTA] o número de hosts na tabela mostra o número total de hosts de vários vCenters.

Ferramentas do ONTAP para VMware vSphere - adaptador de replicação de armazenamento (SRA)

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

* Tamanho da implantação do vCenter*	Pequeno	Médio
Número total de máquinas virtuais configuradas para proteção usando replicação baseada em array	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
Número de VMs	4000	7000

A tabela a seguir mostra o número de VMware Live Site Recovery e as ferramentas ONTAP correspondentes para o tamanho de implantação do VMware vSphere.

Número de instâncias de recuperação do VMware Live Site	Tamanho de implantação de ferramentas ONTAP
Até 4	Pequeno
4 a 8	Média
Mais de 8	Grande

Para obter mais informações, "[Limites operacionais da recuperação do VMware Live Site](#)" consulte .

Requisitos portuários

A tabela a seguir descreve as portas de rede que o NetApp usa e seus propósitos. Certifique-se de que estas portas estão abertas e acessíveis para facilitar o funcionamento e a comunicação adequados dentro do sistema. Certifique-se de que as configurações de rede necessárias estão em vigor para permitir que o tráfego nessas portas funcione corretamente. Dependendo das suas políticas de segurança, pode ser necessário configurar firewalls ou outros dispositivos de segurança para permitir esse tráfego na sua rede.

Porto	Descrição
-------	-----------

22 (TCP)	O Ansible usa essa porta SSH para comunicação durante o provisionamento de cluster. Essa porta é necessária para funcionalidades como alterar a senha do usuário de manutenção, mensagens de status e atualizar valores em todos os três nós no caso de configuração de HA.
443 (TCP)	Esta é a porta de passagem para a comunicação de entrada para o serviço do fornecedor VASA. O certificado auto-assinado do Fornecedor VASA e o certificado CA personalizado estão alojados nesta porta.
8443 (TCP)	Essa porta hospeda a documentação da API por meio do Swagger e do aplicativo de interface de usuário do Manager.
2379 (TCP)	Esta é a porta padrão para solicitações de clientes, como obter, colocar, excluir ou observar chaves no armazenamento de valores de chave etcd.
2380 (TCP)	Esta é a porta padrão para comunicação de servidor para servidor para o cluster etcd usado para o algoritmo de consenso de jangada em que o etcd se baseia para replicação e consistência de dados.
7472 (TCP/UDP)	Esta é a porta de serviço de métricas prometheus.
7946 (TCP/UDP)	Essa porta é usada para a descoberta de rede de contentores do docker.
9083 (TCP)	Esta porta é uma porta de serviço usada internamente para o serviço do fornecedor VASA.
1162 (UDP)	Esta é a porta de pacotes de trap SNMP.
6443 (TCP)	Fonte: RKE2 nós de agentes. Destino: REK2 nós de servidor. Descrição: Kubernetes API
9345 (TCP)	Fonte: RKE2 nós de agentes. Destino: REK2 nós de servidor. Descrição: REK2 supervisor API
8472 (TCP/UDP)	Todos os nós precisam ser capazes de alcançar outros nós através da porta UDP 8472 quando flannel VXLAN é usado. Fonte: Todos os RKE2 nós. Destino: Todos os REK2 nós. Descrição: Canal CNI com VXLAN
10250 (TCP)	Fonte: Todos os RKE2 nós. Destino: Todos os REK2 nós. Descrição: Kubelet metrics
30000-32767 (TCP)	Fonte: Todos os RKE2 nós. Destino: Todos os REK2 nós. Descrição: NodePort Port port range
123 (TCP)	O ntpd usa essa porta para executar a validação do servidor ntp.

Antes de começar...

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

Requisitos	O seu estado
A versão do vSphere, a versão do ONTAP e a versão do host ESXi são compatíveis com a versão das ferramentas do ONTAP.	☐ Sim ☐ não
O ambiente do vCenter Server está configurado e configurado	☐ Sim ☐ não
O cache do navegador é excluído	☐ Sim ☐ não
Você tem as credenciais do vCenter Server pai	☐ Sim ☐ não
Você tem as credenciais de login para a instância do vCenter Server, à qual as ferramentas do ONTAP para VMware vSphere 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 ferramentas ONTAP.	☐ Sim ☐ não
O aplicativo e os serviços internos das ferramentas do ONTAP podem ser acessados a partir do vCenter Server.	☐ Sim ☐ não
Ao usar SVMs de alocação a vários clientes, você tem um LIF de gerenciamento da SVM em cada SVM.	☐ Sim ☐ não

Folha de cálculo de implementação

Para implantação de nó único

Use a seguinte Planilha para reunir as informações necessárias para as ferramentas do ONTAP para a implantação inicial do VMware vSphere: Para as ferramentas do ONTAP para a implantação inicial do VMware vSphere:

Requisito	O seu valor
Endereço IP para o aplicativo ONTAP Tools. Este é o endereço IP para acessar a interface web do ONTAP Tools.	

Requisito	O seu valor
Endereço IP virtual das ferramentas ONTAP para comunicação interna. Este endereço IP é usado para comunicação interna em uma configuração com várias instâncias das ferramentas ONTAP. Este endereço IP não deve ser o mesmo que o endereço IP do aplicativo das ferramentas ONTAP.	
Nome de host DNS para o primeiro nó	
Servidor DNS primário	
Servidor DNS secundário	
Domínio de pesquisa DNS	
Endereço IPv4 para o primeiro nó. É um endereço IPv4 exclusivo para a interface de gerenciamento do nó na rede de gerenciamento.	
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 gratuitos 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 implantação de HA:

Requisito	O 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 de firewall de rede

Abra as portas necessárias para os endereços IP no firewall da rede. As ferramentas do ONTAP devem ser capazes de alcançar esse LIF pela porta 443. ["Requisitos portuários"](#) Consulte para obter as atualizações mais recentes.

Implantar as ferramentas do ONTAP para o VMware vSphere

As ferramentas do ONTAP para o dispositivo VMware vSphere são implantadas como nó único de pequeno porte com serviços básicos para dar suporte a armazenamentos de dados NFS e VMFS.

Antes de começar

Uma biblioteca de conteúdo no VMware é um objeto de contentor que armazena modelos de VM, modelos vApp e outros tipos de arquivos. A implantação com biblioteca de conteúdo oferece uma experiência perfeita, pois não depende da conectividade de rede.



Você deve armazenar a biblioteca de conteúdo em um datastore compartilhado para que todos os hosts dentro de um cluster possam acessá-la. Crie uma biblioteca de conteúdo para armazenar o OVA antes de configurar o dispositivo para a configuração HA. Não exclua o modelo de biblioteca de conteúdo após a implantação.



Para ativar a implantação de HA posteriormente, não implante a máquina virtual que hospeda as ferramentas do ONTAP diretamente em um host ESXi. Em vez disso, implante-o em um cluster ou pool de recursos.

Se você não tiver uma biblioteca de conteúdo, siga estas etapas para criar uma:

Criar biblioteca de conteúdo no seu plano de usar apenas uma pequena implantação de nó único, não é necessário criar uma biblioteca de conteúdo.

1. Faça o download do .zip arquivo que contém binários (.ova) e certificados assinados para ferramentas do ONTAP para VMware vSphere no ["Site de suporte da NetApp"](#).
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. Navegue até a biblioteca de conteúdo que você criou.
7. Selecione **ações** à direita da página e selecione **Importar item** e importe o arquivo OVA.



Para obter mais informações, ["Criando e usando a Biblioteca de conteúdo"](#) consulte o blog.



Antes de prosseguir com a implantação, defina o DRS (Distributed Resource Scheduler) do cluster no inventário como 'Conservative'. Isso garante que as VMs não sejam migradas durante a instalação.

As ferramentas do ONTAP para o VMware vSphere são inicialmente implantadas como uma configuração não HA. Para escalar para implantação HA, você precisará ativar o hot plug-in da CPU e o hot plug-in da memória. Você pode executar esta etapa como parte do processo de implantação ou editar as configurações da VM após a implantação.

Passos

1. Faça o download do .zip arquivo que contém binários (.ova) e certificados assinados para ferramentas

do ONTAP para VMware vSphere no "[Site de suporte da NetApp](#)". Se você tiver importado o OVA para a biblioteca de conteúdo, você pode pular esta etapa e prosseguir com a próxima etapa.

2. Faça login no servidor vSphere.
3. Navegue até o pool de recursos, cluster ou host onde você pretende implantar o OVA.



Nunca armazene as ferramentas do ONTAP para a máquina virtual VMware vSphere em armazenamentos de dados vVols que ele gerencia.

4. Você pode implantar o OVA 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 Deploy OVF template.... b. escolha o arquivo OVA no URL ou navegue até seu local e selecione Next .	r. vá para a 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 pasta**, insira o nome da máquina virtual e escolha sua localização.
 - Se você estiver usando a versão do vCenter Server 8.0.3, selecione a opção **Personalizar o hardware da 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 do vCenter Server 7.0.3, siga as etapas na seção **o que vem a seguir?** no final da implantação.
6. Selecione um recurso de computador e selecione **Next**. Opcionalmente, marque a caixa para **ligar automaticamente a VM implantada**.
7. Revise os detalhes do modelo e selecione **Next**.
8. Leia e aceite o contrato de licença e selecione **Next**.
9. Selecione o armazenamento para a configuração e o formato do disco e selecione **Next**.
10. Selecione a rede de destino para cada rede de origem e selecione **seguinte**.
11. Na janela **Personalizar modelo**, preencha os campos obrigatórios e selecione **seguinte**.
 - As informações são validadas durante a instalação. Se houver uma discrepância, uma mensagem de erro será exibida no console da Web e você será solicitado a corrigi-la.
 - Os nomes de host devem incluir letras (A-Z, a-z), dígitos (0-9) e hífen (-). Para configurar a pilha dupla, especifique o nome do host mapeado para o endereço IPv6.



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

- O endereço IP das ferramentas do ONTAP é a principal interface para comunicação com as ferramentas do ONTAP.
 - O IPv4 é o componente de endereço IP da configuração do nó, que pode ser utilizado para habilitar o acesso de shell de diagnóstico e SSH no nó para fins de depuração e manutenção.
 - O endereço IP da interconexão do nó é usado para comunicação interna.
12. Ao usar a versão do vCenter Server 8.0.3, na janela **Personalizar hardware**, ative as opções **hot add** da CPU e **Memory hot plug** para permitir a funcionalidade HA.
 13. Revise os detalhes na janela **Pronto para concluir**, selecione **concluir**.

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

14. Ligue a VM após a conclusão da tarefa.

Você pode acompanhar o andamento da instalação no console da Web da VM.

Se houver discrepâncias no formulário OVF, uma caixa de diálogo solicitará uma ação corretiva. Use o botão Tab para navegar, fazer as alterações necessárias e selecione "OK.você tem três tentativas para resolver quaisquer problemas. Se os problemas continuarem após três tentativas, o processo de instalação será interrompido e é aconselhável tentar novamente a instalação em uma nova máquina virtual.

O que vem a seguir?

Se você tiver ferramentas de implantação do ONTAP para o VMware vSphere com o vCenter Server 7,0.3, siga estas etapas após a implantação.

1. Faça login no cliente vCenter
2. Desligue o nó de ferramentas do ONTAP.
3. Navegue até as ferramentas do ONTAP para a máquina virtual VMware vSphere em **inventários** e selecione a opção **Editar configurações**.
4. Nas opções **CPU**, marque a caixa de seleção **Enable CPU hot add**
5. Nas opções **memória**, marque a caixa de seleção **Ativar** contra **Memory hot plug**.

Códigos de erro de implantação

Você pode encontrar códigos de erro durante as ferramentas do ONTAP para operações de implantação, reinicialização e recuperação do VMware vSphere. Os códigos de erro têm cinco dígitos, onde os dois primeiros dígitos representam o script que encontrou o problema, e os últimos três dígitos representam o fluxo de trabalho específico dentro desse script.

Todos os logs de erros são registrados no arquivo ansible-perl-errors.log para facilitar o rastreamento e a resolução de problemas. Esse arquivo de log contém o código de erro e a tarefa Ansible com falha.



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 nenhuma 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 de implantação
01	firstboot-network-config.pl, atualização do modo
02	firstboot-inputs-validation.pl
03	firstboot-deploy-otv-ng.pl, implantar, HA
04	firstboot-deploy-otv-ng.pl, implantar, não HA
05	firstboot-deploy-otv-ng.pl, reinicie
06	firstboot-deploy-otv-ng.pl, upgrade, HA

07	firstboot-deploy-otv-ng.pl, upgrade, não HA
08	firstboot-otv-recovery.pl
09	post-deploy-upgrade.pl

Os últimos três dígitos do código de erro indicam o erro de fluxo de trabalho específico dentro do script:

Código de erro de implantação	Fluxo de trabalho	Resolução
050	Falha na geração da chave SSH	Reinicie a máquina virtual principal (VM).
053	Falha ao instalar o RKE2	Execute o seguinte e reinicie a VM principal ou reimplante: Sudo rke2-killall.sh (todas as VMs) sudo rke2-uninstall.sh (todas as VMs).
054	Falha ao definir kubeconfig	Reimplantar
055	Falha ao implantar o Registro	Se o pod de Registro estiver presente, aguarde que o pod esteja pronto e reinicie a VM principal ou então reimplante.
059	A implantação do KubeVip falhou	Certifique-se de que o endereço IP virtual do plano de controle do Kubernetes e o endereço IP do balanceador de carga fornecidos durante a implantação pertencem à mesma VLAN e são endereços IP livres. Reinicie se todos os pontos anteriores estiverem corretos. Caso contrário, reimplante.
060	A implantação do operador falhou	Reinicie
061	A implantação de serviços falhou	Execute a depuração básica do Kubernetes, como Get Pods, get rs, Get svc, e assim por diante no namespace ntv-system para mais detalhes e logs de erro em /var/log/ansible-perl-errors.log e /var/log/ansible-run.log e redeploy.
062	A implantação de serviços de ferramentas do ONTAP falhou	Consulte os logs de erro em /var/log/ansible-perl-errors.log para obter mais detalhes e reimplantar.
065	O URL da página do Swagger não está acessível	Reimplantar

066	As etapas de pós-implantação para o certificado do gateway falharam	Faça o seguinte para recuperar/concluir a atualização: * Ativar shell de diagnóstico. * Executar 'passo perl /home/maint/scripts/post-deploy-upgrade.pl --postDeploy' comando. * Verifique os logs em /var/log/post-deploy-upgrade.log.
088	A configuração da rotação de log para journald falhou	Verifique as configurações de rede da VM compatíveis com o host no qual a VM está hospedada. Você pode tentar migrar para outro host e reiniciar a VM.
089	A alteração da propriedade do registo de resumo, o ficheiro de configuração de rotação falhou	Reinicie a VM principal.
096	Instalar provisionador de storage dinâmico	-
108	Falha no script de semeadura	-

Reboot error code	Fluxo de trabalho	Resolução
067	A aguardar o tempo limite do servidor rke2.	-
101	Falha ao repor a palavra-passe do utilizador de Manut/Console.	-
102	Falha ao eliminar o ficheiro de palavra-passe durante a reposição da palavra-passe do utilizador de manutenção/consola.	-
103	Falha ao atualizar a nova senha de usuário de Manut/Console no Vault.	-
088	A configuração da rotação de log para journald falhou.	Verifique as configurações de rede da VM compatíveis com o host no qual a VM está hospedada. Você pode tentar migrar para outro host e reiniciar a VM.
089	A alteração da propriedade do registo de resumo, o ficheiro de configuração de rotação falhou.	Reinicie a VM.

Configurar as ferramentas do ONTAP para o VMware vSphere

Adicione instâncias do vCenter Server

Adicione instâncias do vCenter Server às ferramentas do ONTAP para o VMware vSphere para configurar, gerenciar e proteger seus datastores virtuais no ambiente do vCenter Server. Ao adicionar várias instâncias do vCenter Server, certificados de CA personalizados são necessários para comunicação segura entre as ferramentas ONTAP e cada vCenter Server.

Sobre esta tarefa

Ao integrar-se ao vCenter, as ferramentas do ONTAP permitem que você execute tarefas de storage como provisionamento, snapshots e proteção de dados diretamente do cliente vSphere, eliminando a necessidade de alternar para consoles de gerenciamento de storage separados.

Passos

1. Abra um navegador da Web e navegue até o URL:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as ferramentas do ONTAP para as credenciais de administrador do VMware vSphere fornecidas durante a implantação.
3. Selecione **vCenters > Add** para integrar as instâncias do vCenter Server. Forneça seu endereço IP ou nome de host do vCenter, nome de usuário, senha e detalhes da porta.



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

Adicionar uma instância do vCenter Server às ferramentas do ONTAP aciona automaticamente as seguintes ações:

- O plug-in do cliente vCenter é registrado como um plug-in remoto.
- Os Privileges personalizados para os plug-ins e APIs são aplicados à instância do vCenter Server.
- Funções personalizadas são criadas para gerenciar os usuários.
- O plug-in aparece como um atalho na interface do usuário do vSphere.

Registre o provedor VASA com uma instância do vCenter Server

Você pode Registrar o provedor VASA com uma instância do vCenter Server usando as ferramentas do ONTAP para VMware vSphere. A seção Configurações do provedor VASA exibe o status de Registro do provedor VASA para o vCenter Server selecionado. Em uma implantação de vários vCenters, certifique-se de ter certificados CA

personalizados para cada instância do vCenter Server.

Passos

1. Faça login no cliente vSphere
2. Selecione **Atalhos > Ferramentas do NetApp ONTAP** na seção plug-ins.
3. Selecione **Definições > Definições do fornecedor VASA**. O estado de registo do fornecedor VASA será apresentado como não registado.
4. Selecione o botão **Register** para registar o Fornecedor VASA.
5. Insira um nome para o provedor VASA e forneça ferramentas ONTAP para credenciais de usuário do aplicativo VMware vSphere e selecione **Registrar**.
6. Depois de um registo e atualização de página bem-sucedidos, o estado, o nome e a versão do fornecedor VASA registado são apresentados. Após o registo, a ação de cancelamento de registo é ativada.

Depois de terminar

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

Passos

1. Navegue até a instância do vCenter Server.
2. Inicie sessão com as credenciais de administrador.
3. Selecione **fornecedores de armazenamento > Configurar**. Verifique se o provedor VASA integrado está listado corretamente.

Instale o plug-in NFS VAAI

O plug-in NFS vStorage API for Array Integration (NFS VAAI) é um componente de software que integra os storage arrays VMware vSphere e NFS. Instale o plug-in NFS VAAI usando as ferramentas do ONTAP para VMware vSphere a fim de aproveitar os recursos avançados do seu storage array NFS para descarregar determinadas operações relacionadas ao storage dos hosts ESXi para o próprio storage array.

Antes de começar

- Baixe o ["Plug-in NFS do NetApp para VMware VAAI"](#) pacote de instalação.
- Verifique se você tem o host ESXi e o patch mais recente do vSphere 7.0U3 ou versões posteriores e o ONTAP 9.14.1 ou versões posteriores.
- Montar um armazenamento de dados NFS.

Passos

1. Faça login no cliente vSphere.
2. Selecione **Atalhos > Ferramentas do NetApp ONTAP** na seção plug-ins.
3. Selecione **Settings > NFS VAAI Tools**.
4. Quando o plug-in VAAI for carregado no vCenter Server, selecione **alterar** na seção **versão existente**. Se um plug-in VAAI não for carregado para o vCenter Server, selecione o botão **Upload**.
5. Navegue e selecione o `.vib` arquivo e selecione **Upload** para carregar o arquivo para as ferramentas do ONTAP.

6. Selecione **Instalar no host ESXi**, selecione o host ESXi no qual você deseja instalar o plug-in NFS VAAI e, em seguida, selecione **Instalar**.

Somente os hosts ESXi elegíveis para a instalação do plug-in são exibidos. Você pode monitorar o progresso da instalação na seção tarefas recentes do vSphere Web Client.

7. Reinicie o host ESXi manualmente após a instalação.

Quando o administrador do VMware reinicia o host ESXi, as ferramentas do ONTAP para VMware vSphere detectam e ativam automaticamente o plug-in NFS VAAI.

O que se segue?

Depois de instalar o plug-in NFS VAAI e reiniciar seu host ESXi, você precisa configurar as políticas de exportação NFS corretas para a descarga de cópia VAAI. Ao configurar o VAAI em um ambiente NFS, configure as regras de política de exportação com os seguintes requisitos em mente:

- O volume ONTAP relevante precisa permitir chamadas NFSv4.
- O usuário raiz deve permanecer como root e NFSv4 deve ser permitido em todos os volumes pai de junção.
- A opção de suporte VAAI precisa ser definida no servidor NFS relevante.

Para obter mais informações sobre o procedimento, consulte ["Configurar as políticas de exportação de NFS corretas para descarga de cópia VAAI"](#) o artigo da KB.

Informações relacionadas

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

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

["Suporte ONTAP para NFSv4,2"](#)

Configure as configurações do host ESXi

A configuração das configurações de multipath e timeout do servidor ESXi garante alta disponibilidade e integridade de dados, permitindo alternar perfeitamente para um caminho de armazenamento de backup se um caminho primário falhar.

Configure as configurações multipath e timeout do servidor ESXi

As ferramentas do ONTAP para VMware vSphere verificam e definem as configurações de multipath do host ESXi e as configurações de tempo limite do HBA que funcionam melhor com os sistemas de armazenamento NetApp.

Sobre esta tarefa

Dependendo da configuração e da carga do sistema, esse processo pode levar muito tempo. O progresso da tarefa é exibido no painel tarefas recentes.

Passos

1. Na página inicial do VMware vSphere Web client, selecione **hosts and clusters**.
2. Clique com o botão direito do Mouse em um host e selecione **Ferramentas do NetApp ONTAP >**

Atualizar dados do host.

3. Na página de atalhos do cliente da Web VMware vSphere, selecione **Ferramentas do NetApp ONTAP** na seção plug-ins.
4. Vá para a placa **ESXi Host Compliance** na visão geral (painel) das ferramentas do ONTAP para o plug-in VMware vSphere.
5. Selecione o link **Apply Recommended Settings** (aplicar configurações recomendadas).
6. Na janela **Apply Recommended host settings** (aplicar configurações de host recomendadas), selecione os hosts que você deseja atualizar para estar em conformidade com as configurações recomendadas do NetApp e selecione **Next** (Avançar).



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

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

Defina os valores do host ESXi

Usando as ferramentas do ONTAP para VMware vSphere, você pode definir tempos limite e outros valores nos hosts ESXi para garantir o melhor desempenho e o failover bem-sucedido. Os valores que as ferramentas do ONTAP para VMware vSphere definem são baseados no teste interno do NetApp.

Você pode definir os seguintes valores em um host ESXi:

Definições do adaptador HBA/CNA

Define os seguintes parâmetros para valores padrão:

- Disk.QFullSampleSize
- Disk.QFullThreshold
- Tempos limite Emulex FC HBA
- Tempos limite do QLogic FC HBA

Definições MPIO

Configurações MPIO definem os caminhos preferidos para sistemas de armazenamento NetApp. Eles determinam quais dos caminhos disponíveis são otimizados (em vez de caminhos não otimizados que atravessam o cabo de interconexão) e definem o caminho preferido para um desses caminhos.

Em ambientes de alto desempenho, ou quando você estiver testando o desempenho com um único armazenamento de dados LUN, considere alterar a configuração de balanceamento de carga da política de seleção de caminho (PSP) de round-robin (VMW_PSP_RR) da configuração padrão de IOPS de 1000 para um valor de 1.



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

Definições 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
Frequência NFS.HeartbeatFrequency	12
NFS.HeartbeatTimeout	5

Configurar as funções de usuário do ONTAP e o Privileges

Você pode configurar novas funções de usuário e Privileges para gerenciar backends de storage usando o arquivo JSON fornecido com as ferramentas do ONTAP para VMware vSphere e ONTAP System Manager.

Antes de começar

- Você deve ter baixado o arquivo ONTAP Privileges das ferramentas do ONTAP para VMware vSphere usando `/https://<loadbalancerIP>:8443/Virtualization/user-Privileges/users_roles.zip`.
- Você deve ter baixado o arquivo ONTAP Privileges de ferramentas do ONTAP usando `\https://<loadbalancerIP>:8443/virtualization/user-privileges/users_roles.zip`o`.



Você pode criar usuários no cluster ou diretamente no nível de máquinas virtuais de armazenamento (SVMs). Você também pode criar usuários sem usar o arquivo `user_roles.json` e, se feito isso, você precisa ter um conjunto mínimo de Privileges no nível SVM.

- Você deve ter feito login com o administrador Privileges para o back-end de storage.

Passos

1. Extraia o arquivo `/https://<loadbalancerIP>:8443/Virtualization/user-Privileges/Users_roles.zip` baixado.
2. Acesse o Gerenciador do sistema do ONTAP usando o endereço IP de gerenciamento de cluster do cluster.
3. Faça login no cluster com admin Privileges. Para configurar um usuário, execute as seguintes etapas:
 - a. Para configurar o usuário de ferramentas do cluster ONTAP, selecione **Cluster > Configurações > usuários e funções** painel.
 - b. Para configurar o usuário das ferramentas do SVM ONTAP, selecione **Storage SVM > Configurações > usuários e funções** painel.
 - c. Selecione **Adicionar** em usuários.
 - d. Na caixa de diálogo **Adicionar usuário**, selecione **Produtos de virtualização**.
 - e. **Procurar** para selecionar e carregar o arquivo JSON do ONTAP Privileges.

O campo produto é preenchido automaticamente.

- f. Selecione a capacidade necessária no menu pendente capacidade do produto.

O campo **Role** é preenchido automaticamente com base na capacidade do produto selecionada.

- g. Introduza o nome de utilizador e a palavra-passe necessários.
- h. Selecione a função Privileges (descoberta, criação de armazenamento, Modificar armazenamento, destruir armazenamento, nas/SAN) necessária para o usuário e selecione **Adicionar**.

A nova função e o usuário são adicionados e você pode ver o Privileges detalhado na função que você configurou.

Requisitos de mapeamento de agregados da SVM

Para usar as credenciais de usuário do SVM para provisionar armazenamentos de dados, internamente, as ferramentas do ONTAP para VMware vSphere criam volumes no agregado especificado na API PÓS-armazenamentos de dados. O ONTAP não permite a criação de volumes em agregados não mapeados em uma SVM usando credenciais de usuário do SVM. Para resolver isso, você precisa mapear os SVMs com os agregados usando a API REST ou CLI do ONTAP, conforme descrito aqui.

API REST:

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

CLI do ONTAP:

```
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
```

Crie manualmente o usuário e a função do ONTAP

Siga as instruções nesta seção para criar o usuário e as funções manualmente sem usar o arquivo JSON.

1. Acesse o Gerenciador do sistema do ONTAP usando o endereço IP de gerenciamento de cluster do cluster.
2. Faça login no cluster com admin Privileges.
 - a. Para configurar as funções de ferramentas do cluster ONTAP, selecione **Cluster > Configurações > usuários e funções** painel.
 - b. Para configurar as funções de ferramentas do cluster SVM ONTAP, selecione **Storage SVM > Configurações > usuários e funções** painel
3. Criar funções:
 - a. Selecione **Adicionar** na tabela **funções**.
 - b. Insira os detalhes **nome da função** e **atributos da função**.

Adicione o **REST API Path** e o respectivo acesso a partir da lista suspensa.

c. Adicione todas as APIs necessárias e salve as alterações.

4. Criar utilizadores:

a. Selecione **Adicionar** na tabela **usuários**.

b. Na caixa de diálogo **Adicionar usuário**, selecione **System Manager**.

c. Introduza o **Nome de utilizador**.

d. Selecione **Role** nas opções criadas na etapa **Create Roles** acima.

e. Introduza as aplicações a que pretende dar acesso e o método de autenticação. ONTAPI e HTTP são as aplicações necessárias e o tipo de autenticação é **Password**.

f. Defina **Senha para o usuário** e **Salvar** para o usuário.

Lista de Privileges mínimo necessário para usuário de cluster com escopo global não administrador

O Privileges mínimo necessário para usuários de cluster com escopo global não admin criados sem usar o arquivo JSON de usuários são listados nesta seção. Se um cluster for adicionado ao escopo local, é recomendável usar o arquivo JSON para criar os usuários, já que as ferramentas do ONTAP para VMware vSphere exigem mais do que apenas o Read Privileges para provisionamento no ONTAP.

Usando APIs:

API	Nível de acesso	Usado para
/api/cluster	Somente leitura	Detecção de configuração do cluster
/api/cluster/licenciamento/licenças	Somente leitura	Verificação de licença para licenças específicas de protocolo
/api/cluster/nós	Somente leitura	Descoberta do tipo de plataforma
/api/security/accounts	Somente leitura	Descoberta de privilégios
/api/security/roles	Somente leitura	Descoberta de privilégios
/api/storage/agregados	Somente leitura	Verificação de espaço agregado durante o provisionamento de armazenamento de dados/volume
/api/storage/cluster	Somente leitura	Para obter os dados de espaço e eficiência no nível do cluster
/api/storage/discos	Somente leitura	Para obter os discos associados em um agregado
/api/storage/qos/políticas	Ler/criar/Modificar	Gerenciamento de políticas de QoS e VM
/api/svm/svms	Somente leitura	Para obter a configuração do SVM, no caso de o cluster ser adicionado localmente.
/api/network/ip/interfaces	Somente leitura	Back-end de storage: Para identificar o escopo de LIF de gerenciamento é Cluster/SVM

Crie ferramentas do ONTAP para o usuário com escopo de cluster baseado na API do VMware vSphere ONTAP



Você precisa de descoberta, criação, modificação e destruição do Privileges para executar operações DE PATCH e reversão automática em caso de falha em datastores. A falta dessas Privileges juntas leva a interrupções no fluxo de trabalho e problemas de limpeza.

Criar ferramentas do ONTAP para o usuário baseado na API do VMware vSphere ONTAP com descoberta, criação de armazenamento, modificação de armazenamento, destruição de armazenamento o Privileges permite iniciar descobertas e gerenciar fluxos de trabalho de ferramentas do ONTAP.

Para criar um usuário com escopo de cluster com todos os Privileges 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
```

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

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

Crie ferramentas do ONTAP para o usuário com escopo SVM baseado na API do VMware vSphere ONTAP

Para criar um usuário com escopo SVM com todos os Privileges, execute os seguintes comandos:

```
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/napmirror/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 o ONTAP versões 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 acima, 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_
```

Para desbloquear a conta, para habilitar o acesso à interface de gerenciamento, execute o seguinte comando:

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

Exemplo:

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

Atualize as ferramentas do ONTAP para o usuário do VMware vSphere 10,1 para o usuário 10,3

Se as ferramentas do ONTAP para o usuário do VMware vSphere 10,1 forem um usuário com escopo de cluster criado usando o arquivo json, execute os seguintes comandos na CLI do ONTAP usando o usuário admin para atualizar para a versão 10,3.

Para obter recursos do produto:

- VSC
- Fornecedor VSC e VASA
- VSC e SRA
- VSC, Fornecedor VASA e SRA.

Cluster Privileges -

```
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 sub show" -access all
```

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

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme sub system 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

Se as ferramentas do ONTAP para o usuário do VMware vSphere 10,1 forem um usuário com escopo SVM criado usando o arquivo json, execute os seguintes comandos na CLI do ONTAP usando o usuário admin para atualizar para a versão 10,3.

SVM Privileges -

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 sub show" -access all -vserver <vserver-name>

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

security login role create -role <existing-role-name> -cmddirname "vserver nvme sub system 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 sub-element 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>

-access all -vserver <vserver-name>

Adicionar o comando *vserver nvme namespace show* e *vserver nvme subsistema show* à função existente adiciona os seguintes comandos.

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

Adicionar um back-end de storage

A adição de um back-end de storage permite a integração de um cluster do ONTAP.

Sobre esta tarefa

No caso de configurações de alocação a vários clientes em que o vCenter atua como locatário de um SVM associado, use o Gerenciador de ferramentas do ONTAP para adicionar o cluster. Associe o back-end de storage ao vCenter Server para mapeá-lo globalmente para a instância integrada do vCenter Server. O locatário do vCenter deve integrar as máquinas virtuais de storage (SVMs) desejadas. Isso permite que um usuário do SVM provisione o vVols datastore. É possível adicionar storage ao vCenter usando o SVM.

Adicione os back-ends de storage local com credenciais de cluster ou SVM usando a interface de usuário das ferramentas do ONTAP. Esses backends de armazenamento estão limitados a um único vCenter. Ao usar credenciais de cluster localmente, os SVMs associados mapeiam automaticamente para o vCenter para gerenciar vVols ou VMFS. Para o gerenciamento do VMFS, incluindo SRA, as ferramentas do ONTAP são compatíveis com credenciais SVM sem a necessidade de um cluster global.

Usando o Gerenciador de ferramentas do ONTAP



Em uma configuração de alocação a vários clientes, é possível adicionar um cluster de back-end de storage globalmente e SVM localmente para usar as credenciais de usuário do SVM.

Passos

1. Inicie o Gerenciador de ferramentas do ONTAP a partir de um navegador da Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as ferramentas do ONTAP para as credenciais de administrador do VMware vSphere fornecidas durante a implantação.
3. Selecione **backends de armazenamento** na barra lateral.
4. Adicione o back-end de armazenamento e forneça o endereço IP do servidor ou FQDN, nome de usuário e detalhes de senha.



LIFs de gerenciamento de endereços IPv4 e IPv6 são compatíveis.

Usando a interface de usuário do cliente vSphere



Ao configurar um back-end de storage por meio da interface de usuário do cliente vSphere, é importante observar que o armazenamento de dados vVols não oferece suporte à adição direta de um usuário SVM.

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



Para adicionar um usuário SVM diretamente, você pode adicionar credenciais baseadas em cluster e LIFs de gerenciamento de endereços IPv4 e IPv6 ou fornecer credenciais baseadas em SVM com um LIF de gerenciamento de SVM.

O que vem a seguir?

A lista é atualizada e você pode ver o back-end de armazenamento recém-adicionado na lista.

Associar um back-end de storage a uma instância do vCenter Server

Associe um back-end de storage ao vCenter Server para criar um mapeamento entre o back-end de storage e a instância integrada do vCenter Server globalmente.

Passos

1. Inicie o Gerenciador de ferramentas do ONTAP a partir de um navegador da Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`

2. Faça login com as ferramentas do ONTAP para as credenciais de administrador do VMware vSphere fornecidas durante a implantação.
3. Selecione vCenter na barra lateral.
4. Selecione as elipses verticais na instância do vCenter Server que você deseja associar aos backends de armazenamento.
5. Selecione o back-end de armazenamento no menu suspenso para associar a instância do vCenter Server ao back-end de armazenamento necessário.

Configurar o acesso à rede

Se você não tiver configurado o acesso à rede, todos os endereços IP descobertos do host ESXi serão adicionados à política de exportação por padrão. Você pode configurá-lo para adicionar alguns endereços IP específicos à política de exportação e excluir o restante. No entanto, quando você executa uma operação de montagem nos hosts ESXi excluídos, a operação falha.

Passos

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

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

4. Selecione **Guardar**.

Crie um datastore

Quando você cria um datastore no nível do cluster do host, o datastore é criado e montado em todos os hosts do destino e a ação é ativada somente se o usuário atual tiver o privilégio de executar.

Crie um datastore vVols

Começando com as ferramentas do ONTAP para VMware vSphere 10,3, você pode criar um datastore vVols em sistemas ASA R2 com eficiência de espaço tão fina. O provedor VASA cria um contentor e os endpoints de protocolo desejados, ao mesmo tempo em que cria o datastore da evolução. Este contentor não terá quaisquer volumes de apoio.

Antes de começar

- Certifique-se de que os agregados de raiz não sejam mapeados para o SVM.
- Certifique-se de que o Fornecedor VASA está registrado no vCenter selecionado.
- No sistema de storage ASA R2, o SVM deve ser mapeado para agregado ao usuário do SVM.

Passos

1. Faça login no cliente vSphere.
2. Clique com o botão direito do Mouse em um sistema host, cluster de host ou data center e selecione **NetApp ONTAP Tools > Create datastore**.
3. Selecione vVols **datastore type**.
4. Insira as informações **nome do datastore** e **Protocolo**.



O sistema ASA R2 dá suporte aos protocolos iSCSI e FC para vVols.

5. Selecione a VM de armazenamento onde você deseja criar o datastore.
6. Selecione uma política de exportação personalizada para o protocolo NFS ou um nome de grupo de iniciadores personalizado para os protocolos iSCSI e FC nas **Opções avançadas**.



No ASA R2, tipo de sistema de storage SVM, unidades de storage (LUN/namespace) não são criadas, pois o armazenamento de dados 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 ativar a QoS no datastore. Por padrão, um volume é criado para cada solicitação criada pelo LUN. Esta etapa não se aplica aos armazenamentos de dados vVols que usam os sistemas de storage ASA R2.

8. Reveja a sua seleção no painel **Summary** e selecione **Finish**.

Criar um armazenamento de dados NFS

Um armazenamento de dados NFS (Network File System) do VMware usa o protocolo NFS para conectar hosts ESXi a um dispositivo de storage compartilhado por uma rede. Os datastores NFS são comumente usados em ambientes VMware vSphere e oferecem várias vantagens, como simplicidade e flexibilidade.

Passos

1. Faça login no cliente vSphere.
2. Clique com o botão direito do Mouse em um sistema host, cluster de host 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 do protocolo do datastore no painel **Nome e protocolo**. Selecione **datastore cluster** e **Kerberos Authentication** nas opções avançadas.



A autenticação Kerberos só está disponível quando o protocolo NFS 4,1 está selecionado.

5. Selecione **Plataforma e Storage VM** no painel **Storage**.
6. Escolha **Política de exportação personalizada** em opções avançadas, se necessário, mas não é recomendado. Se usado, certifique-se de executar a descoberta no vCenter para todos os objetos.



Você não pode criar um armazenamento de dados NFS usando a política de volume raiz/padrão do SVM.

- Nas opções avançadas, o botão de alternância **assimétrico** fica visível apenas se o desempenho ou a capacidade estiver selecionado na lista suspensa da plataforma.
 - Quando você escolhe a opção **any** no menu suspenso da plataforma, você pode ver os SVMs que fazem parte do vCenter, independentemente da plataforma ou do sinalizador assimétrico.
7. Selecione o agregado para criação de volume no painel **atributos de armazenamento**. Nas opções avançadas, escolha **reserva de espaço** e **Ativar QoS** conforme necessário.
 8. Revise as seleções no painel **Summary** e selecione **Finish**.

O datastore NFS é criado e montado em todos os hosts.

Crie um datastore VMFS

O Virtual Machine File System (VMFS) é um sistema de arquivos em cluster que armazena arquivos de máquina virtual em ambientes VMware vSphere. O VMFS permite que vários hosts ESXi acessem os mesmos arquivos de máquina virtual simultaneamente, habilitando recursos como vMotion e alta disponibilidade.

Num cluster protegido:

- Você pode criar apenas um datastores VMFS. Quando você adiciona um datastore VMFS a um cluster protegido, o datastore fica protegido automaticamente.
- Não é possível criar um datastore em um data center com um ou mais clusters de host protegidos.
- Não é possível criar um datastore no host ESXi se o cluster de host pai estiver protegido com uma relação do tipo "Automated failover Duplex policy" (configuração uniforme/não uniforme).
- Você pode criar um datastore VMFS somente em um host ESXi protegido por uma relação assíncrona. Não é possível criar e montar um datastore em um host ESXi que faça parte de um cluster de host protegido pela política "Automated failover Duplex".

Antes de começar

- Ative os serviços e LIFs para cada protocolo no lado do storage do ONTAP.
- Mapear o SVM para agregar usuário do SVM no sistema de storage ASA R2.
- Configure o host ESXi se estiver usando o protocolo NVMe/TCP:
 - a. Reveja o. ["Guia de compatibilidade da VMware"](#)



O VMware vSphere 7,0 U3 e versões posteriores são compatíveis com o protocolo NVMe/TCP. No entanto, o VMware vSphere 8,0 e a versão posterior são recomendados.

- b. Valide se o fornecedor da placa de interface de rede (NIC) suporta NIC ESXi com protocolo NVMe/TCP.
 - c. Configure a NIC ESXi para NVMe/TCP de acordo com as especificações do fornecedor da NIC.
 - d. Ao usar a versão do VMware vSphere 7, siga as instruções no site da VMware "[Configure a vinculação VMkernel para o adaptador NVMe sobre TCP](#)" para configurar a vinculação de portas NVMe/TCP. Ao usar a versão do VMware vSphere 8, siga "[Configurando o NVMe em TCP no ESXi](#)" , para configurar a vinculação de porta NVMe/TCP.
 - e. Para a versão do VMware vSphere 7, siga as instruções na página "[Habilite o NVMe em adaptadores de software RDMA ou NVMe em TCP](#)" para configurar adaptadores de software NVMe/TCP. Para a versão do VMware vSphere 8, siga "[Adicionar software NVMe em adaptadores RDMA ou NVMe em TCP](#)" para configurar os adaptadores de software NVMe/TCP.
 - f. Execute "[Descubra sistemas de storage e hosts](#)" uma ação no host ESXi. Para obter mais informações, "[Como configurar o NVMe/TCP com o vSphere 8,0 Update 1 e o ONTAP 9.13,1 para datastores VMFS](#)" consulte .
- Se você estiver usando o protocolo NVMe/FC, execute as seguintes etapas para configurar o host ESXi:
 - a. Habilite o NVMe sobre Fabrics (NVMe-of) no(s) host(s) ESXi.
 - b. Zoneamento SCSI completo.
 - c. Certifique-se de que os hosts ESXi e o sistema ONTAP estejam conectados em uma camada física e lógica.

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

Para obter mais informações sobre como usar o protocolo NVMe/FC com o VMware vSphere 8,0, "[Configuração de host NVMe-of para ESXi 8.x com ONTAP](#)" consulte .

Para obter mais informações sobre como usar o NVMe/FC com o VMware vSphere 7,0, "[Guia de configuração de host ONTAP NVMe/FC](#)" consulte e "[TR-4684](#)".

Passos

1. Faça login no cliente vSphere.
2. Clique com o botão direito do Mouse em um sistema host, cluster de host ou data center e selecione **NetApp ONTAP Tools > Create datastore**.
3. Selecione o tipo de armazenamento de dados VMFS.
4. Insira o nome, o tamanho e as informações do protocolo do datastore no painel **Nome e Protocolo**. Se você optar por adicionar o novo datastore a um cluster de datastore VMFS existente, selecione o seletor de cluster de datastore em Opções avançadas.
5. Selecione Storage VM (VM de armazenamento) no painel **Storage** (armazenamento). Forneça o **Nome do grupo de iniciadores personalizados** na seção **Opções avançadas** conforme necessário. Você pode escolher um grupo existente para o datastore ou criar um novo grupo com um nome personalizado.

Quando o protocolo NVMe/FC ou NVMe/TCP é selecionado, um novo subsistema de namespace é criado e usado para mapeamento de namespace. O subsistema namespace é criado 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 **armazenamento**.

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

- a. Selecione **agregar** nas opções suspensas.



Para sistemas de armazenamento ASA R2, a opção **agregado** não é mostrada porque o armazenamento ASA R2 é um armazenamento desagregado. Quando você escolhe um tipo de sistema de storage ASA R2, a página atributos de storage mostra as opções para ativar a QoS.

- b. De acordo com o protocolo selecionado, uma unidade de armazenamento (LUN/namespace) é criada com uma reserva de espaço do tipo thin.

- c. Selecione **Use as opções de volume existente**, **Enable 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/namespace). Portanto, essas opções não são mostradas.



Para a criação do armazenamento de dados VMFS com protocolo NVMe/FC ou NVMe/TCP, não é possível usar o volume existente, você deve criar um novo volume.

7. Revise os detalhes do datastore no painel **Summary** e selecione **Finish**.



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

Resultado

O datastore VMFS é criado e montado em todos os hosts.

Proteja armazenamentos de dados e máquinas virtuais

Proteger usando a proteção do cluster de host

As ferramentas do ONTAP para o VMware vSphere gerenciam a proteção dos clusters de host. Todos os armazenamentos de dados pertencentes ao SVM selecionado e montados em um ou mais hosts do cluster são protegidos em um cluster de host.

Antes de começar

Certifique-se de que os seguintes pré-requisitos são cumpridos:

- O cluster de host tem armazenamentos de dados somente em uma SVM.
- O datastore montado no cluster de host não deve ser montado em nenhum host fora do cluster.
- Todos os armazenamentos de dados montados no cluster de host precisam ser armazenamentos de dados VMFS com protocolo iSCSI/FC. Armazenamentos de dados vVols, NFS ou VMFS com protocolos NVMe/FC e NVMe/TCP não são compatíveis.
- Armazenamentos de dados de formação de FlexVol/LUN montados no cluster de host não devem fazer parte de nenhum grupo de consistência existente (CG).
- Armazenamentos de dados de formação de FlexVol/LUN montados no cluster de host não devem fazer parte de qualquer relacionamento existente com o SnapMirror.
- O cluster de host deve ter pelo menos um datastore.

Passos

1. Faça login no cliente vSphere
2. Clique com o botão direito do Mouse em um cluster de host e selecione **NetApp ONTAP Tools > Protect Cluster**.
3. Na janela do cluster Protect, os detalhes do tipo de datastore e da máquina virtual de armazenamento de origem (VM) são preenchidos automaticamente. Selecione o link datastores para exibir os datastores protegidos.
4. Digite o nome do grupo **consistência**.
5. Selecione **Adicionar relacionamento**.
6. Na janela **Add SnapMirror Relationship**, selecione **Target storage VM** e o tipo **Policy**.

O tipo de política pode ser assíncrono ou AutomatedFailOverDuplex.

Quando você adiciona a relação do SnapMirror como uma política de tipo AutomatedFailOverDuplex, você deve adicionar a VM de armazenamento de destino como back-end de armazenamento ao mesmo vCenter onde as ferramentas do ONTAP para VMware vSphere são implantadas.

No tipo de política AutomatedFailOverDuplex, existem configurações de host uniformes e não uniformes. Quando você seleciona o botão de alternância **Uniform host Configuration**, a configuração do grupo de iniciadores do host é implicitamente replicada no site de destino. Para obter detalhes, "[Principais conceitos e termos](#)" consulte .

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

8. Selecione **Adicionar**.
9. Na janela **Protect cluster**, não é possível editar o cluster protegido durante a operação criar. Você pode excluir e adicionar proteção novamente. Durante a operação Modificar proteção do cluster do host, a opção de edição está disponível. Você pode editar ou excluir as relações usando as opções do menu de elipse.
10. Selecione o botão **Protect**.

Uma tarefa do vCenter é criada com detalhes de ID da tarefa e seu progresso é mostrado no painel tarefas recentes. Esta é uma tarefa assíncrona; a interface do usuário mostra apenas o status de envio da solicitação e não espera que a tarefa seja concluída.

11. Para exibir os clusters de host protegidos, navegue até **Ferramentas do NetApp ONTAP > proteção > relacionamentos de cluster do host**.

Proteja usando proteção SRA

Ative o SRA para proteger datastores

As ferramentas do ONTAP para VMware vSphere oferecem a opção de habilitar o recurso SRA para configurar a recuperação de desastres.

Antes de começar

- Você deve ter configurado a instância do vCenter Server e configurado o host ESXi.
- Você deve ter implantado as ferramentas do ONTAP para o VMware vSphere.
- Você deve ter baixado o arquivo do adaptador SRA `.tar.gz` do ["Site de suporte da NetApp"](#).
- Os clusters do ONTAP de origem e destino devem ter as mesmas programações personalizadas do SnapMirror criadas antes de executar os workflows do SRA.

Passos

1. Faça login na interface de gerenciamento do VMware Live Site Recovery Appliance usando o URL: `https://:<srm_ip>:5480` E vá para adaptadores de replicação de armazenamento na interface de gerenciamento do VMware Live Site Recovery Appliance.
2. Selecione **novo adaptador**.
3. Carregue o instalador `.tar.gz` para o plug-in SRA para o VMware Live Site Recovery.
4. Volte a verificar os adaptadores para verificar se os detalhes estão atualizados na página adaptadores de replicação de armazenamento de recuperação de site do VMware Live.

Configurar o SRA para ambientes SAN e nas

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

Configurar o SRA para ambientes SAN

Antes de começar

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

- Recuperação do VMware Live Site

A documentação sobre a instalação do VMware Live Site Recovery está no site da VMware.

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

- SRA

O adaptador é instalado no VMware Live Site Recovery.

Passos

1. Verifique se os hosts ESXi primários estão conectados aos LUNs no sistema de armazenamento primário no local protegido.
2. Verifique se os LUNS estão em grupos que têm a `ostype` opção definida como *VMware* no sistema de armazenamento primário.
3. Verifique se os hosts ESXi no local de recuperação têm conectividade iSCSI adequada à máquina virtual de armazenamento (SVM). Os hosts ESXi do local secundário devem ter acesso ao armazenamento do local secundário e os hosts ESXi do local principal devem ter acesso ao armazenamento do local primário.

Você pode fazer isso verificando se os hosts ESXi têm LUNs locais conectados na SVM ou o comando nas SVMs `iscsi show initiators`. Verifique o acesso LUN para os LUNs mapeados no host ESXi para verificar a conectividade iSCSI.

Configurar o SRA para ambientes nas

Antes de começar

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

- Recuperação do VMware Live Site

A documentação sobre a instalação do VMware Live Site Recovery pode ser encontrada no site da VMware.

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

- SRA

O adaptador é instalado no VMware Live Site Recovery e no servidor SRA.

Passos

1. Verifique se os datastores no site protegido contêm máquinas virtuais registradas no vCenter Server.
2. Verifique se os hosts ESXi no local protegido montaram os volumes de exportações NFS da máquina virtual de storage (SVM).
3. Verifique se endereços válidos, como o endereço IP, nome do host ou FQDN em que as exportações NFS estão presentes, estão especificados no campo **endereços NFS** ao usar o assistente Array Manager para adicionar arrays ao VMware Live Site Recovery.
4. Use o `ping` comando em cada host ESXi no local de recuperação para verificar se o host tem uma porta VMkernel que pode acessar os endereços IP usados para atender às exportações NFS do SVM.

Configure o SRA para ambientes altamente dimensionados

Você deve configurar os intervalos de tempo de armazenamento de acordo com as

configurações recomendadas para Storage Replication Adapter (SRA) para ter um desempenho ideal em ambientes altamente dimensionados.

Definições do fornecedor de armazenamento

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

* Configurações avançadas*	Valores de tempo limite
<code>StorageProvider.resignatureTimeout</code>	Aumente o valor da definição de 900 segundos para 12000 segundos.
<code>storageProvider.hostRescanDelaySec</code>	60
<code>storageProvider.hostRescanRepeatCnt</code>	20
<code>storageProvider.hostRescanTimeoutSec</code>	Definir um valor alto (por exemplo: 99999)

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

<https://techdocs.broadcom.com/us/en/vmware-cis/live-recovery/live-site-recovery/9-0/how-do-i-protect-my-environment/advanced-srm-configuration/reconfigure-srm-settings/change-storage-provider-settings.html>["Altere as definições do fornecedor de armazenamento"]Consulte para obter mais informações sobre como modificar as definições do fornecedor de armazenamento.

Definições de armazenamento

Quando você atinge 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.

<https://techdocs.broadcom.com/us/en/vmware-cis/live-recovery/live-site-recovery/9-0/how-do-i-protect-my-environment/advanced-srm-configuration/reconfigure-srm-settings/change-storage-provider-settings.html>["Altere as definições de armazenamento"]Consulte para modificar as definições do fornecedor de SAN.

Configure o SRA no VMware Live Site Recovery Appliance

Depois de implantar o VMware Live Site Recovery Appliance, você deve configurar o SRA no VMware Live Site Recovery Appliance. A configuração bem-sucedida do SRA permite que o VMware Live Site Recovery Appliance se comunique com o SRA para gerenciamento de recuperação de desastres. Você deve armazenar as ferramentas do ONTAP para credenciais do VMware vSphere (endereço IP) no dispositivo VMware Live Site Recovery para permitir a comunicação entre o VMware Live Site Recovery Appliance e o SRA.

Antes de começar

Você deve ter baixado o arquivo *tar.gz* do ["Site de suporte da NetApp"](#).

Sobre esta tarefa

A configuração do SRA no VMware Live Site Recovery Appliance armazena as credenciais SRA no VMware Live Site Recovery Appliance.

Passos

1. Na tela do VMware Live Site Recovery Appliance, selecione **Storage Replication Adapter > New Adapter**.
2. Carregue o arquivo *.tar.gz* para o VMware Live Site Recovery.
3. Faça login usando a conta de administrador no VMware Live Site Recovery Appliance usando o putty.
4. Mude para o usuário root usando o comando: `su root`
5. Execute o comando `cd /var/log/vmware/srm` para navegar para o diretório de log.
6. No local do log, digite o comando para obter o ID do docker usado pelo SRA: `docker ps -l`
7. Para fazer login no ID do contentor, digite o comando: `docker exec -it -u srm <container id> sh`
8. Configure o VMware Live Site Recovery com as ferramentas do ONTAP para o endereço IP e a senha do 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>`



Você precisa fornecer o valor da senha dentro de aspas simples para garantir que o script Perl não leia os caracteres especiais na senha como delimitador da entrada.



O nome de usuário e a senha do aplicativo são definidos durante a implantação de ferramentas do ONTAP. Isto é necessário para o registo do fornecedor/SRA da VASA.

9. Volte a verificar os adaptadores para verificar se os detalhes estão atualizados na página adaptadores de replicação de armazenamento de recuperação de site do VMware Live.

Uma mensagem de sucesso confirmando que as credenciais de armazenamento são armazenadas é exibida. O SRA pode se comunicar com o servidor SRA usando o endereço IP, porta e credenciais fornecidos.

Atualizar credenciais SRA

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 se tiver modificado as credenciais.

Antes de começar

Você deve ter executado as etapas mencionadas no ["Configurando o SRA no VMware Live Site Recovery Appliance"](#) tópico .

Passos

1. Execute os seguintes comandos para excluir a pasta da máquina VMware Live Site Recovery senha do nome de usuário das ferramentas do ONTAP em cache:

- 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 ter uma única cotação em torno do valor da senha.

Uma mensagem de sucesso confirmando que as credenciais de armazenamento são armazenadas é exibida. O SRA pode se comunicar com o servidor SRA usando o endereço IP, porta e credenciais fornecidos.

Configurar sites protegidos e de recuperação

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

Configurar grupos de proteção

Antes de começar

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

- Mesma versão do VMware Live Site Recovery instalada
- Máquinas virtuais
- Emparelhados sites protegidos e de recuperação
- Os datastores de origem e destino devem ser montados nos respectivos sites

Passos

1. Faça login no vCenter Server e selecione **Site Recovery > Protection Groups**.

2. No painel **grupos de proteção**, selecione **novo**.
3. Especifique um nome e uma descrição para o grupo de proteção, direção e selecione **Next**.
4. No campo **Type**, selecione a opção **Type field...** como grupos de datastore (replicação baseada em array) para armazenamento de dados NFS e VMFS. O domínio de falha não é nada além de SVMs com replicação ativada. Os SVMs que só têm peering implementado e não têm problemas são exibidos.
5. Na guia grupos de replicação, selecione o par de matrizes ativado ou os grupos de replicação que têm a máquina virtual configurada e, em seguida, selecione **Next**.

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

6. Selecione o plano de recuperação existente ou crie um novo plano selecionando **Adicionar ao novo plano de recuperação**.
7. Na guia Pronto para concluir, revise os detalhes do grupo de proteção que você criou e selecione **concluir**.

Emparelhe locais protegidos e de recuperação

Você deve emparelhar os sites protegidos e de recuperação criados usando o vSphere Client para habilitar o Storage Replication Adapter (SRA) para descobrir os sistemas de armazenamento.

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. Clique duas vezes em **Site Recovery** na página inicial do vSphere Client e selecione **Sites**.
2. Selecione **Objects > actions > Pair Sites**.
3. Na caixa de diálogo **Emparelhar servidores do Gestor de recuperação de Site**, introduza o endereço do controlador de Serviços de Plataforma do site protegido e, em seguida, selecione **seguinte**.
4. Na seção Selecionar vCenter Server, faça o seguinte:
 - a. Verifique se o vCenter Server do site protegido aparece como um candidato correspondente para emparelhar.
 - b. Insira as credenciais administrativas SSO e selecione **Finish**.
5. Se solicitado, selecione **Sim** para aceitar os certificados de segurança.

Resultado

Os locais protegidos e de recuperação aparecerão na caixa de diálogo objetos.

Configurar recursos do site protegidos e de recuperação

Configurar mapeamentos de rede

Você deve configurar seus mapeamentos de recursos, como redes de VM, hosts ESXi e pastas em ambos os sites, para habilitar 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
- Mapeamentos de pastas
- Mapeamentos de recursos
- Datastores de espaço reservado

Antes de começar

Você deve ter conectado os sites protegidos e de recuperação.

Passos

1. Inicie sessão no vCenter Server e selecione **Site Recovery > Sites**.
2. Selecione seu site protegido e selecione **Gerenciar**.
3. Selecione **Mapeamentos de rede > novo** na guia gerenciar para criar um novo mapeamento de rede.
4. No assistente criar mapeamento de rede, faça o seguinte:
 - a. Selecione **Prepare automaticamente Mapeamentos para redes com nomes correspondentes** e selecione **Next**.
 - b. Selecione os objetos de data center necessários para os sites protegidos e de recuperação e selecione **Adicionar mapeamentos**.
 - c. Selecione **Next** depois que os mapeamentos forem criados com êxito.
 - d. Selecione o objeto usado anteriormente para criar mapeamento reverso e 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.

Configurar mapeamentos de pastas

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

Antes de começar

Você deve ter conectado os sites protegidos e de recuperação.

Passos

1. Inicie sessão no vCenter Server e selecione **Site Recovery > Sites**.
2. Selecione seu site protegido e selecione **Gerenciar**.
3. Selecione **Mapeamentos de pastas > pasta** ícone na guia Gerenciar para criar um novo mapeamento de pastas.
4. No assistente criar Mapeamento de pastas, execute o seguinte:
 - a. Selecione **Prepare automaticamente Mapeamentos para pastas com nomes correspondentes** e selecione **Next**.
 - b. Selecione os objetos de data center necessários para os sites protegidos e de recuperação e selecione **Adicionar mapeamentos**.
 - c. Selecione **Next** depois que os mapeamentos forem criados com êxito.
 - d. Selecione o objeto usado anteriormente para criar mapeamento reverso e selecione **Finish**.

Resultado

A página Mapeamentos de pastas 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.

Configurar mapeamentos de recursos

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

Antes de começar

Você deve ter conectado os sites protegidos e de recuperação.



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

Passos

1. Inicie sessão no vCenter Server e selecione **Site Recovery > Sites**.
2. Selecione seu site protegido e selecione **Gerenciar**.
3. Selecione **Mapeamentos de recursos > novo** na guia gerenciar para criar um novo mapeamento de recursos.
4. No assistente criar mapeamento de recursos, execute o seguinte:
 - a. Selecione **Prepare automaticamente Mapeamentos para recurso com nomes correspondentes** e selecione **Next**.
 - b. Selecione os objetos de data center necessários para os sites protegidos e de recuperação e selecione **Adicionar mapeamentos**.
 - c. Selecione **Next** depois que os mapeamentos forem criados com êxito.
 - d. Selecione o objeto usado anteriormente para criar mapeamento reverso e selecione **Finish**.

Resultado

A página Mapeamentos de recursos 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.

Configurar datastores de espaço reservado

Você deve configurar um datastore de espaço reservado para manter um lugar no inventário do vCenter no site de recuperação da máquina virtual protegida (VM). O datastore de espaço reservado não precisa ser grande, pois as VMs de espaço reservado são pequenas e usam apenas algumas centenas ou menos kilobytes.

Antes de começar

- Você deve ter conectado os sites protegidos e de recuperação.
- Você deve ter configurado seus mapeamentos de recursos.

Passos

1. Inicie sessão no vCenter Server e selecione **Site Recovery > Sites**.
2. Selecione seu site protegido e selecione **Gerenciar**.

3. Selecione **datastores de espaço > novo** na guia gerenciar para criar um novo datastore de espaço reservado.
4. Selecione o datastore apropriado e selecione **OK**.



Os datastores de espaço reservado podem ser locais ou remotos e não devem ser replicados.

5. Repita as etapas de 3 a 5 para configurar um datastore de espaço reservado para o site de recuperação.

Configure o SRA usando o gerenciador de array

Você pode configurar o Storage Replication Adapter (SRA) usando o assistente do Array Manager do VMware Live Site Recovery para habilitar interações entre o VMware Live Site Recovery e as máquinas virtuais de armazenamento (SVMs).

Antes de começar

- Você deve ter emparelhado os sites protegidos e os sites de recuperação no VMware Live Site Recovery.
- Você deve ter configurado o storage integrado antes de configurar o gerenciador de array.
- Você deve ter configurado e replicado as relações do SnapMirror entre os sites protegidos e os sites de recuperação.
- Você deve ter habilitado os LIFs de gerenciamento da SVM para habilitar a alocação a vários clientes.

SRA é compatível com gerenciamento em nível de cluster e gerenciamento em nível de SVM. Se você adicionar storage em um nível de cluster, poderá descobrir e executar operações em todos os SVMs no cluster. Se você adicionar storage no nível da SVM, poderá gerenciar apenas essa SVM específica.

Passos

1. No VMware Live Site Recovery, selecione **Array Managers > Add Array Manager**.
2. Insira as seguintes informações para descrever o array no VMware Live Site Recovery:
 - a. Digite um nome para identificar o gerenciador de matrizes no campo **Nome de exibição**.
 - b. No campo **tipo de SRA**, selecione **adaptador de replicação de armazenamento NetApp para ONTAP**.
 - c. Insira as informações para se conectar ao cluster ou ao SVM:
 - Se você estiver se conectando a um cluster, deverá inserir o LIF de gerenciamento de cluster.
 - Se você estiver se conectando diretamente a uma SVM, insira o endereço IP do LIF de gerenciamento da SVM.



Ao configurar o gerenciador de array, você deve usar a mesma conexão (endereço IP) para o sistema de storage usado para integrar o sistema de storage nas ferramentas do ONTAP para VMware vSphere. Por exemplo, se a configuração do gerenciador de array for SVM com escopo, o storage em ferramentas do ONTAP para VMware vSphere deve ser adicionado ao nível da SVM.

- d. Se você estiver se conectando a um cluster, digite o nome do SVM no campo **Nome do SVM**.

Você também pode deixar este campo em branco.

e. Insira os volumes a serem descobertos no campo **Lista de inclusão de volume**.

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

Por exemplo, se você quiser descobrir o volume *src_vol1* que está em um relacionamento 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.

f. **(Opcional)** Digite os volumes a serem excluídos da descoberta no campo **Lista de exclusão de volume**.

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

Por exemplo, se você quiser excluir o volume *src_vol1* que está em um relacionamento 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 **seguinte**.

4. Verifique se o array é descoberto e exibido na parte inferior da janela Add Array Manager e selecione **Finish**.

Você pode seguir as mesmas etapas para o local de recuperação usando os endereços IP e as credenciais apropriadas de gerenciamento da SVM. Na tela Habilitar pares de matrizes do assistente Adicionar Gestor de matrizes, você deve verificar se o par de matrizes correto está selecionado e se mostra pronto para ser ativado.

Verificar sistemas de storage replicados

Você deve verificar se o site protegido e o site de recuperação foram emparelhados com êxito após a configuração do adaptador de replicação de armazenamento (SRA). O sistema de storage replicado deve ser detetável tanto pelo local protegido quanto pelo local de recuperação.

Antes de começar

- Você deve ter configurado seu sistema de storage.
- Você deve ter emparelhado o site protegido e o site de recuperação usando o gerenciador de array 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 programações do SnapMirror nos sites de origem e destino.

Passos

1. Faça login no vCenter Server.
2. Navegue até **Site Recovery > Array Based Replication**.
3. Selecione o par de matrizes necessário e verifique os detalhes correspondentes.

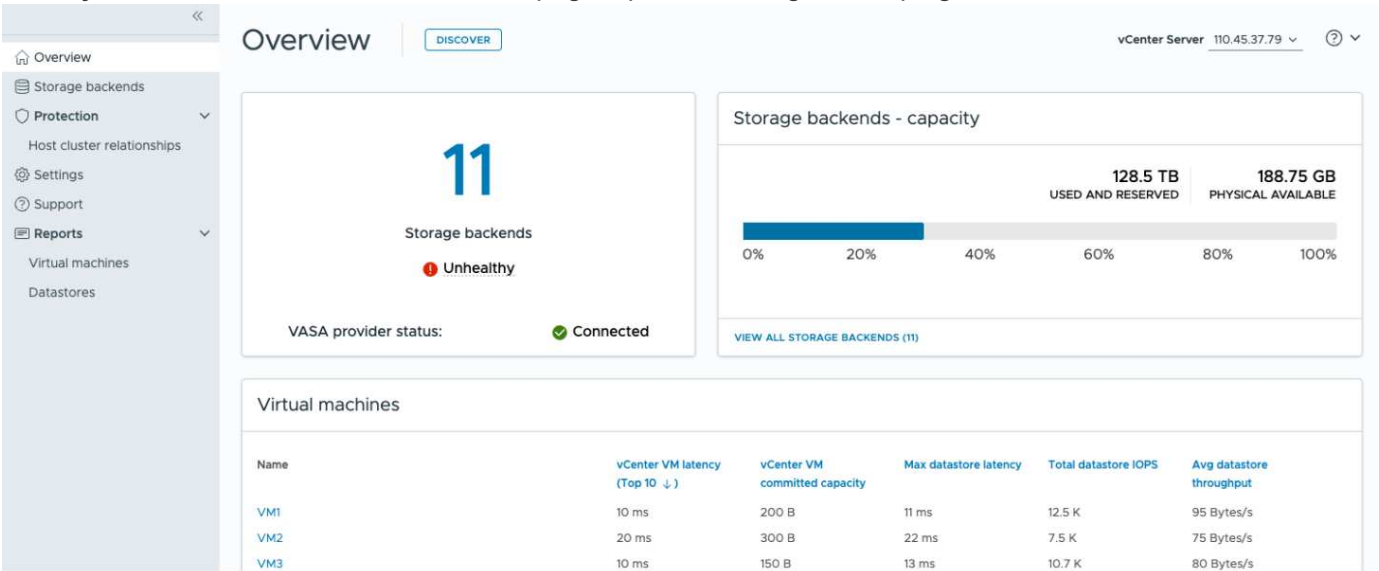
Os sistemas de armazenamento devem ser descobertos no local protegido e no local de recuperação com o Status como ""habilitado"".

Gerenciar as ferramentas do ONTAP para VMware vSphere

Visão geral das ferramentas do ONTAP para o painel do VMware vSphere

Quando você seleciona o ícone de plug-in das ferramentas do ONTAP para VMware vSphere na seção de atalhos no cliente vCenter, a interface do usuário navega para a página de visão geral. Essa página funciona como o painel que fornece o resumo das ferramentas do ONTAP para o plug-in do VMware vSphere.

No caso da configuração Enhanced Linked Mode (ELM), o menu suspenso vCenter Server SELECT (seleção do vCenter Server) é exibido e você pode selecionar um vCenter Server desejado para ver os dados relevantes a ele. Esta lista suspensa está disponível para todas as outras visualizações de listagem do plugin. A seleção do vCenter Server feita em uma página persiste nas guias do plug-in.



Na página de visão geral, você pode executar a ação **Discovery**. A ação de descoberta executa a descoberta no nível do vCenter para detectar quaisquer backends de storage, hosts, datastores e status/relacionamentos de proteção recém-adicionados ou atualizados. Você pode executar uma descoberta sob demanda de entidades sem ter que esperar pela descoberta agendada.



O botão Action (Ação) só será ativado se tiver o privilégio de executar a ação de descoberta.

Depois que a solicitação de descoberta for enviada, você poderá acompanhar o andamento da ação no painel tarefas recentes.

O painel de instrumentos tem vários cartões que mostram diferentes elementos do sistema. A tabela a seguir mostra as diferentes cartas e o que elas representam.

Cartão	Descrição
--------	-----------

Estado	O cartão Status mostra o número de backends de armazenamento e o status geral dos backends de armazenamento e do provedor VASA. O status dos backends de armazenamento mostra saudável quando todo o status dos backends de armazenamento é normal e mostra insalubre se algum dos backends de armazenamento tiver um problema (status desconhecido/inalcunçável/degradado). Selecione a dica da ferramenta para abrir os detalhes de status dos backends de armazenamento. Você pode selecionar qualquer back-end de armazenamento para obter mais detalhes. O link outros estados do provedor VASA mostra o estado atual do provedor VASA registrado no vCenter Server.
Back-ends de armazenamento - capacidade	Este cartão mostra a capacidade agregada usada e disponível de todos os backends de armazenamento para a instância do vCenter Server selecionada. No caso de sistemas de storage ASA R2, os dados de capacidade não são exibidos, pois são sistemas desagregados.
Máquinas virtuais	Esta placa mostra as 10 principais VMs classificadas por métrica de desempenho. Você pode selecionar o cabeçalho para obter as 10 principais VMs para a métrica selecionada ordenadas por ordem crescente ou decrescente. As alterações de classificação e filtragem feitas no cartão persistem até que você altere ou limpe o cache do navegador.
Armazenamentos de dados	Este cartão mostra 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 por ordem ascendente ou descendente. As alterações de classificação e filtragem feitas no cartão persistem até que você altere ou limpe o cache do navegador. Há uma lista suspensa tipo de datastore para selecionar o tipo de datastores - NFS, VMFS ou vVols.
Placa de conformidade do host ESXi	Esta placa mostra o status geral de conformidade de todos os hosts ESXi (para o vCenter selecionado) com relação às configurações recomendadas do host NetApp por grupo/categoria de configurações. Você pode selecionar o link Apply Recommended Settings (aplicar configurações recomendadas) para aplicar as configurações recomendadas. Você pode selecionar o status de conformidade dos hosts para ver a lista de hosts.

Interface de usuário do Gerenciador de ferramentas do ONTAP

As ferramentas do ONTAP para VMware vSphere são um sistema de alocação a vários clientes que pode gerenciar várias instâncias do vCenter Server. O Gerenciador de ferramentas do ONTAP fornece mais controle às ferramentas do ONTAP para o administrador do VMware vSphere sobre as instâncias gerenciadas do vCenter Server e os back-ends de storage integrados.

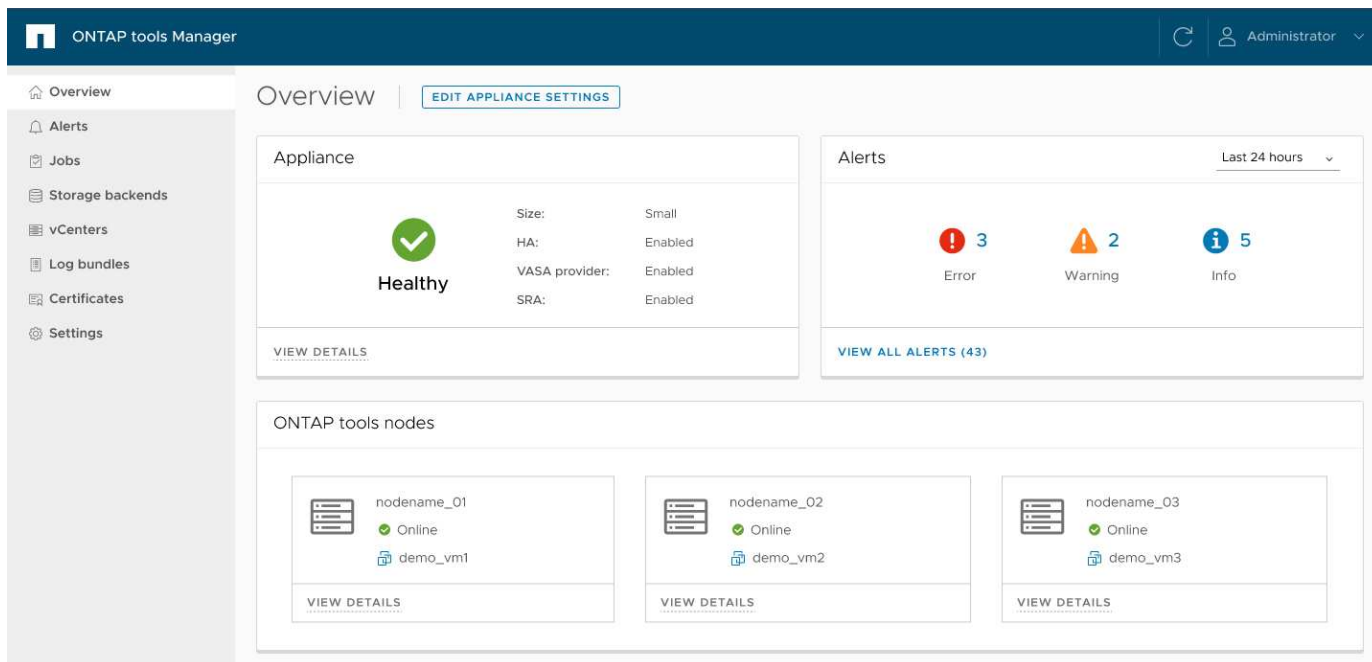
O Gerenciador de ferramentas do ONTAP ajuda a:

- Gerenciamento de instâncias do vCenter Server - Adicione e gerencie instâncias do vCenter Server às ferramentas do ONTAP.
- Gerenciamento de back-end de storage: Adicione e gerencie clusters de storage do ONTAP às ferramentas do ONTAP para VMware vSphere e mapeie-os para instâncias integradas do vCenter Server globalmente.
- Downloads do pacote de log - colete arquivos de log para as ferramentas do ONTAP para VMware vSphere.
- Gerenciamento de certificados - altere o certificado auto-assinado para um certificado CA personalizado e renove ou atualize todos os certificados do provedor VASA e das ferramentas do ONTAP.
- Gerenciamento de senhas - Redefina a senha do aplicativo OVA do usuário.

Para acessar o Gerenciador de ferramentas do ONTAP, inicie a

<https://<ONTAPtoolsIP>:8443/virtualization/ui/> partir do navegador e faça login com as ferramentas do ONTAP para as credenciais de administrador do VMware vSphere fornecidas durante a implantação.

A seção de visão geral do Gerenciador de ferramentas do ONTAP ajuda a gerenciar a configuração do dispositivo, como gerenciamento de serviços, aumento do tamanho dos nós e capacitação de alta disponibilidade (HA). Você também pode monitorar as informações gerais das ferramentas do ONTAP relacionadas aos nós, como integridade, detalhes da rede e alertas.



Cartão	Descrição
Cartão do aparelho	O cartão de dispositivo fornece o status geral do dispositivo ONTAP Tools. Ele mostra os detalhes de configuração do dispositivo e o status dos serviços habilitados. Para obter informações adicionais sobre o dispositivo ONTAP Tools, selecione o link Exibir detalhes . Quando um trabalho de ação de configuração de dispositivo de edição está em andamento, o portlet do dispositivo mostra o status e os detalhes do trabalho.
Cartão de alertas	A placa Alertas lista os alertas das ferramentas do ONTAP por tipo, incluindo os alertas no nível do nó de HA. Pode ver a lista de alertas selecionando no texto de contagem (hiperligação). A ligação encaminha-o para a página de visualização de alertas filtrada pelo tipo selecionado.
Placa de nós de ferramentas do ONTAP	A placa de nós de ferramentas do ONTAP mostra a lista de nós com nome do nó, nome da VM do nó, status e todos os dados relacionados à rede. Você pode selecionar em Exibir detalhes para exibir os detalhes adicionais relacionados ao nó selecionado. [NOTA] em uma configuração que não seja de HA, somente um nó é exibido. Na configuração de HA, três nós são mostrados.

Entenda igroups e políticas de exportação em ferramentas ONTAP para VMware vSphere

Grupos iniciadores (igroups) são tabelas de nomes de portas mundiais (WWPNs) de hosts de protocolo FC ou nomes de nós qualificados de hosts iSCSI. Você pode definir

grupos e mapeá-los para LUNs para controlar quais iniciadores têm acesso a LUNs.

Nas ferramentas ONTAP para VMware vSphere 9.x, os igroups eram criados e gerenciados em uma estrutura plana, onde cada datastore no vCenter era associado a um único igroup. Esse modelo limitava a flexibilidade e a reutilização de igroups em múltiplos datastores. As ferramentas ONTAP para VMware vSphere 10.x introduzem igroups aninhados, onde cada datastore no vCenter é associado a um igroup pai, enquanto cada host é vinculado a um igroup filho sob esse pai. Você pode definir igroups pais personalizados com nomes definidos pelo usuário para reutilização em vários armazenamentos de dados, permitindo um gerenciamento mais flexível e interconectado de igroups. Entender o fluxo de trabalho dos igroups é essencial para gerenciar LUNs e datastores de forma eficaz nas ferramentas ONTAP para 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 de igroups reais. Os igroups gerenciados pelas ferramentas ONTAP usam o prefixo "otv_". Igroups personalizados podem receber qualquer nome.

Prazo	Descrição
DS<número>	Armazenamento de dados
iqn<número>	IQN do iniciador
host<número>	Anfitrião MoRef
lun<número>	ID LUN
<NomeDS>Grupol<número>	igroup pai padrão (gerenciado por ferramentas ONTAP)
<Host-Moref>Igroup<número>	igroup infantil
CustomIgroup<número>	igroup pai personalizado definido pelo usuário
ClassicIgroup<número>	Igroup usado nas versões 9.x das ferramentas ONTAP.

Exemplo 1:

Crie um armazenamento de dados em um único host com um iniciador

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

Resultado:

- DS1Igroup:
 - host1Igroup → (iqn1: lun1)

Um igroup pai, DS1Igroup, é criado nos sistemas ONTAP para DS1, com um igroup filho, host1Igroup, mapeado para lun1. LUNs são sempre mapeados para igroups filhos.

Exemplo 2:

Montar o armazenamento de dados existente em um host adicional

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

Resultado:

- DS1lgroup:
 - host1lgroup → (iqn1: lun1)
 - host2lgroup → (iqn2: lun1)

Um igroup filho host2lgroup é criado e adicionado ao igroup pai existente DS1lgroup.

Exemplo 3:

Desmontar um armazenamento de dados de um host

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

Resultado:

- DS1lgroup:
 - host2lgroup → (iqn2: lun1)

O host1lgroup é removido da hierarquia. Os igroups filhos não são excluídos explicitamente. A exclusão ocorre sob estas duas condições: • Se nenhum LUN for mapeado, o sistema ONTAP exclui o igroup filho. • Uma tarefa de limpeza agendada remove os igroups filhos pendentes sem mapeamentos de LUN. Esses cenários se aplicam apenas a igroups gerenciados por ferramentas ONTAP, não a igroups criados de forma personalizada.

Exemplo 4:

Excluir armazenamento de dados

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

Resultado:

- DS1lgroup:
 - host2lgroup → (iqn2: lun1)

Os igroups pai e filho são removidos se outro repositório de dados não reutilizar o igroup pai. Os igroups filhos nunca são excluídos explicitamente.

Exemplo 5:

Crie vários armazenamentos de dados em 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)

O Customlgroup1 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 LUNs relevantes.

Exemplo 6:

Exclua um armazenamento de dados em um igroup pai personalizado.

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

Resultado:

- CustomIgroup1:
 - host1Igroup → (iqn1: lun3)
 - host3Igroup → (iqn3: lun3)
- Mesmo que CustomIgroup1 não seja reutilizado, ele não é excluído.
- Se nenhum LUN for mapeado, o sistema ONTAP excluirá o host2Igroup.
- O host1Igroup não é excluído, pois é mapeado para lun3 do DS3. Igroups personalizados nunca são excluídos, independentemente do status de reutilização.

Exemplo 7:

Expandir o armazenamento de dados vVols (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 o armazenamento de dados 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) não está mapeado do igroup filho. O igroup permanece ativo enquanto tiver pelo menos um LUN mapeado.

Exemplo 9:

Migração das ferramentas ONTAP 9 para 10 (normalização igroup)

Fluxo de trabalho

As ferramentas ONTAP para VMware vSphere 9.x não oferecem suporte a 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) → Classicgroup1 (iqn6 e iqn7: lun6, lun7)

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

Após a migração:

[Migração] DS6 (lun6, lun7): host6 (iqn6), host7 (iqn7) → Classicgroup1: otv_Classicgroup1 (iqn6 e iqn7: lun6, lun7)

Durante a migração:

- Um novo igroup pai (Classicgroup1) é criado.
- O igroup original é renomeado com o prefixo otv_ e se torna um igroup filho.

Isso garante a conformidade com o modelo hierárquico.

Tópicos relacionados

["Sobre os grupos"](#)

Políticas de exportação

As políticas de exportação controlam o acesso aos datastores NFS nas ferramentas ONTAP para VMware vSphere. Elas definem quais clientes podem acessar os datastores e quais permissões eles têm. As políticas de exportação são criadas e gerenciadas em sistemas ONTAP e podem ser associadas aos 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 acesso e as permissões concedidas (somente leitura ou leitura/gravação).

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

Ao montar um repositório de dados NFS em um novo host ESXi, as ferramentas ONTAP para VMware vSphere adicionam o endereço IP do host à política de exportação existente associada ao repositório de dados. Isso permite que o novo host acesse o repositório de dados sem criar uma nova política de exportação.

Ao excluir ou desmontar um repositório de dados NFS de um host ESXi, o 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 repositório de dados NFS, o ONTAP Tools for VMware

vSphere remove a política de exportação associada a esse repositório de dados se ela não for reutilizada por outros repositórios de dados. Se a política de exportação for reutilizada, ela manterá o endereço IP do host e permanecerá inalterada. Ao excluir os repositórios de dados, 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 repositórios de dados. Ao reutilizar a política de exportação, você pode anexá-la ao novo endereço IP do host. Ao excluir ou desmontar um repositório de dados 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 repositórios de dados. A reutilização de políticas de exportação não é recomendada, pois pode levar a problemas de acesso e latência.

Tópicos relacionados

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

Habilite as ferramentas do ONTAP para os serviços do VMware vSphere

Gerenciador para habilitar serviços como o provedor VASA, importação de configuração vVols e recuperação de desastres (SRA) usando o Gerenciador de ferramentas do ONTAP.

Passos

1. Inicie o Gerenciador de ferramentas do ONTAP a partir de um navegador da Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as ferramentas do ONTAP para as credenciais de administrador do VMware vSphere fornecidas durante a implantação.
3. Selecione **Edit Appliance Settings** (Editar definições do dispositivo) na seção Overview (Descrição geral).
4. Na seção **Serviços**, você pode habilitar serviços opcionais como o provedor VASA, a importação de configuração vVols e a recuperação de desastres (SRA) de acordo com suas necessidades.

Ao ativar os serviços pela primeira vez, você deve criar as credenciais do provedor VASA e do SRA. Eles são usados para Registrar ou habilitar o provedor VASA e os serviços SRA no vCenter Server.



Antes de desativar quaisquer serviços opcionais, certifique-se de que as ferramentas vCenter Servers gerenciados pelo ONTAP não os usem.

A opção **Allow import of vVols Configuration** é mostrada somente quando o serviço do provedor VASA está habilitado. Esta opção permite a migração de dados vVols das ferramentas ONTAP 9.x para as ferramentas ONTAP 10,3.

Alterar as ferramentas do ONTAP para a configuração do VMware vSphere

Usando o Gerenciador de ferramentas do ONTAP, faça a escalabilidade vertical das ferramentas do ONTAP para a configuração do VMware vSphere para aumentar o

número de nós na implantação ou alterar a configuração para a configuração de alta disponibilidade (HA). As ferramentas do ONTAP para o dispositivo VMware vSphere são implantadas inicialmente em uma configuração de nó único que não é de HA.

Antes de começar

- Certifique-se de que o seu MODELO OVA tem a mesma versão OVA que o nó 1. O nó 1 é o nó padrão em que as ferramentas do ONTAP para o VMware vSphere OVA são implantadas inicialmente.
- Certifique-se de que o hot add e o hot plug de memória da CPU estejam ativados.

Passos

1. Inicie o Gerenciador de ferramentas do ONTAP a partir de um navegador da Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as ferramentas do ONTAP para as credenciais de administrador do VMware vSphere fornecidas durante a implantação.
3. Selecione **Edit Appliance Settings** (Editar definições do dispositivo) na seção Overview (Descrição geral).
4. Na seção **Configuração**, você pode fazer a escalabilidade vertical para aumentar o tamanho do nó e ativar a configuração de HA de acordo com suas necessidades. Você precisa das credenciais do vCenter Server para fazer quaisquer alterações.

Quando as ferramentas do ONTAP estão na configuração HA, você pode alterar os detalhes da biblioteca de conteúdo. Você deve fornecer a senha novamente para o novo envio de edição.



Nas ferramentas do ONTAP para VMware vSphere, você só tem permissão para aumentar o tamanho do nó; não pode reduzir o tamanho do nó. Em uma configuração não HA, apenas uma configuração de tamanho médio é suportada. Em uma configuração de HA, configurações médias e grandes são suportadas.

5. Utilize o botão de alternância HA para ativar a configuração HA. Na página **HA settings**, certifique-se de que:
 - A biblioteca de conteúdo pertence ao mesmo vCenter Server onde as VMs de nó de ferramentas do ONTAP são executadas. As credenciais do vCenter Server são usadas para validar e baixar o modelo OVA para alterações de dispositivo.
 - A máquina virtual que hospeda as ferramentas do ONTAP não é implantada diretamente em um host ESXi. A VM deve ser implantada em um cluster ou em um pool de recursos.



Depois que a configuração de HA estiver ativada, você não poderá reverter para uma configuração de nó único que não seja de HA.

6. Na seção **HA settings** da janela **Edit Appliance Settings** (Editar configurações do dispositivo), você pode inserir os detalhes dos nós 2 e 3. As ferramentas do ONTAP para VMware vSphere são compatíveis com três nós na configuração de HA.



A maioria das opções de entrada são pré-preenchidas com os detalhes da rede do nó 1 para facilitar o fluxo de trabalho. No entanto, você pode editar os dados de entrada antes de navegar para a página final do assistente. Você pode inserir detalhes de endereço IPv6 para os outros dois nós somente quando o endereço IPv6 estiver ativado no primeiro nó.

Certifique-se de que um host ESXi contenha apenas uma VM de ferramentas ONTAP. As entradas são

validadas cada vez que você passa para a próxima janela.

7. Revise os detalhes na seção **Resumo** e **Salvar** as alterações.

O que se segue?

A página **Visão geral** mostra o status da implantação. Utilizando a ID do trabalho, também pode controlar o estado do trabalho de definições do dispositivo de edição a partir da vista trabalhos.

Se a implantação de HA falhar e o status do novo nó for exibido como "novo", exclua a nova VM no vCenter antes de tentar novamente a operação Habilitar HA.

A guia **Alertas** no painel esquerdo lista alertas de ferramentas do ONTAP para VMware vSphere.

Gerenciar armazenamentos de dados

Montar armazenamentos de dados NFS e VMFS

A montagem de um datastore fornece acesso ao storage a hosts adicionais. Você pode montar o datastore nos hosts adicionais depois de adicionar os hosts ao seu ambiente VMware.

Sobre esta tarefa

- Algumas ações com o botão direito do Mouse são desativadas ou indisponíveis dependendo da versão do cliente vSphere e do tipo de datastore selecionado.
 - Se você estiver usando o vSphere Client 8,0 ou versões posteriores, algumas das opções de clique com o botão direito do Mouse ficam ocultas.
 - Das versões vSphere 7.0U3 ao vSphere 8,0, mesmo que as opções apareçam, a ação será desativada.
- A opção Mount datastore é desativada quando o cluster de host é protegido com configurações uniformes.

Passos

1. Na página inicial do vSphere Client, selecione **hosts and clusters**.
2. No painel de navegação esquerdo, selecione os data centers que contêm os hosts.
3. Para montar datastores NFS/VMFS no cluster de host ou host, clique com o botão direito do Mouse e selecione **Ferramentas NetApp ONTAP > montar datastores**.
4. Selecione os armazenamentos de dados que você deseja montar e selecione **Mount**.

O que se segue?

Você pode acompanhar o progresso no painel de tarefas recentes.

Desmonte armazenamentos de dados NFS e VMFS

A ação desmontar datastore desmonta um datastore NFS ou VMFS dos hosts ESXi. A ação desmontar datastore está habilitada para armazenamentos de dados NFS e VMFS que são descobertos ou gerenciados pelas ferramentas do ONTAP para VMware vSphere.

Passos

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

Uma caixa de diálogo é aberta e lista os hosts ESXi nos quais o datastore está montado. Quando a operação é executada 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 do usuário sugere que você use a operação delete datastore em vez disso.

4. Selecione o botão **Desmontar**.

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



Se o datastore protegido estiver desmontado, a configuração de proteção de saída pode resultar em proteção parcial. "[Modificar cluster de host protegido](#)" Consulte para ativar a proteção completa.

O que se segue?

Você pode acompanhar o progresso no painel tarefas recentes.

Montar um datastore vVols

É possível montar um armazenamento de dados do VMware Virtual volumes (vVols) em um ou mais hosts adicionais para fornecer acesso ao storage a hosts adicionais. Você pode desmontar o armazenamento de dados vVols somente por meio das APIs.

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 no datastore e selecione **NetApp ONTAP Tools > Mount datastore**.
4. Na caixa de diálogo **montar datastores em hosts**, selecione os hosts nos quais deseja montar o datastore e, em seguida, selecione **montar**.

Você pode acompanhar o progresso no painel de tarefas recentes.

Redimensione o armazenamento de dados NFS e VMFS

O redimensionamento de um datastore permite aumentar o armazenamento de seus arquivos de máquina virtual. Você pode alterar o tamanho de um armazenamento de dados conforme os requisitos de infraestrutura mudam.

Sobre esta tarefa

Você só pode aumentar o tamanho de um datastores NFS e VMFS. Um FlexVol volume que faz parte de um datastores NFS e VMFS não pode diminuir abaixo do tamanho existente, mas pode crescer no máximo 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 **Ferramentas NetApp ONTAP > Redimensionar datastore**.
4. Na caixa de diálogo Redimensionar, especifique um novo tamanho para o datastore e selecione **OK**.

Expanda o armazenamento de dados vVols

Quando você clica com o botão direito do Mouse no objeto datastore na visualização de objetos do vCenter, as ferramentas do ONTAP para ações compatíveis com o VMware vSphere são mostradas na seção plug-in. Ações específicas são ativadas dependendo do tipo de armazenamento de dados e do usuário atual Privileges.



A operação do armazenamento de dados Expand vVols não é aplicável ao armazenamento de dados vVols baseado no 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 > Add storage to datastore**.
4. Na janela **criar ou Selecionar volumes**, você pode criar novos volumes ou escolher entre os volumes existentes. A interface do utilizador é auto-explicativa. Siga as instruções conforme sua escolha.
5. Na janela **Summary**, revise as seleções e selecione **Expand**. Você pode acompanhar o progresso no painel tarefas recentes.

Diminua o armazenamento de dados do vVols

A ação Excluir datastore exclui o datastore quando não há vVols no datastore selecionado.



A operação do armazenamento de dados do vVols não é compatível com o armazenamento de dados vVols baseado no 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 > Remove storage from datastore**.
4. Selecione volumes que não tenham vVols e selecione **Remover**.



A opção para selecionar o volume no qual o vVols está residindo está desativada.

5. Na janela pop-up **Remover armazenamento**, marque **Excluir volumes do cluster ONTAP** para excluir os volumes do armazenamento de dados e do armazenamento ONTAP e selecione **Excluir**.

Excluir datastores

A ação de remoção do armazenamento de dados é suportada em todas as ferramentas do ONTAP para armazenamentos de dados vVols descobertos ou gerenciados do VMware vSphere no vCenter Server. Essa ação permite a remoção de volumes do datastore vVols.

A opção remover é desativada quando há vVols residentes em um volume específico. Além de remover volumes do datastore, você pode excluir o volume selecionado no storage ONTAP.

Excluir tarefa de armazenamento de dados das ferramentas do ONTAP para VMware vSphere no vCenter Server faz o seguinte:

- Desmonta o recipiente VVol.
- Limpa o igrop. Se o igrop não estiver em uso, remove o iqn do igrop.
- Elimina o recipiente Vvol.
- Deixa os volumes Flex no storage array.

Siga as etapas abaixo para excluir o armazenamento de dados NFS, VMFS ou vVOL de ferramentas do ONTAP do vCenter Server:

Passos

1. Faça login no cliente vSphere
2. Clique com o botão direito do Mouse em um sistema host ou em um cluster de host ou em um data center e selecione **NetApp ONTAP Tools > Delete datastore**.



Não é possível excluir os datastores se houver máquinas virtuais usando esse datastore. Você precisa mover as máquinas virtuais para um datastore diferente antes de excluir o datastore. Não é possível selecionar a caixa de verificação eliminação de volume se o datastore pertencer a um cluster de host protegido.

- a. No caso do armazenamento de dados NFS ou VMFS, uma caixa de diálogo aparece com a lista de VMs que estão usando o armazenamento de dados.
 - b. Se o datastore VMFS for criado em sistemas ASA R2 e se for parte da proteção, você precisará desproteger o datastore antes de excluí-lo.
 - c. No caso do datastore vVols, a ação Excluir datastore exclui o datastore somente quando não houver vVols associados a ele. A caixa de diálogo Excluir datastore fornece uma opção para excluir volumes do cluster ONTAP.
 - d. No caso do armazenamento de dados vVols baseado em sistemas ASA R2, a caixa de seleção para excluir os volumes de backup não é aplicável.
3. Para excluir os volumes de backup no armazenamento ONTAP, selecione **Excluir volumes no cluster ONTAP**.



Não é possível excluir o volume no cluster do ONTAP para um datastore VMFS que faça parte do cluster de host protegido.

Visualizações de storage do ONTAP para datastores

As ferramentas do ONTAP para VMware vSphere mostram a visualização lateral do storage do ONTAP dos datastores e seus volumes na guia configure.

Passos

1. No cliente vSphere, navegue até o datastore.
2. Selecione a guia **Configure** no painel direito.
3. Selecione **Ferramentas NetApp ONTAP > armazenamento ONTAP**. Dependendo do tipo de armazenamento de dados, a exibição muda. Consulte a tabela abaixo para obter informações:

Tipo de datastore	Informação disponível
Armazenamento de dados NFS	A página Detalhes do armazenamento contém backends de armazenamento, informações agregadas e de volume. A página de detalhes do NFS contém dados relacionados ao armazenamento de dados NFS.
Armazenamentos de dados VMFS	A página Detalhes do armazenamento contém informações de back-end, agregado e volume de armazenamento. A página detalhes do LUN contém dados relacionados ao LUN. A página detalhes do namespace contém dados relacionados ao namespace quando o datastore VMFS usa o protocolo NVMe/TCP ou NVMe/FC. Os detalhes de volume e agregado não são exibidos para armazenamentos de dados baseados no sistema de storage ASA R2.
Armazenamentos de dados vVols	Lista todos os volumes. Você pode expandir ou remover o armazenamento do painel de armazenamento do ONTAP. Essa exibição não é compatível com o armazenamento de dados vVols baseado no sistema do ASA R2.

Visualização de armazenamento de máquina virtual

A visualização de armazenamento mostra a lista de vVols criados pela máquina virtual.



Essa exibição é aplicável à VM que tem pelo menos uma ferramenta ONTAP para o disco relacionado ao armazenamento de dados vVols gerenciado do VMware vSphere montado nele.

Passos

1. No vSphere Client, navegue até a máquina virtual.
2. Selecione a guia **Monitor** no painel direito.
3. Selecione **Ferramentas NetApp ONTAP > armazenamento**. Os detalhes **Storage** aparecem no painel direito. Você pode ver a lista de vVols que estão presentes na VM.

Você pode usar a opção 'Gerenciar colunas' para ocultar ou mostrar diferentes colunas.

Gerenciar limites de storage

Você pode definir o limite para receber notificações no vCenter Server quando o volume e a capacidade agregada atingirem determinados níveis.

Passos:

1. Faça login no cliente vSphere
2. Na página atalhos, selecione **Ferramentas do NetApp ONTAP** na seção plug-ins.
3. No painel esquerdo das ferramentas do ONTAP, navegue até **Configurações > Configurações de limiar > Editar**.
4. Na janela **Edit Threshold** (Editar limite), forneça os valores desejados nos campos **Near Full** (quase completo) e **Full** (completo) e selecione **Save** (Guardar). Você pode redefinir os números para valores recomendados, que são 80 para quase cheio e 90 para cheio.

Gerenciar backends de armazenamento

Os backends de armazenamento são sistemas que os hosts ESXi usam para armazenamento de dados.

Descubra o armazenamento

É possível executar a descoberta de um back-end de storage sob demanda sem esperar que uma descoberta agendada atualize os detalhes do storage.

Siga os passos abaixo para descobrir os backends de armazenamento.

Passos

1. Faça login no cliente vSphere
2. Na página atalhos, selecione **Ferramentas do NetApp ONTAP** na seção plug-ins.
3. No painel esquerdo das ferramentas do ONTAP, navegue até **backends de armazenamento** e selecione um back-end de armazenamento.
4. Selecione o menu elipses verticais e selecione **Discover storage**

Você pode acompanhar o progresso no painel tarefas recentes.

Modificar backends de armazenamento

Siga as etapas nesta seção para modificar um back-end de armazenamento.

1. Faça login no cliente vSphere
2. Na página atalhos, selecione **Ferramentas do NetApp ONTAP** na seção plug-ins.
3. No painel esquerdo das ferramentas do ONTAP, navegue até **backends de armazenamento** e selecione um back-end de armazenamento.
4. Selecione o menu reticências verticais e selecione **Modificar** para modificar as credenciais ou o nome da porta. Você pode acompanhar o progresso no painel tarefas recentes.

Você pode executar a operação Modificar para clusters globais do ONTAP usando o Gerenciador de ferramentas do ONTAP seguindo as etapas a seguir.

1. Inicie o Gerenciador de ferramentas do ONTAP a partir de um navegador da Web:
<https://<ONTAPtoolsIP>:8443/virtualization/ui/>
2. Faça login com as ferramentas do ONTAP para as credenciais de administrador do VMware vSphere fornecidas durante a implantação.
3. Selecione backends de armazenamento na barra lateral.
4. Selecione o back-end de armazenamento que você deseja modificar.
5. Selecione o menu elipses verticais e selecione **Modificar**.
6. Você pode modificar as credenciais ou a porta. Digite **Nome de usuário** e **Senha** para modificar o back-end de armazenamento.

Remova as extremidades de armazenamento

Você precisa excluir todos os datastores anexados ao back-end de armazenamento antes de remover o back-end de armazenamento. Siga as etapas abaixo para remover um back-end de armazenamento.

1. Faça login no cliente vSphere
2. Na página atalhos, selecione **Ferramentas do NetApp ONTAP** na seção plug-ins.
3. No painel esquerdo das ferramentas do ONTAP, navegue até **backends de armazenamento** e selecione um back-end de armazenamento.
4. Selecione o menu elipses verticais e selecione **Remover**. Certifique-se de que o back-end de armazenamento não contenha nenhum datastore. Você pode acompanhar o progresso no painel tarefas recentes.

Você pode executar a operação de remoção de clusters globais do ONTAP usando o Gerenciador de ferramentas do ONTAP.

1. Inicie o Gerenciador de ferramentas do ONTAP a partir de um navegador da Web:
<https://<ONTAPtoolsIP>:8443/virtualization/ui/>
2. Faça login com as ferramentas do ONTAP para as credenciais de administrador do VMware vSphere fornecidas durante a implantação.
3. Selecione **backends de armazenamento** na barra lateral.
4. Selecione o back-end de armazenamento que você deseja remover
5. Selecione o menu elipses verticais e selecione **Remover**.

Visualização detalhada do back-end de storage

A página de back-end de armazenamento lista todos os backends de armazenamento. É possível realizar a descoberta de storage, modificar e remover operações nos back-ends de storage adicionados, e não na SVM filho individual no cluster.

Quando você seleciona o cluster pai ou o filho no back-end de armazenamento, você pode ver o resumo geral do componente. Quando você seleciona o cluster pai, você tem o menu suspenso ações a partir do qual você pode executar as operações de armazenamento de descoberta, modificação e remoção.

A página de resumo fornece os seguintes detalhes:

- Status do back-end de storage
- Informações de capacidade

- Informações básicas sobre a VM
- Informações de rede, como o endereço IP e a porta da rede. Para o SVM filho, as informações serão as mesmas que o back-end de storage pai.
- Privileges permitido e restrito para o back-end de storage. Para o SVM filho, as informações serão as mesmas que o back-end de storage pai. Os Privileges são exibidos apenas nos backends de armazenamento baseados em cluster. Se você adicionar SVM como back-end de storage, as informações do Privileges não serão exibidas.
- A visualização de detalhamento do cluster do ASA R2 não inclui a guia camadas locais quando a propriedade desagregada for definida como "verdadeira" para o SVM ou para o cluster.
- Para sistemas ASA R2 SVM, o portlet de capacidade não é mostrado. O portal de capacidade só é necessário quando a propriedade desagregada é definida como "verdadeiro" para o SVM ou cluster.
- Para sistemas ASA R2 SVM, a seção de informações básicas mostra o tipo de plataforma.

A guia interface fornece informações detalhadas sobre a interface.

A guia níveis locais fornece informações detalhadas sobre a lista de agregados.

Gerenciar instâncias do vCenter Server

As instâncias do vCenter Server são plataformas de gerenciamento central que permitem controlar hosts, máquinas virtuais e backends de armazenamento.

Dissociar os backends de armazenamento com a instância do vCenter Server

A página de listagem do vCenter Server mostra o número associado de backends de armazenamento. Cada instância do vCenter Server tem a opção de associar ou desassociar a um back-end de armazenamento.

Passos

1. Inicie o Gerenciador de ferramentas do ONTAP a partir de um navegador da Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as ferramentas do ONTAP para as credenciais de administrador do VMware vSphere fornecidas durante a implantação.
3. Selecione a instância do vCenter Server necessária na barra lateral.
4. Selecione as elipses verticais em relação ao vCenter Server que você deseja associar ou dissociar com backends de armazenamento.
5. Selecione **dissociar o back-end de armazenamento**.

Modifique uma instância do vCenter Server

Siga as etapas abaixo para modificar as instâncias do vCenter Server.

1. Inicie o Gerenciador de ferramentas do ONTAP a partir de um navegador da Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as ferramentas do ONTAP para as credenciais de administrador do VMware vSphere fornecidas durante a implantação.
3. Selecione a instância aplicável do vCenter Server na barra lateral
4. Selecione as elipses verticais em relação ao vCenter Server que você deseja modificar e selecione

Modificar.

5. Modifique os detalhes da instância do vCenter Server e selecione **Modificar**.

Remova uma instância do vCenter Server

Você precisa remover todos os backends de armazenamento conectados ao vCenter Server antes de removê-lo.

1. Inicie o Gerenciador de ferramentas do ONTAP a partir de um navegador da Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as ferramentas do ONTAP para as credenciais de administrador do VMware vSphere fornecidas durante a implantação.
3. Selecione as instâncias aplicáveis do vCenter Server na barra lateral
4. Selecione as elipses verticais em relação ao vCenter Server que você deseja remover e selecione **Remover**.



Depois de remover instâncias do vCenter Server, elas não serão mais mantidas pelo aplicativo.

Quando você remove instâncias do vCenter Server nas ferramentas do ONTAP, as seguintes ações são executadas automaticamente:

- O plug-in não está registrado.
- As funções plug-in Privileges e plug-in são removidas.

Gerenciar certificados

Um certificado autoassinado é gerado por padrão para as ferramentas do ONTAP e o provedor VASA durante a implantação. Usando a interface do Gerenciador de ferramentas do ONTAP, você pode renovar o certificado ou atualizá-lo para uma CA personalizada. Certificados de CA personalizados são obrigatórios em uma implantação multi-vCenter.

Antes de começar

- O nome de domínio no qual o certificado é emitido deve ser mapeado para o endereço IP virtual.
- Execute a verificação nslookup no nome de domínio para verificar se o domínio está sendo resolvido para o endereço IP pretendido.
- Os certificados devem ser criados com o nome de domínio e o endereço IP do balanceador de carga.



Um endereço IP do loadbalancer deve ser mapeado para um nome de domínio totalmente qualificado (FQDN). Os certificados devem conter o mesmo FQDN mapeado para o endereço IP do balanceador de carga em nomes alternativos de assunto ou assunto.



Não é possível alternar de um certificado assinado pela CA para um certificado autoassinado.

Atualize o certificado das ferramentas do ONTAP

A guia Ferramentas do ONTAP mostra detalhes como tipo de certificado (autoassinado/CA assinado) e nome de domínio. Durante a implantação, o certificado autoassinado é gerado por padrão. Você pode renovar o certificado ou atualizar o certificado para CA.

Passos

1. Inicie o Gerenciador de ferramentas do ONTAP a partir de um navegador da Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as ferramentas do ONTAP para as credenciais de administrador do VMware vSphere fornecidas durante a implantação.
3. Selecione **certificados > Ferramentas ONTAP > renovar** para renovar os certificados.

Você pode renovar o certificado se tiver expirado ou estiver próximo da data de validade. A opção renovar está disponível quando o tipo de certificado é assinado pela CA. Na janela pop-up, forneça os detalhes do certificado do servidor, da chave privada, da CA raiz e do certificado intermediário.



O sistema estará offline até que o certificado seja renovado e você será desconectado da interface do Gerenciador de ferramentas do ONTAP.

4. Para atualizar o certificado auto-assinado para certificado CA personalizado, selecione **certificados > Ferramentas ONTAP > Atualizar para CA** opção.
 - a. Na janela pop-up, carregue o certificado do servidor, a chave privada do certificado do servidor, o certificado da CA raiz e os ficheiros de certificado intermédios.
 - b. Introduza o nome de domínio para o qual gerou este certificado e atualize o certificado.



O sistema estará offline até que a atualização esteja concluída, e você será desconectado da interface do Gerenciador de ferramentas do ONTAP.

Atualize o certificado do fornecedor VASA

As ferramentas do ONTAP para o VMware vSphere são implantadas com um certificado autoassinado para o provedor VASA. Com isso, apenas uma instância do vCenter Server pode ser gerenciada para armazenamentos de dados vVols. Quando você gerencia várias instâncias do vCenter Server e deseja habilitar o recurso vVols nelas, você precisa alterar o certificado autoassinado para um certificado de CA personalizado.

Passos

1. Inicie o Gerenciador de ferramentas do ONTAP a partir de um navegador da Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as ferramentas do ONTAP para as credenciais de administrador do VMware vSphere fornecidas durante a implantação.
3. Selecione **certificados > Fornecedor VASA ou Ferramentas ONTAP > renovar** para renovar os certificados.
4. Selecione **certificados > Fornecedor VASA ou Ferramentas ONTAP > Upgrade para CA** para atualizar o certificado auto-assinado para certificado CA personalizado.
 - a. Na janela pop-up, carregue o certificado do servidor, a chave privada do certificado do servidor, o certificado da CA raiz e os ficheiros de certificado intermédios.
 - b. Introduza o nome de domínio para o qual gerou este certificado e atualize o certificado.



O sistema estará offline até que a atualização esteja concluída, e você será desconectado da interface do Gerenciador de ferramentas do ONTAP.

Acesse as ferramentas do ONTAP para o console de manutenção do VMware vSphere

Visão geral das ferramentas do ONTAP para o console de manutenção do VMware vSphere

Você pode gerenciar suas configurações de aplicativo, sistema e rede usando o console de manutenção das ferramentas do ONTAP. Pode alterar a palavra-passe do administrador e a palavra-passe de manutenção. Você também pode gerar pacotes de suporte, definir diferentes níveis de log, exibir e gerenciar configurações TLS e iniciar diagnósticos remotos.

Você deve ter as ferramentas VMware instaladas depois de implantar as ferramentas do ONTAP para o VMware vSphere para acessar o console de manutenção. Você deve usar `maint` como nome de usuário e senha configurados durante a implantação para fazer login no console de manutenção das ferramentas do ONTAP. Você deve usar **nano** para editar os arquivos em manutenção ou console de login root.



Você deve definir uma senha para `diag` o usuário ao ativar o diagnóstico remoto.

Você deve usar a guia **Resumo** das ferramentas do ONTAP implantadas para o VMware vSphere para acessar o console de manutenção. Quando você seleciona , o console de manutenção é iniciado.

Menu Console	Opções
Configuração da aplicação	1. Apresentar resumo do estado do servidor 2. Altere o nível DE LOG para os Serviços de fornecedores VASA e Serviços SRA 3. Desative o AutoSupport 4. Atualize o URL do proxy do AutoSupport
Configuração do sistema	1. Reinicie a máquina virtual 2. Encerre a máquina virtual 3. Altere a palavra-passe do utilizador 'não' 4. Alterar fuso horário 5. Adicionar novo servidor NTP 6. Aumentar o tamanho do disco de cadeia (/jail) 7. Atualização 8. Instale o VMware Tools

Configuração de rede	1. Apresentar definições de endereço IP 2. Exibir configurações de pesquisa de nome de domínio 3. Altere as configurações de pesquisa de nome de domínio 4. Apresentar rotas estáticas 5. Alterar rotas estáticas 6. Confirmar alterações 7. Faça ping em um host 8. Restaure as predefinições
Suporte e Diagnóstico	1. Aceder ao shell de diagnóstico 2. Ative o acesso de diagnóstico remoto 3. Forneça credenciais do vCenter para backup 4. Faça backup

Configure o acesso de diagnóstico remoto

Você pode configurar as ferramentas do ONTAP para o VMware vSphere para habilitar o acesso SSH para o usuário diag.

Antes de começar

A extensão do provedor VASA deve estar habilitada para sua instância do vCenter Server.

Sobre esta tarefa

Usar SSH para acessar a conta de usuário diag tem as seguintes limitações:

- Você só tem permissão para uma conta de login por ativação do SSH.
- O acesso SSH à conta de usuário diag é desativado quando uma das seguintes situações acontece:
 - O tempo expira.

A sessão de início de sessão permanece válida apenas até à meia-noite do dia seguinte.

- Você faz login como um usuário diag novamente usando SSH.

Passos

1. No vCenter Server, abra um console para o provedor VASA.
2. Inicie sessão como utilizador de manutenção.
3. Entre 4 para seleccionar suporte e Diagnóstico.
4. Entre 2 para seleccionar Ativar acesso ao diagnóstico remoto.
5. Introduza y na caixa de diálogo confirmação para ativar o acesso de diagnóstico remoto.
6. Introduza uma palavra-passe para acesso remoto ao diagnóstico.

Inicie o SSH em outros nós

Você precisa iniciar o SSH em outros nós antes de atualizar.

Antes de começar

A extensão do provedor VASA deve estar habilitada para sua instância do vCenter Server.

Sobre esta tarefa

Execute este procedimento em cada um dos nós antes de atualizar.

Passos

1. No vCenter Server, abra um console para o provedor VASA.
2. Inicie sessão como utilizador de manutenção.
3. Entre 4 para seleccionar suporte e Diagnóstico.
4. Introduza 1 para seleccionar Access diagnostic shell (Acesso à shell de diagnóstico).
5. Entre y para continuar.
6. Execute o comando *sudo systemctl restart ssh*.

Atualize as credenciais do vCenter Server e do ONTAP

Você pode atualizar a instância do vCenter Server e as credenciais do ONTAP usando o console de manutenção.

Antes de começar

Você precisa ter credenciais de login de usuário de manutenção.

Sobre esta tarefa

Se você tiver alterado as credenciais para a implantação pós-vCenter Server, ONTAP ou Data LIF, precisará atualizar as credenciais usando este procedimento.

Passos

1. No vCenter Server, abra um console para o provedor VASA.
2. Inicie sessão como utilizador de manutenção.
3. Entre 2 para seleccionar Menu Configuração do sistema.
4. Digite 9 para alterar as credenciais do ONTAP.
5. Digite 10 para alterar as credenciais do vCenter.

Relatórios de ferramentas do ONTAP

O plug-in das ferramentas do ONTAP para VMware vSphere fornece relatórios para máquinas virtuais e datastores. Quando você seleciona o ícone do plug-in das ferramentas do NetApp ONTAP para VMware vSphere na seção Atalhos do cliente vCenter, a interface do usuário navega para a página Visão geral. Selecione a guia relatórios para exibir a máquina virtual e o relatório de datastores.

O relatório de máquinas virtuais mostra a lista de máquinas virtuais descobertas (deve ter pelo menos um disco de datastores baseados em storage ONTAP) com métricas de desempenho. Quando você expande o Registro da VM, todas as informações do datastore relacionadas ao disco são exibidas.

O relatório de datastores mostra a lista de ferramentas descobertas ou reconhecidas do ONTAP para datastores gerenciados do VMware vSphere que são provisionados a partir do back-end de storage do ONTAP de todos os tipos com métricas de desempenho.

Você pode usar a opção Gerenciar colunas para ocultar ou mostrar diferentes colunas.

Recolha os ficheiros de registo

Você pode coletar arquivos de log para as ferramentas do ONTAP para VMware vSphere a partir das opções disponíveis na interface de usuário do Gerenciador de ferramentas do ONTAP. O suporte técnico pode solicitar que você colete os arquivos de log para ajudar a solucionar um problema.



A geração de logs a partir do Gerenciador de ferramentas do ONTAP inclui todos os logs para todas as instâncias do vCenter Server. A geração de logs a partir da interface de usuário do cliente vCenter é definida para o vCenter Server selecionado.

Passos

1. Inicie o Gerenciador de ferramentas do ONTAP a partir de um navegador da Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as ferramentas do ONTAP para as credenciais de administrador do VMware vSphere fornecidas durante a implantação.
3. Selecione **Log Bundles** na barra lateral.

Esta operação pode demorar vários minutos.

4. Selecione **Generate** para gerar os arquivos de log.
5. Insira o rótulo do Pacote de Log e selecione **Generate**.

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

Siga as etapas abaixo para gerar o pacote de log usando a interface do usuário do cliente vCenter:

Passos

1. Faça login no cliente vSphere
2. Na página inicial do vSphere Client, vá para **Support > Log bundle > Generate**.
3. Forneça o rótulo do pacote de log e gere o pacote de log. Você pode ver a opção de download quando os arquivos são gerados. O download pode levar algum tempo.



O pacote de log gerado substitui o pacote de log gerado nos últimos 3 dias ou 72 horas.

Gerenciar máquinas virtuais

Considerações para migrar ou clonar máquinas virtuais

Você deve estar ciente de algumas das considerações ao migrar máquinas virtuais existentes em seu data center.

Migrar máquinas virtuais protegidas

Você pode migrar as máquinas virtuais protegidas para:

- O mesmo datastore vVols em um host ESXi diferente
- Armazenamento de dados vVols compatível diferente no mesmo host ESXi
- Armazenamento de dados vVols compatível diferente em um host ESXi diferente

Se a máquina virtual for migrada para um FlexVol volume diferente, o respectivo arquivo de metadados também será atualizado com as informações da máquina virtual. Se uma máquina virtual for migrada para um host ESXi diferente, mas o mesmo armazenamento, o arquivo de metadados FlexVol volume subjacente não será modificado.

Máquinas virtuais protegidas contra clones

Você pode clonar máquinas virtuais protegidas para o seguinte:

- Mesmo contêiner do mesmo FlexVol volume usando o grupo de replicação

O arquivo de metadados do mesmo FlexVol volume é atualizado com os detalhes da máquina virtual clonada.

- Mesmo contêiner de um FlexVol volume diferente usando o grupo de replicação

O FlexVol volume onde a máquina virtual clonada é colocada, o arquivo de metadados é atualizado com os detalhes da máquina virtual clonada.

- Datastore diferente de contêiner ou vVols

O FlexVol volume onde a máquina virtual clonada é colocada, o arquivo de metadados recebe detalhes atualizados da máquina virtual.

Atualmente, a VMware não suporta máquinas virtuais clonadas para um modelo de VM.

É suportado clone-of-Clone de uma máquina virtual protegida.

```
https://docs.vmware.com/en/VMware-Horizon/2103/virtual-desktops/GUID-B5020738-8649-4308-A8B0-70AF80527DF6.html["Criando uma Máquina Virtual para Clonagem"]Consulte para obter mais detalhes.
```

Instantâneos de máquina virtual

Atualmente, apenas instantâneos de máquina virtual sem memória são suportados. Se a máquina virtual tiver Snapshot com memória, a máquina virtual não será considerada para proteção.

Você também não pode proteger máquinas virtuais desprotegidas que tenham Snapshot de memória. Para

esta versão, espera-se que você exclua o instantâneo da memória antes de ativar a proteção para a máquina virtual.

Para o Windows VM com tipo de armazenamento ASA R2, quando você tirar um instantâneo da máquina virtual, ele será um instantâneo somente leitura. Quando há uma chamada de ativação para a VM, o provedor VASA cria um LUN usando o snapshot somente leitura e, em seguida, ele o habilita para IOPS. Durante a solicitação de desligamento, o provedor VASA exclui o LUN que foi criado e desativa o IOPS.

Migre máquinas virtuais com datastores NFS e VMFS para armazenamentos de dados vVols

É possível migrar máquinas virtuais de datastores NFS e VMFS para armazenamentos de dados de volumes virtuais (vVols) para aproveitar o gerenciamento de VM baseado em políticas e outros recursos do vVols. Os datastores do vVols permitem que você atenda a requisitos maiores de workload.

Antes de começar

Certifique-se de que o Fornecedor VASA não está em execução em nenhuma das máquinas virtuais que pretende migrar. Se você migrar uma máquina virtual que esteja executando o VASA Provider para um datastore vVols, não será possível executar nenhuma operação de gerenciamento, incluindo a ativação das máquinas virtuais que estão nos datastores vVols.

Sobre esta tarefa

Quando você migra de um datastore NFS e VMFS para um datastore vVols, o vCenter Server usa descarregamentos de APIs do vStorage para Array Integration (VAAI) ao mover dados de datastores VMFS, mas não de um arquivo VMDK NFS. As descargas VAAI normalmente reduzem a carga no host.

Passos

1. Clique com o botão direito do rato na máquina virtual que pretende migrar e selecione **migrar**.
2. Selecione **Change storage only** (alterar apenas armazenamento) e, em seguida, selecione **Next** (seguinte).
3. Selecione um formato de disco virtual, uma Política de armazenamento de VM e um datastore da evolução que corresponda aos recursos do datastore que você está migrando.
4. Revise as configurações e selecione **Finish**.

Limpeza VASA

Siga as etapas nesta seção para executar a limpeza VASA.



É recomendável que você remova todos os armazenamentos de dados vVols antes de executar a Limpeza VASA.

Passos

1. Desmarque o plug-in entrando no https://OTV_IP:8143/Register.html
2. Verifique se o plug-in não está mais disponível no vCenter Server.
3. Encerre as ferramentas do ONTAP para a VM VMware vSphere.
4. Excluir ferramentas do ONTAP para VM VMware vSphere.

Descubra sistemas de storage e hosts

Quando você executa pela primeira vez as ferramentas do ONTAP para VMware vSphere em um cliente vSphere, as ferramentas do ONTAP descobrem os hosts ESXi, suas exportações de LUNs e NFS, e os sistemas de storage NetApp que possuem esses LUNs e exportações.

Antes de começar

- Todos os hosts ESXi devem estar ligados e conectados.
- Todas as máquinas virtuais de armazenamento (SVMs) a serem descobertas devem estar em execução e cada nó de cluster deve ter pelo menos um LIF de dados configurado para o protocolo de armazenamento em uso (NFS ou iSCSI).

Sobre esta tarefa

Você pode descobrir novos sistemas de armazenamento ou atualizar informações sobre sistemas de armazenamento existentes para obter as informações mais recentes sobre capacidade e configuração a qualquer momento. Você também pode modificar as credenciais que as ferramentas do ONTAP para VMware vSphere usam para fazer login nos sistemas de storage.

Ao descobrir os sistemas de armazenamento, as ferramentas do ONTAP para VMware vSphere coletam 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 rato no centro de dados pretendido e selecione **Ferramentas NetApp ONTAP > Atualizar dados do anfitrião**.

Na caixa de diálogo **Confirm** (confirmar), confirme a sua escolha.

3. Selecione os controladores de armazenamento descobertos que têm o status `Authentication Failure` e selecione **ações > Modificar**.
4. Preencha as informações necessárias na caixa de diálogo **Modificar sistema de armazenamento**.
5. Repita as etapas 4 e 5 para todos os controladores de armazenamento com `Authentication Failure` status.

Depois que o processo de descoberta estiver concluído, execute as seguintes ações:

- Use as ferramentas do ONTAP para VMware vSphere para configurar as configurações do host ESXi para hosts que exibem o ícone de alerta na coluna Configurações do adaptador, na coluna Configurações do MPIO ou na coluna Configurações de NFS.
- Forneça as credenciais do sistema de storage.

Modifique as configurações do host ESXi usando as ferramentas do ONTAP

Você pode usar o painel das ferramentas do ONTAP para o VMware vSphere para editar as configurações do host ESXi.

Antes de começar

Se houver um problema com as configurações do host ESXi, o problema será exibido no portlet dos sistemas host ESXi do painel. Você pode selecionar o problema para exibir o nome do host ou o endereço IP do host ESXi que tem o problema.

Passos

1. Faça login no cliente vSphere
2. Na página atalhos, selecione **Ferramentas do NetApp ONTAP** na seção plug-ins.
3. Vá para **portlet de conformidade do host ESXi** na Visão geral (painel) das ferramentas do ONTAP para o plug-in do VMware vSphere.
4. Selecione o link **Apply Recommended Settings** (aplicar configurações recomendadas).
5. Na janela **Apply Recommended host settings** (aplicar configurações de host recomendadas), selecione os hosts que você deseja cumprir com as configurações de host recomendadas pelo NetApp e selecione **Next** (Avançar).



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

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

Informações relacionadas

["Configure as configurações do host ESXi"](#)

Gerenciar senhas

Alterar a senha do Gerenciador de ferramentas do ONTAP

Você pode alterar a senha do administrador usando o Gerenciador de ferramentas do ONTAP.

Passos

1. Inicie o Gerenciador de ferramentas do ONTAP a partir de um navegador da Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as ferramentas do ONTAP para as credenciais de administrador do VMware vSphere fornecidas durante a implantação.
3. Selecione o ícone **administrador** no canto superior direito da tela e selecione **alterar senha**.
4. Na janela pop-up alterar senha, insira a senha antiga e os detalhes da nova senha. A restrição para alterar a palavra-passe é apresentada no ecrã da interface do utilizador.
5. Selecione **alterar** para implementar as alterações.

Redefinir a senha do Gerenciador de ferramentas do ONTAP

Se você Esqueceu a senha do Gerenciador de ferramentas do ONTAP, poderá redefinir as credenciais do administrador usando o token gerado pelas ferramentas do ONTAP para o console de manutenção do VMware vSphere.

Passos

1. Inicie o Gerenciador de ferramentas do ONTAP a partir de um navegador da Web:

`https://<ONTAPtoolsIP>:8443/virtualization/ui/`

2. No ecrã de início de sessão, selecione a opção **Repor palavra-passe**.

Para redefinir a senha do Gerenciador, você precisa gerar o token de redefinição usando as ferramentas do ONTAP para o console de manutenção do VMware vSphere.

- a. No vCenter Server, abra o console de manutenção
 - b. Introduza "2" para selecionar a opção System Configuration (Configuração do sistema)
 - c. Introduza '3' para alterar a palavra-passe do utilizador 'não'.
3. Na janela pop-up alterar senha, digite o token de redefinição de senha, o nome de usuário e os detalhes da nova senha.
 4. Selecione **Reset** para implementar as alterações. Na redefinição bem-sucedida da senha, você pode usar a nova senha para fazer login.

Repor a palavra-passe do utilizador da aplicação

A senha do usuário do aplicativo é usada para Registro do SRA e do provedor VASA com o vCenter Server.

Passos

1. Inicie o Gerenciador de ferramentas do ONTAP a partir de um navegador da Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Faça login com as ferramentas do ONTAP para as credenciais de administrador do VMware vSphere fornecidas durante a implantação.
3. Selecione **Configurações** na barra lateral.
4. Na tela **credenciais VASA/SRA**, selecione **Redefinir senha**.
5. Forneça uma nova senha e confirme as novas entradas de senha.
6. Selecione **Reset** para implementar as alterações.

Redefinir a senha do usuário do console de manutenção

Durante a operação de reinicialização do sistema operacional convidado, o menu grub exibe uma opção para redefinir a senha do usuário do console de manutenção. Esta opção é usada para atualizar a senha do usuário do console de manutenção presente na VM correspondente. Quando a senha de redefinição estiver concluída, a VM será reiniciada para definir a nova senha. No cenário de implantação do HA, após a reinicialização da VM, a senha é atualizada automaticamente nas outras duas VMs.

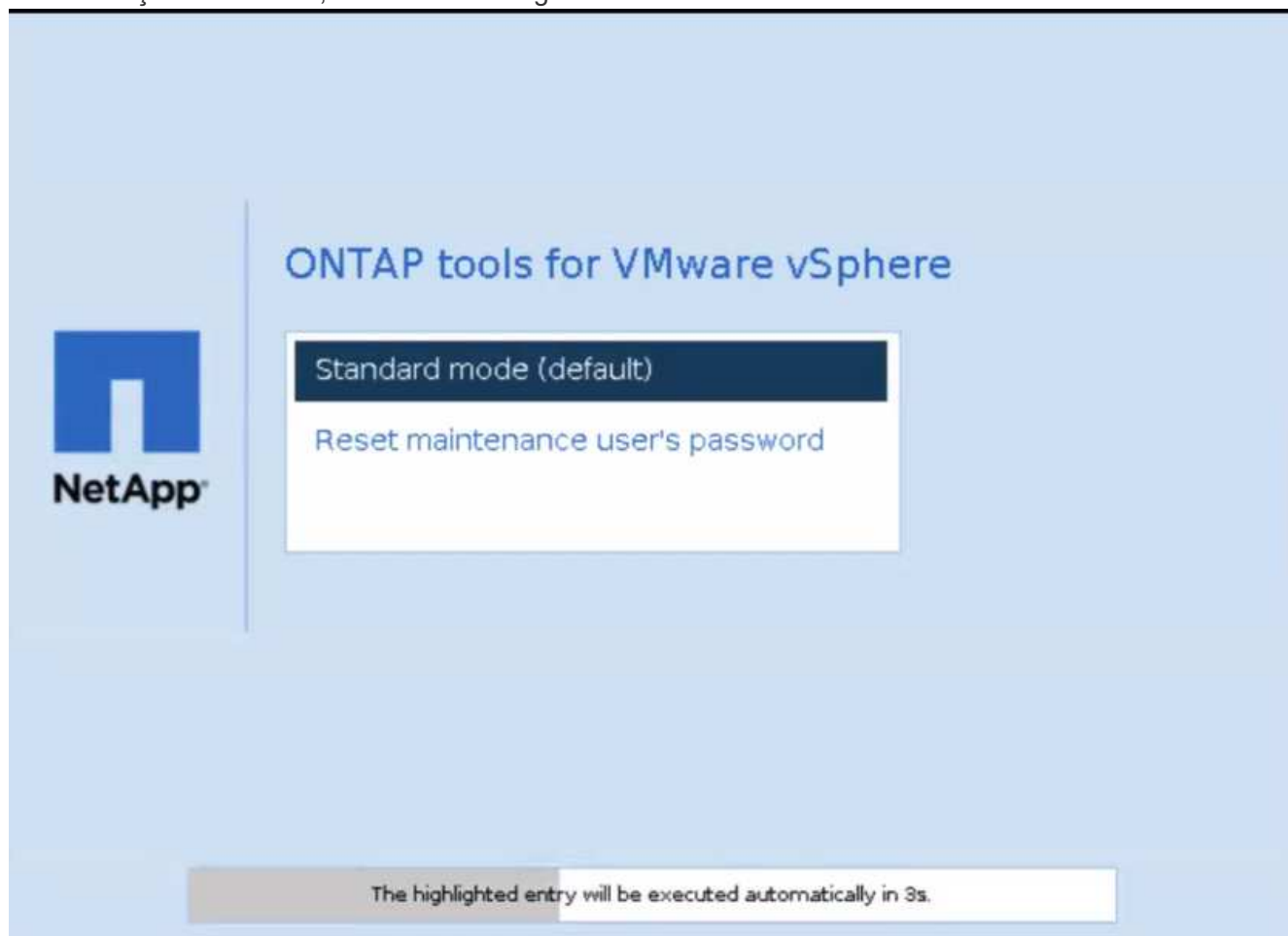


Para ferramentas ONTAP para implantação do VMware vSphere HA, você deve alterar a senha do usuário do console de manutenção no primeiro nó, que é node1.

Passos

1. Faça login no vCenter Server

2. Clique com o botão direito do Mouse na VM e selecione **Power > Restart Guest os** durante a reinicialização do sistema, você obtém a seguinte tela:



Você tem 5 segundos para escolher sua opção. Prima qualquer tecla para parar o progresso e congelar o menu GRUB.

3. Selecione a opção **Repor a senha do usuário de manutenção**. A consola de manutenção abre-se.
4. No console, insira os detalhes da nova senha. A nova palavra-passe e o novo tipo de dados da palavra-passe devem corresponder para repor a palavra-passe com êxito. Você tem três chances de inserir a senha correta. O sistema é reiniciado depois de introduzir com êxito a nova palavra-passe.
5. Pressione Enter para continuar. A senha é atualizada na VM.



O mesmo menu GRUB aparece durante a ativação da VM também. No entanto, você deve usar a opção redefinir senha somente com a opção **Restart Guest os**.

Gerenciar a proteção do cluster de host

Modificar cluster de host protegido

Você pode executar as seguintes tarefas como parte da proteção de modificação. Você pode executar todas as alterações no mesmo fluxo de trabalho.

- Adicione novos armazenamentos de dados ou hosts ao cluster protegido.

- Adicione novas relações SnapMirror às configurações de proteção.
- Exclua relacionamentos SnapMirror existentes das configurações de proteção.
- Modificar uma relação SnapMirror existente.

Monitorar a proteção do cluster de host

Use este procedimento para monitorar o status da proteção do cluster do host. Você pode monitorar cada cluster de host protegido, juntamente com seu estado de proteção, relacionamentos do SnapMirror, datastores e o status SnapMirror correspondente.

Passos

1. Faça login no cliente vSphere
2. Navegue até **Ferramentas do NetApp ONTAP > proteção > relacionamentos de cluster de host**.

O ícone sob a coluna de proteção mostra o status da proteção

3. Passe o Mouse sobre o ícone para ver mais detalhes.

Adicione novos armazenamentos de dados ou hosts

Use este procedimento para proteger os armazenamentos de dados ou hosts recém-adicionados. Você pode adicionar novos hosts ao cluster protegido ou criar novos datastores no cluster de host usando a interface de usuário nativa do vCenter.

Passos

1. Faça login no cliente vSphere
2. Para editar as propriedades de um cluster protegido, é possível
 - a. Navegue até **Ferramentas do NetApp ONTAP > proteção > relacionamentos de cluster de host**, selecione o menu de elipse no cluster e selecione **Editar** ou
 - b. Clique com o botão direito do Mouse em um cluster de host e selecione **NetApp ONTAP Tools > Protect Cluster**.
3. Se você tiver criado um datastore na interface de usuário nativa do vCenter, esse datastore será mostrado como desprotegido. A interface do usuário mostra todos os armazenamentos de dados no cluster e seu status de proteção em uma caixa de diálogo. Selecione o botão **Protect** para ativar a proteção completa.
4. Se você tiver adicionado um novo host ESXi, o status de proteção será exibido como parcialmente protegido. Selecione o menu de elipse nas configurações do SnapMirror e selecione **Editar** para definir a proximidade do host ESXi recém-adicionado.



No caso de relação de tipo assíncrono, a ação de edição não é suportada, pois não é possível adicionar o SVM de destino para local terciário à mesma instância de ferramentas do ONTAP. No entanto, você pode usar o gerente do sistema ou a CLI do SVM de destino para alterar a configuração do relacionamento.

5. Selecione **Salvar** depois de fazer as alterações necessárias.
6. Você pode ver as alterações na janela **Protect Cluster**.

Uma tarefa do vCenter é criada e você pode acompanhar o progresso no painel **tarefa recente**.

Adicione uma nova relação do SnapMirror

Passos

1. Faça login no cliente vSphere
2. Para editar as propriedades de um cluster protegido, é possível
 - a. Navegue até **Ferramentas do NetApp ONTAP > proteção > relacionamentos de cluster do host**, selecione o menu de elipse no cluster e selecione **Editar** ou
 - b. Clique com o botão direito do Mouse em um cluster de host e selecione **NetApp ONTAP Tools > Protect Cluster**.
3. Selecione **Adicionar relacionamento**.
4. Adicione um novo relacionamento como tipo de política **assíncrono** ou **AutomatedFailOverDuplex**.
5. Selecione **Protect**.

Você pode ver as alterações na janela **Protect Cluster**.

Uma tarefa do vCenter é criada e você pode acompanhar o progresso no painel **tarefa recente**.

Eliminar uma relação SnapMirror existente

Para excluir uma relação assíncrona do SnapMirror, o SVM ou cluster do local secundário devem ser adicionados como back-end de storage nas ferramentas do ONTAP para VMware vSphere. Não é possível eliminar todas as relações SnapMirror. Quando você exclui um relacionamento, o relacionamento respectivo no cluster do ONTAP também é removido. Quando você exclui uma relação de SnapMirror de failover automático, os armazenamentos de dados no destino não são mapeados e o grupo de consistência, LUNs, volumes e grupos de dados são removidos do cluster do ONTAP de destino.

A exclusão da relação aciona uma nova verificação no site secundário para remover o LUN não mapeado como caminho ativo dos hosts.

Passos

1. Faça login no cliente vSphere
2. Para editar as propriedades de um cluster protegido, é possível
 - a. Navegue até **Ferramentas do NetApp ONTAP > proteção > relacionamentos de cluster do host**, selecione o menu de elipse no cluster e selecione **Editar** ou
 - b. Clique com o botão direito do Mouse em um cluster de host e selecione **NetApp ONTAP Tools > Protect Cluster**.
3. Selecione o menu de elipse nas configurações do SnapMirror e selecione **Excluir**.

Uma tarefa do vCenter é criada e você pode acompanhar o progresso no painel **tarefa recente**.

Modificar uma relação SnapMirror existente

Para modificar uma relação assíncrona do SnapMirror, o SVM ou cluster do local secundário devem ser adicionados como back-end de storage nas ferramentas do ONTAP para VMware vSphere. Se for um relacionamento SnapMirror AutomatedFailOverDuplex, você pode modificar a proximidade do host em caso de configuração uniforme e o acesso do host em caso de configuração não uniforme. Não é possível trocar tipos de política assíncronos e AutomatedFailOverDuplex. Você pode definir a proximidade ou o acesso dos hosts recém-descobertos no cluster.



Não é possível editar uma relação de SnapMirror assíncrona existente.

Passos

1. Faça login no cliente vSphere
2. Para editar as propriedades de um cluster protegido, é possível
 - a. Navegue até **Ferramentas do NetApp ONTAP > proteção > relacionamentos de cluster do host**, selecione o menu de elipse no cluster e selecione **Editar** ou
 - b. Clique com o botão direito do Mouse em um cluster de host e selecione **NetApp ONTAP Tools > Protect Cluster**.
3. Se o tipo de política AutomatedFailOverDuplex estiver selecionado, adicione a proximidade do host ou os detalhes do acesso ao host.
4. Selecione o botão **Protect**.

Uma tarefa do vCenter é criada e você pode acompanhar o progresso no painel **tarefa recente**.

Remova a proteção do cluster do host

Quando você remove a proteção do cluster de host, os datastores ficam desprotegidos.

Passos

1. Para exibir os clusters de host protegidos, navegue até **Ferramentas do NetApp ONTAP > proteção > relacionamentos de cluster do host**.

Nesta página, você pode monitorar os clusters de host protegidos, juntamente com seu estado de proteção, a relação do SnapMirror e seu status de SnapMirror correspondente.
2. Na janela **Host cluster protection**, selecione o menu de elipse contra o cluster e, em seguida, selecione **Remove protection**.

Desative o AutoSupport

Ao configurar o sistema de armazenamento pela primeira vez, o AutoSupport é ativado por padrão. Ele envia mensagens para o suporte técnico 24 horas depois de ativado. Ao desativar o AutoSupport, você não receberá mais suporte e monitoramento proativos.



Recomenda-se que mantenha o AutoSupport ativado. Ele ajuda a acelerar a detecção e resolução de problemas. O sistema coleta informações do AutoSupport e as armazena localmente, mesmo quando desativado.

Passos

1. No vCenter Server, abra o console de manutenção.
2. Inicie sessão como utilizador de manutenção.
3. Introduza 1 para selecionar **Configuração da aplicação**.
4. Introduza 3 para selecionar **Desativar AutoSupport**.
5. Insira y na caixa de diálogo de confirmação.

Atualize o URL do proxy do AutoSupport

Atualize o URL do proxy AutoSupport para garantir o funcionamento adequado do recurso AutoSupport em cenários em que um servidor proxy é usado para controle de acesso à rede ou medidas de segurança. Ele permite que os dados do AutoSupport sejam roteados através do proxy apropriado, permitindo transmissão e conformidade seguras.

Passos

1. No vCenter Server, abra o console de manutenção.
2. Inicie sessão como utilizador de manutenção.
3. Introduza 1 para seleccionar **Configuração da aplicação**.
4. Digite 4 para seleccionar **Atualizar o URL do proxy AutoSupport**.
5. Insira o URL do proxy.

Crie backup e recupere a configuração

Como as ferramentas do ONTAP para o VMware vSphere 10,3 usam provisionador de storage dinâmico, você não pode alcançar RPO zero. No entanto, você pode alcançar RPO quase zero. Para alcançar quase zero-RPO, você precisa criar backup da instalação e restaurá-lo em uma nova máquina virtual.

Criar cópia de segurança e transferir o ficheiro de cópia de segurança

Passos

1. No vCenter Server, abra o console de manutenção.
2. Inicie sessão como utilizador de manutenção.
3. Digite 4 para seleccionar **suporte e Diagnóstico**.
4. Digite 3 para seleccionar **Ativar Backup do sistema** opção.
5. No caso de não-HA, insira as credenciais do vCenter onde a máquina virtual ONTAP Tools é implantada.
6. Introduza o valor da frequência de cópia de segurança entre 5-60 minutos.
7. Pressione **Enter**

Isso cria o backup e envia o backup para o armazenamento de dados da máquina virtual em um intervalo regular.

8. Para acessar o backup, navegue até a seção armazenamento e selecione o datastore da máquina virtual
9. Selecione a seção **Files**.

Na secção ficheiro, pode ver o diretório. O nome do diretório será o endereço IP das ferramentas ONTAP onde os pontos (.) são substituídos por sublinhados, sufixos com *backup*.

10. Para obter mais informações sobre a cópia de segurança, transfira o ficheiro backup_info.txt a partir de **Files > Download**.

Recuperar

Para recuperar a configuração, desligue a máquina virtual existente e implante uma nova máquina virtual usando o OVA que foi usado na implantação inicial.

Você precisa usar o mesmo endereço IP das ferramentas ONTAP (IP do balanceador de carga) para a nova máquina virtual e a configuração do sistema, como serviços habilitados, tamanho do nó e modo HA, deve ser igual à implantação inicial.

Execute as etapas a seguir para recuperar a configuração do arquivo de backup.

1. No vCenter Server, abra o console de manutenção.
2. Inicie sessão como utilizador de manutenção.
3. Digite 4 para selecionar **suporte e Diagnóstico**.
4. Digite 2 para selecionar a opção **Ativar acesso de diagnóstico remoto** e criar uma nova senha para o acesso de diagnóstico.
5. Selecione qualquer cópia de segurança a partir do diretório transferido. O nome do arquivo de backup mais recente é gravado no arquivo *backup_info.txt*.
6. Execute o comando abaixo para copiar o backup para a nova máquina virtual e digite a senha de diagnóstico quando solicitado.

```
scp <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.

7. Depois que o arquivo de backup é copiado, faça login no shell de diagnóstico e execute o seguinte comando:

```
sudo perl /home/maint/scripts/post-deploy-upgrade.pl -recovery
```

Os registos são gravados no ficheiro */var/log/post-deploy-upgrade.log*.

8. Após a recuperação bem-sucedida, os serviços e os objetos do vCenter são restaurados.

Desinstale as ferramentas do ONTAP para o VMware vSphere

A desinstalação das ferramentas do ONTAP para VMware vSphere exclui todos os dados das ferramentas.

Passos

1. Remova ou mova todas as máquinas virtuais das ferramentas do ONTAP para armazenamentos de dados gerenciados do VMware vSphere.
 - Para remover as máquinas virtuais, consulte ["Remover e Registrar novamente VMs e modelos de VM"](#)

- Para movê-los para um datastore não gerenciado, consulte ["Storage vMotion"](#)
- 2. ["Excluir datastores"](#) Criado nas ferramentas do ONTAP para VMware vSphere.
- 3. Se você ativou o provedor VASA, selecione **Configurações > Configurações do provedor VASA > DesRegistrar** nas ferramentas do ONTAP para cancelar o Registro dos provedores VASA de todos os servidores vCenter.
- 4. Desassocie todos os backends de armazenamento da instância do vCenter Server. ["Dissociar os backends de armazenamento com a instância do vCenter Server"](#) Consulte a .
- 5. Excluir todos os backends de armazenamento. ["Gerenciar backends de armazenamento"](#) Consulte a .
- 6. Remova o adaptador SRA do VMware Live Site Recovery:
 - a. Faça login como administrador na interface de gerenciamento do VMware Live Site Recovery Appliance usando a porta 5480.
 - b. Selecione **adaptadores de replicação de armazenamento**.
 - c. Selecione o cartão SRA apropriado e, no menu suspenso, selecione **Excluir**.
 - d. Confirme se você sabe os resultados da exclusão do adaptador e selecione **Excluir**.
- 7. Exclua as instâncias do vCenter Server integradas às ferramentas do ONTAP para VMware vSphere. ["Gerenciar instâncias do vCenter Server"](#) Consulte a .
- 8. Desligue as ferramentas do ONTAP para VMs VMware vSphere do vCenter Server e exclua as VMs.

O que vem a seguir?

["Remover volumes FlexVol"](#)

Remover volumes FlexVol

Quando você usa um cluster ONTAP dedicado para ferramentas do ONTAP para implantação do VMware, ele cria muitos volumes FlexVol não utilizados. Depois de remover as ferramentas do ONTAP para VMware vSphere, você deve remover os volumes do FlexVol para evitar possíveis impactos no desempenho.

Passos

1. Determine as ferramentas ONTAP para o tipo de implantação do VMware vSphere a partir da primeira VM do nó.

```
cat /opt/NetApp/meta/ansible_vars.yaml | grep -i protocol
```

Se for uma implantação iSCSI, você precisa excluir os grupos também.

2. Obtenha a lista de volumes do FlexVol.

```
kubectl describe persistentvolumes | grep internalName | awk -F' ' '{print $2}'
```

3. Remova as VMs do vCenter Server. Consulte a ["Remover e Registrar novamente VMs e modelos de VM"](#).
4. Excluir volumes FlexVol do Gerenciador de sistema do ONTAP. Consulte a ["Eliminar um FlexVol volume"](#). No comando CLI para excluir um volume, forneça o nome exato dos volumes FlexVol.
5. Excluir grupos SAN do sistema de armazenamento ONTAP em caso de implantação iSCSI. Consulte a ["Visualizar e gerenciar iniciadores e grupos SAN"](#).

Atualize as ferramentas do ONTAP para o VMware vSphere

Atualize as ferramentas do ONTAP para o VMware vSphere 10.x para o 10,3

A atualização é compatível com implantações de HA e não HA. Os caminhos de atualização suportados são:

Das ferramentas do ONTAP para a configuração do VMware vSphere 10,1 e 10,2	Para as ferramentas do ONTAP para a configuração do VMware vSphere 10,3
Não-HA pequeno	Não-HA e pequeno avançado
Meio não-HA	Não-HA e meio avançado
Avançado pequeno	Não-HA e pequeno avançado
Meio avançado	Não-HA e meio avançado
HA pequena	HA pequena
HA médio	HA médio
HA grande	HA grande



Atualizações das ferramentas do ONTAP para VMware vSphere 10,1 e 10,2 para 10,3 são suportadas. Atualizações diretas das ferramentas ONTAP 10,0 para 10,3 não são suportadas.

Antes de começar

Para uma atualização sem HA, desligue a VM do ONTAP Tools e, para uma atualização de HA, desligue o primeiro nó antes de fazer as seguintes alterações nas configurações da máquina virtual (VM).

- Adicione um disco rígido adicional de 100 GB a cada nó, pois os dados do serviço são armazenados localmente na VM.
- Altere a CPU e a memória da VM desligada de acordo com o sabor da sua implementação. Ative o hot plugin para CPU e RAM.

Tipo de implantação do 10,3	CPU (núcleo) por nó	Memória (GB) por nó	Espaço em disco (GB) por nó	CPU total (núcleo)	Memória (GB)	Espaço total em disco (GB)
Não-HA pequeno	9	18	350	9	18	350
Meio não-HA	13	26	350	13	26	350
HA pequena	9	18	350	27	54	1050
HA média	13	26	350	39	78	1050
HA grande	17	34	350	51	102	1050

- LIGUE a VM depois que as alterações forem feitas e aguarde que os serviços cheguem ao estado em execução.
- Em caso de implantação de HA, faça as alterações de recursos, ative o hot plugin para CPU e RAM e adicione discos rígidos de 100 GB para o segundo e terceiro nó também. Não há necessidade de reinicializar esses nós.
- Se o dispositivo foi implantado como um caminho local (implantação fácil) com as ferramentas 10,1 ou 10,2 do ONTAP, você precisa fazer um snapshot do quiesce antes de atualizar.

Se você estiver atualizando das ferramentas do ONTAP para VMware vSphere 10,0 para 10,1, precisará concluir as etapas a seguir antes de prosseguir com a tarefa de atualização:

Ativar diagnóstico

1. No vCenter Server, abra um console para as ferramentas do ONTAP.
2. Inicie sessão como utilizador de manutenção.
3. Digite **4** para selecionar **suporte e Diagnóstico**.
4. Introduza **2** para selecionar **Ativar acesso de diagnóstico remoto**.
5. Digite **y** para definir a senha de sua escolha.
6. Inicie sessão no endereço IP da VM a partir do terminal/massa com o utilizador como 'diag' e a palavra-passe definida na etapa anterior.

Faça um backup do MongoDB

Execute os seguintes comandos para fazer um backup do MongoDB:

- `kn exec -it ntv-mongodb-0 sh` - `kn` é um alias do `kubectl -n ntv-system`.
- Execute o comando `env | grep MONGODB_root_PASSWORD` dentro do pod.
- Execute o comando `exit` para sair do pod.
- Execute `kn exec ntv-mongodb-0 --mongodump -u root -p MONGODB_ROOT_PASSWORD --archive tmp/mongodb-backup.gz --gzip` comando para substituir o conjunto `MONGO_ROOT_PASSWORD` do comando acima.
- Execute o comando `kn cp ntv-mongodb-0:/tmp/mongodb-backup.gz ./mongodb-backup.gz` para copiar o backup do mongodb criado usando o comando acima do pod para o host.

Pegue o instantâneo quaise de todos os volumes

- Execute o comando '`kn get pvc`' e salve a saída do comando.
- Tire snapshots de todos os volumes um a um usando um dos seguintes métodos:
 - Na CLI, execute o comando `volume snapshot create -vserver <vserver_name> -volume <volume_name> -snapshot <snapshot_name>`
 - Na interface de usuário do Gerenciador de sistema do ONTAP, pesquise o volume pelo nome na barra de pesquisa e abra esse volume selecionando no nome. Vá para snapshot e adicione o snapshot desse volume.

Faça o snapshot das ferramentas do ONTAP para VMs VMware vSphere no vCenter (3VMs no caso de implantação HA, 1 VMs no caso de implantação não HA)

- Na interface de usuário do cliente vSphere, selecione a VM.

- Vá para a guia instantâneos e selecione o botão **tirar instantâneo**. Faça um snapshot bloqueado da VM. ["Tire um instantâneo de uma máquina virtual"](#) Consulte para obter detalhes.

Antes de executar a atualização, exclua os pods concluídos do pacote de log com o prefixo "gerar suporte-pacote-job". Se a geração de pacotes de suporte estiver em andamento, aguarde que ela seja concluída e exclua o pod.

Para qualquer tipo de atualização, você precisa adicionar uma unidade de disco rígido (HDD) adicional de 100 GB. Para adicionar um disco rígido, execute a seguinte tarefa.

1. Selecione a VM na configuração de nó único ou todas as três VMs na configuração de HA.
2. Clique com o botão direito do rato na(s) VM(s) e selecione **Adicionar novo dispositivo > disco rígido**
3. Adicione um HDD de 100 GB no campo **novo disco rígido**.
4. Selecione **aplicar**

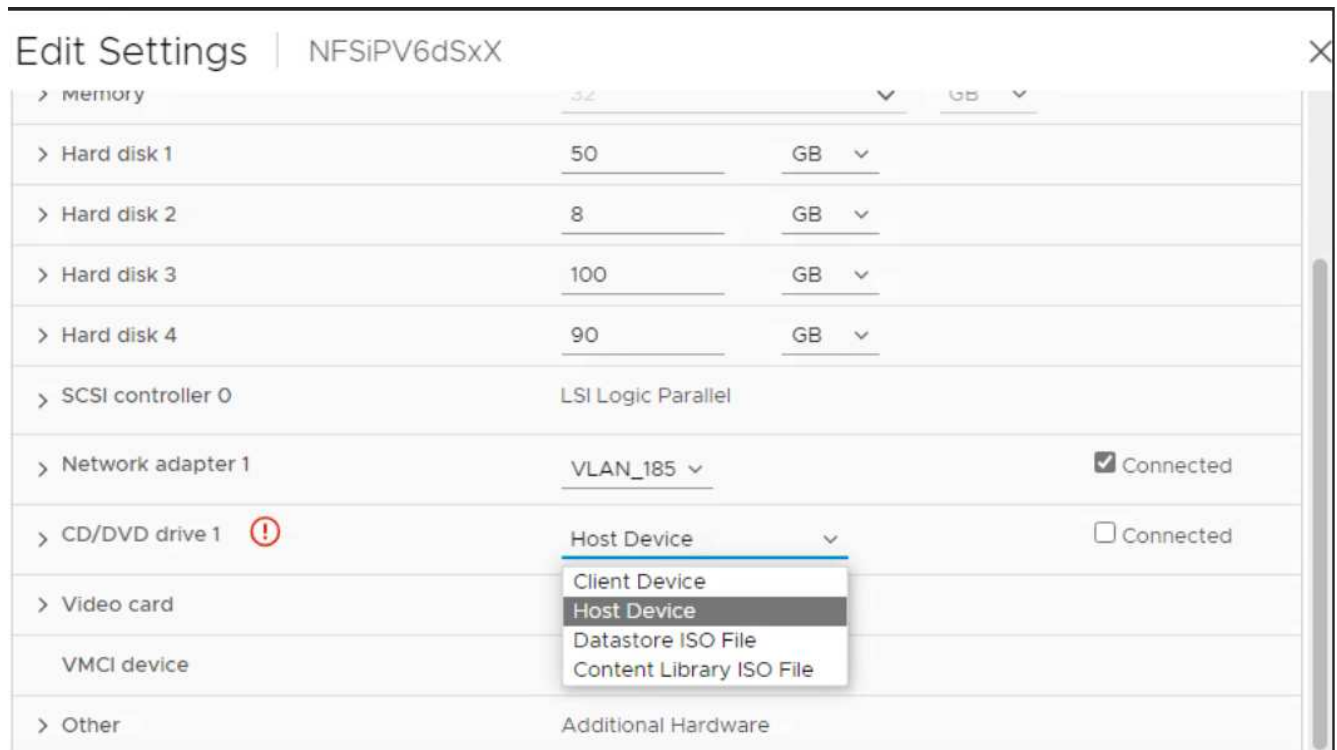
Depois de adicionar o disco rígido, atualize os recursos da VM para as respectivas configurações e reinicie a VM principal.

Será criado um novo HDD. O provisionador de storage dinâmico usa esse HDD para gerar ou replicar volumes.

Passos

1. Faça o upload das ferramentas do ONTAP para a ISO de atualização do VMware vSphere para a biblioteca de conteúdo.
2. Na página principal da VM, selecione **Ações > Editar configurações**. Para identificar o nome da máquina virtual principal:
 - 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 configurações de edição no campo **unidade de CD/DVD**.
4. Selecione o ficheiro ISO e selecione **OK**. Selecione a caixa de verificação Connected (ligado) no campo **CD/DVD drive** (unidade de CD/DVD).



5. No vCenter Server, abra um console para as ferramentas do ONTAP.
6. Inicie sessão como utilizador de manutenção.
7. Introduza **3** para seleccionar o menu Configuração do sistema.
8. Introduza **7** para seleccionar a opção de actualização.
9. Ao actualizar, as seguintes ações são executadas automaticamente:
 - a. Actualização do certificado
 - b. Actualização remota do plug-in

Depois de actualizar para as ferramentas do ONTAP para o VMware vSphere 10,3, você pode:

- Desative os serviços da interface de usuário do gerenciador
- Passar de uma configuração que não seja HA para uma configuração HA
- Faça escalabilidade vertical de uma configuração pequena que não seja HA, um meio que não seja HA, ou uma configuração média ou grande de HA.
- No caso de uma actualização que não seja de HA, reinicie a VM das ferramentas do ONTAP para refletir as alterações. No caso de uma actualização de HA, reinicie o primeiro nó para refletir as alterações no nó.

Depois de terminar

Depois de actualizar de versões anteriores das ferramentas do ONTAP para o VMware vSphere para o 10,3, volte a digitalizar os adaptadores SRA para verificar se os detalhes estão actualizados na página adaptadores de replicação de armazenamento de recuperação de site do VMware Live.

Depois de actualizar com êxito, exclua os volumes Trident do ONTAP manualmente usando o seguinte procedimento:



Essas etapas não são necessárias se as ferramentas do ONTAP para VMware vSphere 10,1 ou 10,2 estiverem em configurações não-HA de caminho local (caminho local) pequeno ou médio (caminho local).

1. No vCenter Server, abra um console para as ferramentas do ONTAP.
2. Inicie sessão como utilizador de manutenção.
3. Digite **4** para seleccionar o menu **suporte e Diagnóstico**.
4. Digite **1** para seleccionar a opção **Access Diagnostics shell**.
5. Execute o seguinte comando

```
sudo python3 /home/maint/scripts/ontap_cleanup.py
```

6. Introduza o nome de utilizador e a palavra-passe do ONTAP

Isso exclui todos os volumes do Trident no ONTAP usados nas ferramentas do ONTAP para VMware vSphere 10,1/10,2.

Informações relacionadas

["Migrar das ferramentas do ONTAP para o VMware vSphere 9.x para o 10,3"](#)

Atualizar códigos de erro

Você pode encontrar códigos de erro durante as ferramentas do ONTAP para a operação de atualização do VMware vSphere. Os códigos de erro têm cinco dígitos, onde os dois primeiros dígitos representam o script que encontrou o problema, e os últimos três dígitos representam o fluxo de trabalho específico dentro desse script.

Todos os logs de erros são registrados no arquivo `ansible-perl-errors.log` para facilitar o rastreamento e a resolução de problemas. Esse arquivo de log contém o código de erro e a tarefa Ansible com falha.



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 nenhuma 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 de implantação
01	firstboot-network-config.pl, atualização do modo
02	firstboot-inputs-validation.pl
03	firstboot-deploy-otv-ng.pl, implantar, HA
04	firstboot-deploy-otv-ng.pl, implantar, não HA
05	firstboot-deploy-otv-ng.pl, reinicie
06	firstboot-deploy-otv-ng.pl, upgrade, HA

07	firstboot-deploy-otv-ng.pl, upgrade, não HA
08	firstboot-otv-recovery.pl
09	post-deploy-upgrade.pl

Os últimos três dígitos do código de erro indicam o erro de fluxo de trabalho específico dentro do script:

Código de erro de atualização	Fluxo de trabalho	Resolução
068	A reversão de pacotes Debian falhou	Use a recuperação baseada em snapshot ou zero RPO e tente fazer a atualização novamente.
069	Falha ao restaurar ficheiros	Use a recuperação baseada em snapshot ou zero RPO e tente fazer a atualização novamente.
070	Falha ao eliminar cópia de segurança	-
071	O cluster do Kubernetes não estava íntegro	-
074	A montagem ISO falhou	Verifique o /var/log/upgrade-run.log e tente atualizar novamente.
075	As pré-verificações de atualização falharam	Tente novamente a atualização.
076	A atualização do registo falhou	Use a recuperação baseada em snapshot ou zero RPO e tente fazer a atualização novamente.
077	A reversão do Registro falhou	Use a recuperação baseada em snapshot ou zero RPO e tente fazer a atualização novamente.
078	A atualização do operador falhou	Use a recuperação baseada em snapshot ou zero RPO e tente fazer a atualização novamente.
079	A reversão do operador falhou	Use a recuperação baseada em snapshot ou zero RPO e tente fazer a atualização novamente.
080	A atualização dos serviços falhou	Use a recuperação baseada em snapshot ou zero RPO e tente fazer a atualização novamente.
081	Falha na reversão de serviços	Use a recuperação baseada em snapshot ou zero RPO e tente fazer a atualização novamente.
082	Falha ao eliminar imagens antigas do contentor	Use a recuperação baseada em snapshot ou zero RPO e tente fazer a atualização novamente.

083	A eliminação da cópia de segurança falhou	Use a recuperação baseada em snapshot ou zero RPO e tente fazer a atualização novamente.
084	Falha ao alterar o JobManager de volta à produção	Siga os passos abaixo para recuperar/concluir a atualização. 1. Ative o Shell de Diagnóstico 2. Execute o comando: <i>Sudo perl /home/manut/scripts/post-deploy-upgrade.pl --postupgrade</i> 3. Verifique os logs em /var/log/post-deploy-upgrade.log
087	As etapas de pós-atualização falharam.	Execute as seguintes etapas para recuperar/concluir a atualização. 1. Ative o Shell de Diagnóstico 2. Execute <i>sudo perl /home/manut/scripts/post-deploy-upgrade.pl --postupgrade</i> comando 3. Verifique os logs em /var/log/post-deploy-upgrade.log
088	A configuração da rotação de log para journald falhou	Verifique as configurações de rede da VM compatíveis com o host no qual a VM está hospedada. Você pode tentar migrar a VM para outro host e reiniciar.
089	A alteração da propriedade do registo de resumo, o ficheiro de configuração de rotação falhou	Tente novamente a atualização.
093	A atualização do provisionador de storage dinâmico falhou	Tente novamente a atualização.
094	A reversão do provisionador de storage dinâmico falhou	Tente novamente a atualização.
095	Falha na atualização DO SO	Sem recuperação para atualização do SO. Os serviços de ferramentas do ONTAP são atualizados e novos pods serão executados.
096	Instalar provisionador de storage dinâmico	Verifique os logs de atualização e tente atualizar novamente.
097	A desinstalação de serviços para atualização falhou	Use recuperação baseada em snapshots ou RPO zero e tente fazer a atualização novamente.
098	a cópia do segredo do provisionador de armazenamento dinâmico do sistema ntv para o namespace do provisionador de armazenamento dinâmico falhou	Verifique os logs de atualização e tente atualizar novamente.

099	Falha ao validar a nova adição de HDD	Adicione o novo HDD a todos os nós no caso de HA e a um nó em caso de implantação não HA.
108	Falha no script de sementeira	-
109	o backup de dados de volume persistentes falhou	Verifique os logs de atualização e tente atualizar novamente.
110	a restauração de dados de volume persistentes falhou	Use a recuperação baseada em snapshot ou zero RPO e tente fazer a atualização novamente.
111	A atualização dos parâmetros de tempo limite do etcd para RKE2 falhou	Verifique os logs de atualização e tente atualizar novamente.
112	A desinstalação do provisionador de armazenamento dinâmico falhou	-
113	A atualização de recursos em nós secundários falhou	Verifique os logs de atualização e tente atualizar novamente.



As ferramentas do ONTAP para VMware vSphere 10,3 são compatíveis com RPO zero.

Saiba mais sobre ["Como restaurar as ferramentas do ONTAP para VMware vSphere se a atualização falhar da versão 10,0 para a 10,1"](#)

Migrar as ferramentas do ONTAP para o VMware vSphere 9.xx para o 10,3

Migrar das ferramentas do ONTAP para o VMware vSphere 9.xx para o 10,3

Mover as ferramentas NetApp ONTAP para a configuração do VMware vSphere da versão 9.xx para a 10.x exige um processo de migração devido às atualizações e melhorias significativas do produto entre as versões.

Você pode migrar das ferramentas do ONTAP para as versões do VMware vSphere 9.12D1 e 9.13D2 para o 10,3.

Se você tiver datastores NFS e VMFS e nenhum datastores vVols em sua configuração, basta desinstalar o ONTAP Tools 9.xx e implantar o ONTAP Tools 10.x. No entanto, se sua configuração contiver datastores vVols, você terá que passar por 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 armazenamentos de dados vVols	Se a configuração contiver apenas armazenamentos de dados NFS e VMFS
Etapas: 1. "Migrar o provedor VASA" 2. "Criar políticas de armazenamento de VM"	Etapas: 1. Remova as ferramentas ONTAP 9.xx do seu ambiente. Consulte "Como remover o OTV 9.xx do seu ambiente" Artigo da Base de conhecimento da NetApp. 2. "Implantar e configurar ferramentas ONTAP para VMware vSphere 10.3" 3. "Atualize o SRA" 4. "Criar políticas de armazenamento de VM"



Depois de migrar das ferramentas do ONTAP para o VMware vSphere 9.xx para o 10,3, os armazenamentos de dados vVols que usam o protocolo NVMe/FC tornam-se não operacionais porque o ONTAP Tools 10,3 oferece suporte ao protocolo NVMe-of somente com datastores VMFS.

Migrar o Provedor VASA e atualizar o SRA

Etapas para migrar o provedor VASA

1. Para ativar A PORTA Derby 1527 nas ferramentas existentes do ONTAP para VMware vSphere, ative o usuário raiz e faça login na CLI por meio de SSH. Em seguida, execute o seguinte comando:

```
iptables -I INPUT 1 -p tcp --dport 1527 -j ACCEPT
```

2. Implantar as ferramentas OVA para ONTAP para VMware vSphere 10,3.
3. Adicione a instância do vCenter Server que você deseja migrar para as ferramentas do ONTAP para a versão do VMware vSphere 10,3. ["Adicione uma instância do vCenter Server"](#) Consulte para obter mais informações.

- Integre o backend de armazenamento localmente a partir das APIs do servidor vCenter para o plug-in de ferramentas ONTAP.
- Emita a seguinte API do Swagger ou no Postman para migrar.

Curl -X POST <https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/{vcguid}/migration-jobs>

Você pode acessar o Swagger através deste URL: 'https://\$FQDN_IP_PORT/, por exemplo <https://10.67.25.33:8443/>.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
POST	/api/v1

Tipo de processamento

Assíncrono

Curl exemplo

```
curl -X POST 'https://<OTV-NG-IP>:8443/virtualization/api/v1/vcenters/<vcguid>/migration-jobs' \
--header 'x-auth: <token_de_autenticação>' --header 'Tipo de conteúdo: aplicativo/json' --data '{
"otv_ip": "xx.xx.xx.xx", "vasa_provider_credentials": { "nome de usuário": "xxxxx", "senha": "" },
"senha_do_banco_de_dados": "" }'
```

Corpo de solicitação para outra migração de liberação:

```
{ "otv_ip": "xx.xx.xx.xx", "vasa_provider_credentials": { "nome de usuário": "xxxxx", "senha": "" } }
```

◦ Exemplo de saída JSON*

Um objeto de tarefa é retornado. Você deve salvar o identificador do trabalho para usá-lo na próxima etapa.

```
[id]: 123, "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35", "status": "running"
```

- Use o seguinte URI no Swagger para verificar o status:

```
curl
https://xx.xx.xx.xxx:8443/virtualization/api/jobmanager/v2/jobs/<JobID>?
includeSubJobsAndTasks=true
```

Depois de concluir o trabalho, reveja o relatório de migração. Este relatório está incluído nos dados do trabalho e pode ser acessado a partir da resposta do trabalho.

- Adicione as ferramentas ONTAP para o provedor de armazenamento VMware vSphere ao vCenter Server e ["Registre o Fornecedor VASA"](#) com ferramentas ONTAP para VMware vSphere.

8. "Ative o fornecedor VASA" Serviço em ferramentas do ONTAP para VMware vSphere 10,3.
9. Pare as ferramentas do ONTAP para o provedor de armazenamento VMware vSphere 9,10/9,11/9,12/9,13 Serviço do provedor VASA a partir do console de manutenção.

Não elimine o fornecedor VASA.

Depois que o antigo provedor VASA é interrompido, o vCenter Server faz failover para as ferramentas do ONTAP para VMware vSphere. Todos os armazenamentos de dados e VMs ficam acessíveis e são servidos a partir das ferramentas do ONTAP para VMware vSphere.

10. Os armazenamentos de dados NFS e VMFS migrados das ferramentas do ONTAP para o VMware vSphere 9.xxx são visíveis nas ferramentas do ONTAP para o VMware vSphere 10,3 somente após a ativação do job de descoberta do datastore, o que pode levar até 30 minutos para ser concluído. Verifique se os armazenamentos de dados estão visíveis na página de visão geral das ferramentas ONTAP para a página de interface do usuário do plug-in VMware vSphere.
11. Execute a migração de patch usando a seguinte API no Swagger ou no Postman:

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
PATCH	/api/v1

Tipo de processamento

Assíncrono

Curl exemplo

Curl -X PATCH <https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/56d373bd-4163-44f9-a872-9adabb008ca9/migration-jobs/84dr73bd-9173-65r7-w345-8ufdbb887d43>

- Exemplo de saída JSON*

Um objeto de tarefa é retornado. Você deve salvar o identificador do trabalho para usá-lo na próxima etapa.

[id]: 123, "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35", "status": "running"

O corpo da solicitação está vazio para operação de patch.



UUID é a migração UUID retornada em resposta à API pós-migração.

Depois de executar a API de migração de patches, todas as VMs estão em conformidade com a política de storage.

O que vem a seguir

Após concluir a migração e o Registro das ferramentas do ONTAP 10,3 para o vCenter Server, siga estas etapas:

- Aguarde que **Discovery** seja concluído, os certificados serão atualizados automaticamente em todos os hosts.
- Permita tempo suficiente antes de iniciar operações de datastore e máquina virtual. O período de espera necessário varia de acordo com o número de hosts, datastores e máquinas virtuais dentro da configuração. A falha na espera pode resultar em falhas operacionais intermitentes.

Após a atualização, se o estado de conformidade da máquina virtual estiver desatualizado, reapply a política de armazenamento usando as seguintes etapas:

1. Navegue até o datastore e selecione **Summary > VM Storage Policies**.

O status de conformidade em **conformidade com a política de armazenamento de VM** é exibido como **desatualizado**.

2. Selecione a política Storage VM e a VM correspondente
3. Selecione **aplicar**

O status de conformidade em **conformidade com a política de armazenamento de VM** agora é mostrado como compatível.

Informações relacionadas

- ["Saiba mais sobre as ferramentas do ONTAP para VMware vSphere 10 RBAC"](#)
- ["Atualize das ferramentas do ONTAP para o VMware vSphere 10.x para o 10,3"](#)

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 em execução, enquanto o site de recuperação é onde as VMs serão recuperadas. A interface do SRM exibe o estado do plano de recuperação com detalhes sobre os sites protegidos e de recuperação. No plano de recuperação, os botões LIMPAR e REPROTEGER estão desabilitados, enquanto os botões TESTE e EXECUTAR permanecem habilitados. 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 reproteção estiver pendente. Certifique-se de que o processo de reproteção está concluído antes de prosseguir com a migração. Se um failover de teste estiver em andamento, limpe o failover de teste e inicie a migração.

1. Siga estas etapas para excluir o adaptador SRA das ferramentas do ONTAP para VMware vSphere 9.xx na recuperação de site da VMware:
 - a. Vá para a página de gerenciamento de configuração do VMware Live Site Recovery
 - b. Vá para a seção **Storage Replication Adapter**.
 - c. No menu de elipses, selecione **Reset Configuration**.
 - d. No menu de elipses, selecione **Delete**.
2. Execute estas etapas nos locais de proteção e recuperação.
 - a. Instale as ferramentas do ONTAP para o adaptador VMware vSphere 10,3 SRA usando as etapas em ["Configure o SRA no VMware Live Site Recovery Appliance"](#).

- b. Na página de interface de usuário do VMware Live Site Recovery, execute as operações **Discover Arrays** e **Discover Devices** e confirme se os dispositivos são exibidos como antes da migração.

Automatize usando a API REST

Saiba mais sobre as ferramentas do ONTAP para a API REST do VMware vSphere 10

As ferramentas do ONTAP para VMware vSphere 10 são um conjunto de ferramentas para o gerenciamento do ciclo de vida da máquina virtual. Ele inclui uma API REST robusta que você pode usar como parte de seus processos de automação.

Base de serviços web REST

Representational State Transfer (REST) é um estilo para criar aplicativos da Web distribuídos, incluindo o design de APIs de serviços da Web. Ele estabelece um conjunto de tecnologias para expor recursos baseados em servidor e gerenciar seus estados.

Recursos e representação do Estado

Os recursos são os componentes fundamentais de um aplicativo de serviços da Web REST. Há duas tarefas iniciais importantes ao projetar uma API REST:

- Identificar os recursos baseados no sistema ou no servidor
- Definir os estados de recurso e as operações de transição de estado associadas

Os aplicativos clientes podem exibir e alterar os estados do recurso por meio de fluxos de mensagens bem definidos.

Mensagens HTTP

O Hypertext Transfer Protocol (HTTP) é o protocolo usado pelo cliente e servidor de serviços da Web para trocar mensagens sobre os recursos. Ele segue o modelo CRUD com base nas operações genéricas criar, ler, atualizar e excluir. O protocolo HTTP inclui cabeçalhos de solicitação e resposta, bem como códigos de status de resposta.

Formatação de dados JSON

Embora existam vários formatos de mensagem disponíveis, a opção mais popular é JavaScript Object Notation (JSON). JSON é um padrão da indústria para representar estruturas de dados simples em texto simples e é usado para transferir informações de estado descrevendo os recursos e ações desejadas.

Segurança

A segurança é um aspecto importante de uma API REST. Além do protocolo TLS (Transport Layer Security) usado para proteger o tráfego HTTP pela rede, as ferramentas do ONTAP para a API REST do VMware vSphere 10 também usam tokens de acesso para autenticação. Você precisa adquirir um token de acesso e usá-lo em chamadas de API subsequentes.

Suporte para solicitações assíncronas

As ferramentas do ONTAP para a API REST do VMware vSphere 10 executam a maioria das solicitações de forma síncrona, retornando um código de status quando a operação for concluída. Ele também suporta processamento assíncrono para tarefas que exigem mais tempo para serem concluídas.

Ambiente do Gerenciador de ferramentas do ONTAP

Há vários aspectos do ambiente do Gerenciador de ferramentas do ONTAP que você deve considerar.

Máquina virtual

As ferramentas do ONTAP para VMware vSphere 10 são implantadas usando a arquitetura de plug-in remoto vSphere. O software, incluindo suporte para a API REST, é executado em uma máquina virtual separada.

Endereço IP das ferramentas ONTAP

As ferramentas do ONTAP para VMware vSphere 10 expõem um único endereço IP que fornece um gateway para os recursos da máquina virtual. Você precisa fornecer o endereço durante a configuração inicial e ele é atribuído a um componente do balanceador de carga interno. O endereço é usado pela interface de usuário do Gerenciador de ferramentas do ONTAP, bem como para acessar diretamente a página de documentação do Swagger e a API REST.

Duas APIs REST

Além das ferramentas do ONTAP para a API REST do VMware vSphere 10, o cluster do ONTAP tem sua própria API REST. O Gerenciador de ferramentas do ONTAP usa a API REST do ONTAP como cliente para executar tarefas relacionadas ao storage. É importante ter em mente que essas duas APIs são separadas e distintas. Para obter mais informações, ["Automação da ONTAP"](#) consulte .

Detalhes de implementação das ferramentas do ONTAP para a API REST do VMware vSphere 10

Embora O REST estabeleça um conjunto comum de tecnologias e práticas recomendadas, a implementação exata de cada API pode variar com base nas escolhas de design. Você deve estar familiarizado com a forma como as ferramentas do ONTAP para a API REST do VMware vSphere 10 são projetadas antes de usá-las.

A API REST inclui várias categorias de recursos, como vCenters e agregados. Consulte a ["Referência da API"](#) para obter mais informações.

Como acessar a API REST

Você pode acessar as ferramentas do ONTAP para a API REST do VMware vSphere 10 por meio do endereço IP do balanceador de carga das ferramentas do ONTAP junto com a porta. Existem várias partes para o URL completo, incluindo:

- Porta e endereço IP das ferramentas ONTAP
- Versão da API
- Categoria do recurso
- Recurso específico

Você precisa configurar o endereço IP durante a configuração inicial e a porta é sempre 8443. Além disso, para uma instância específica do ONTAP Tools for VMware vSphere 10, a primeira parte do URL é constante. Apenas a categoria de recurso e o recurso específico variam 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 para acessar serviços de autenticação

```
https://10.61.25.34:8443/virtualization/api/v1/auth/login
```


Esse URL pode ser usado 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`

Esse URL pode ser usado para solicitar uma lista das instâncias definidas do vCenter Server usando o método GET.

Detalhes HTTP

As ferramentas do ONTAP para a API REST do VMware vSphere 10 usam HTTP e parâmetros relacionados para agir nas instâncias e coleções de recursos. Detalhes da implementação HTTP são apresentados abaixo.

Métodos HTTP

Os métodos HTTP ou verbos suportados pela API REST são apresentados na tabela abaixo.

Método	CRUD	Descrição
OBTER	Leia	Recupera propriedades de objeto para uma instância ou coleção de recursos. Isso é considerado uma operação de lista quando usado com uma coleção.
POST	Criar	Cria uma nova instância de recurso com base nos parâmetros de entrada.
COLOQUE	Atualização	Atualiza uma instância de recurso inteira com o corpo de solicitação JSON fornecido. Os valores-chave que não são modificáveis pelo usuário são preservados.
PATCH	Atualização	Solicita que um conjunto de alterações selecionadas na solicitação seja aplicado à instância de recurso.
ELIMINAR	Eliminar	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.

Colhedor	Tipo	Notas de utilização
Aceitar	Pedido	Este é o tipo de conteúdo que o aplicativo cliente pode aceitar. Os valores válidos incluem "/" ou <code>application/json</code> .
x-auth	Pedido	Contém um token de acesso que identifica o usuário que emite a solicitação através do aplicativo cliente.
Tipo de conteúdo	Resposta	Devolvido 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.
201	Criado	Um objeto foi criado com sucesso com um identificador exclusivo para a instância de recurso.
202	Aceito	A solicitação foi aceita e um trabalho em segundo plano criado para executar a solicitação.
204	Nenhum conteúdo	A solicitação foi bem-sucedida, embora nenhum conteúdo tenha sido retornado.
400	Pedido incorreto	A entrada de solicitação não é reconhecida ou é inadequada.
401	Não autorizado	O usuário não está autorizado e deve autenticar.
403	Proibido	O acesso é negado devido a um erro de autorização.
404	Não encontrado	O recurso referido na solicitação não existe.
409	Conflito	Uma 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 para a API REST é realizada usando 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 Gerenciador de ferramentas do ONTAP (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.

"[Sua primeira chamada de API REST](#)" Consulte para obter um exemplo de solicitação e uso de um token de acesso.

Solicitações síncronas e assíncronas

A maioria das chamadas de API REST são concluídas rapidamente e, portanto, executadas de forma síncrona. Ou seja, eles retornam um código de status (como 200) depois que uma solicitação foi concluída. As solicitações que levam mais tempo para serem concluídas são executadas assincronamente usando um trabalho em segundo plano.

Depois de emitir uma chamada de API que é executada de forma assíncrona, o servidor retorna um código de status HTTP 202. Isto indica que a solicitação foi aceita mas ainda não foi concluída. Você pode consultar o trabalho em segundo plano para determinar seu status, incluindo sucesso ou falha.

O processamento assíncrono é usado para vários tipos de operações de longa duração, incluindo operações de datastore e evolução. Consulte a categoria do gerenciador de tarefas da API REST na página Swagger para obter mais informações.

Suas primeiras ferramentas do ONTAP para chamada de API REST do VMware vSphere 10

Você pode emitir uma chamada de API usando o curl para começar a usar as ferramentas do ONTAP para a API REST do VMware vSphere 10.

Antes de começar

Você deve rever as informações e os parâmetros necessários nos exemplos curl.

Informações necessárias

Você precisa do seguinte:

- Ferramentas do ONTAP para o endereço IP ou FQDN do VMware vSphere 10, bem como a porta
- Credenciais para o administrador do Gerenciador de ferramentas do ONTAP (nome de usuário e senha)

Parâmetros e variáveis

Os exemplos de curl apresentados abaixo incluem variáveis de estilo Bash. Você pode definir essas variáveis no ambiente Bash ou atualizá-las manualmente antes de emitir os comandos. Se você definir as variáveis, o shell substituirá os valores em cada comando antes de ser executado. As variáveis são descritas na tabela abaixo.

Variável	Descrição
FQDN_IP_PORT	O nome de domínio totalmente qualificado ou o endereço IP do Gerenciador de ferramentas do ONTAP juntamente com o número da porta.
O PREÇO É DE USD	Nome de usuário para a conta do Gerenciador de ferramentas do ONTAP.
MYPASSWORD	Senha associada ao nome de usuário do Gerenciador de ferramentas do ONTAP.
ACCESS_TOKEN	O token de acesso emitido pelo Gerenciador de ferramentas do ONTAP.

Os seguintes comandos e saída na CLI 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
```

Passo 1: Adquirir um token de acesso

Você precisa adquirir 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: Emita a chamada da API REST

Depois de ter um token de acesso, você pode usar o curl para emitir uma chamada de API REST. Inclua o token de acesso adquirido na primeira etapa.

Curl exemplo

```
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 para o Gerenciador de ferramentas do ONTAP.

Referência de API para as ferramentas do ONTAP para a API REST do VMware vSphere 10

As ferramentas do ONTAP para referência da API REST do VMware vSphere 10 contêm detalhes sobre todas as chamadas de API. Esta referência é útil ao desenvolver aplicações de automação.

Você pode acessar as ferramentas do ONTAP para a documentação da API REST do VMware vSphere 10 online por meio da interface de usuário do Swagger. Você precisa do endereço IP ou FQDN das ferramentas do ONTAP para o serviço de gateway VMware vSphere 10, bem como da porta.

Passos

1. Digite o seguinte URL no seu navegador substituindo o endereço IP apropriado e a combinação de porta para a 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 muito mais.

Direitos de autor

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marcas comerciais

NetApp, o logotipo DA NetApp e as marcas listadas na página de marcas comerciais da NetApp são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Patentes

Uma lista atual de patentes de propriedade da 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 aviso fornecem informações sobre direitos autorais de terceiros e licenças usadas no software NetApp.

["Aviso para as ferramentas do ONTAP para VMware vSphere 10,3"](#)

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES DOCUMENTOS, 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.