Documentação das ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
September 29, 2025

This PDF was generated from https://docs.netapp.com/pt-br/ontap-tools-vmware-vsphere-104/index.html on September 29, 2025. Always check docs.netapp.com for the latest.

Índice

Documentação das ONTAP tools for VMware vSphere . . . 1
Notas de lançamento . . . 2
- Notas de lançamento . . . 2
- Novidades nas ONTAP tools for VMware vSphere 10.4 . . . 2
- Comparação de recursos das ONTAP tools for VMware vSphere 9 e ONTAP tools for VMware vSphere 10 . . . 3

Conceitos . . . 5
- Visão geral das ONTAP tools for VMware vSphere . . . 5
- Principais conceitos e termos . . . 5
- Controle de acesso baseado em função . . . 8
  - Saiba mais sobre as ONTAP tools for VMware vSphere 10 RBAC . . . 8
  - RBAC com VMware vSphere . . . 9
  - RBAC com ONTAP . . . 13
- Alta disponibilidade para ONTAP tools for VMware vSphere . . . 16
- Interface de usuário do gerenciador de ferramentas ONTAP . . . 16

Implantar ONTAP tools for VMware vSphere . . . 19
- Início rápido para ONTAP tools for VMware vSphere . . . 19
- Fluxo de trabalho de implantação de alta disponibilidade (HA) . . . 21
- ONTAP tools for VMware vSphere . . . 21
  - Requisitos do sistema . . . 21
  - Requisitos mínimos de armazenamento e aplicação . . . 22
  - Requisitos portuários . . . 22
  - Limites de configuração para implantar ONTAP tools for VMware vSphere . . . 24
  - ONTAP tools for VMware vSphere - Adaptador de Replicação de Armazenamento (SRA) . . . 25
- Antes de começar… . . . 25
  - Planilha de implantação . . . 26
  - Configuração de firewall de rede . . . 27
  - Configurações de armazenamento ONTAP . . . 27
- Implantar ONTAP tools for VMware vSphere . . . 28
- Códigos de erro de implantação . . . 33

Configurar ONTAP tools for VMware vSphere . . . 36
- Adicionar instâncias do vCenter Server . . . 36
- Registre o provedor VASA com uma instância do vCenter Server . . . 36
- Instalar o plug-in NFS VAAI . . . 37
- Configurar as definições do host ESXi . . . 38
  - Configurar configurações de multicaminho e tempo limite do servidor ESXi . . . 38
  - Definir valores do host ESXi . . . 39
- Configurar funções e privilégios de usuário do ONTAP . . . 40
  - Requisitos de mapeamento agregado de SVM . . . 41
  - Crie o usuário e a função ONTAP manualmente . . . 41
  - Atualizar ONTAP tools for VMware vSphere 10.1 para 10.3 . . . 49
  - Atualizar ONTAP tools for VMware vSphere 10.3 para 10.4 . . . 51
- Adicionar um backend de armazenamento . . . 52

Associar um backend de armazenamento a uma instância do vCenter Server . . . 53
Configurar acesso à rede . . . 54
Criar um armazenamento de dados . . . 54
Proteja datastores e máquinas virtuais . . . 60
Proteger usando proteção de cluster de host . . . 60
Proteja usando proteção SRA . . . 61
Configurar SRA para proteger armazenamentos de dados . . . 61
Configurar SRA para ambientes SAN e NAS . . . 61
Configurar SRA para ambientes altamente escalonados . . . 63
Configurar SRA no dispositivo VMware Live Site Recovery . . . 63
Atualizar credenciais SRA . . . 64
Configurar sites protegidos e de recuperação . . . 65
Configurar recursos de site protegidos e de recuperação . . . 66
Verificar sistemas de armazenamento replicados . . . 70
Proteção contra dispersão . . . 71
Gerenciar ONTAP tools for VMware vSphere . . . 74
Visão geral do painel de ONTAP tools for VMware vSphere . . . 74
Interface de usuário do gerenciador de ferramentas ONTAP . . . 76
Entenda igroups e políticas de exportação em ONTAP tools for VMware vSphere . . . 77
Políticas de exportação . . . 81
Entenda os igroups gerenciados pelas ferramentas ONTAP . . . 82
Habilitar ONTAP tools for VMware vSphere . . . 85
Alterar ONTAP tools for VMware vSphere . . . 86
Gerenciar armazenamentos de dados . . . 87
Montar datastores NFS e VMFS . . . 87
Desmontar datastores NFS e VMFS . . . 88
Montar um armazenamento de dados vVols . . . 89
Redimensionar armazenamento de dados NFS e VMFS . . . 89
Expandir armazenamentos de dados vVols . . . 89
Reduzir armazenamento de dados vVols . . . 90
Excluir armazenamentos de dados . . . 90
Visualizações de armazenamento ONTAP para repositórios de dados . . . 91
Visualização de armazenamento da máquina virtual . . . 92
Gerenciar limites de armazenamento . . . 92
Gerenciar backends de armazenamento . . . 92
Descubra o armazenamento . . . 93
Modificar backends de armazenamento . . . 93
Remover backends de armazenamento . . . 93
Visão detalhada do backend de armazenamento . . . 94
Gerenciar instâncias do vCenter Server . . . 95
Desassociar backends de armazenamento com a instância do vCenter Server . . . 95
Modificar uma instância do vCenter Server . . . 95
Remover uma instância do vCenter Server . . . 95
Gerenciar certificados . . . 96
Acesse as ONTAP tools for VMware vSphere . . . 98

Visão geral das ONTAP tools for VMware vSphere . . . 98
Configurar acesso de diagnóstico remoto . . . 99
Inicie o SSH em outros nós . . . 100
Atualize as credenciais do vCenter Server e do ONTAP . . . 100
Relatórios de ferramentas ONTAP . . . 100
Coletar os arquivos de log . . . 101
Gerenciar máquinas virtuais . . . 101
Considerações para migrar ou clonar máquinas virtuais . . . 102
Migrar máquinas virtuais com datastores NFS e VMFS para datastores vVols . . . 103
Limpeza VASA . . . 103
Anexar ou desanexar um disco de dados de uma máquina virtual . . . 103
Descubra sistemas de armazenamento e hosts . . . 104
Modificar as configurações do host ESXi usando ferramentas ONTAP . . . 105
Gerenciar senhas . . . 106
Alterar senha do gerenciador de ferramentas ONTAP . . . 106
Redefinir a senha do gerenciador de ferramentas ONTAP . . . 106
Redefinir a senha do usuário do aplicativo . . . 107
Redefinir a senha do usuário do console de manutenção . . . 107
Gerenciar a proteção do cluster do host . . . 108
Modificar cluster de host protegido . . . 108
Remover proteção do cluster do host . . . 111
Desativar AutoSupport . . . 111
Atualizar URL do AutoSupport do AutoSupport . . . 112
Adicionar servidores NTP . . . 112
Crie um backup e recupere a configuração das ferramentas ONTAP . . . 112
Crie um backup e baixe o arquivo de backup . . . 113
Recuperar . . . 113
Desinstalar ONTAP tools for VMware vSphere . . . 114
Remover volumes FlexVol . . . 115
Atualizar ONTAP tools for VMware vSphere . . . 116
Atualização das ONTAP tools for VMware vSphere 10.x para 10.4 . . . 116
Códigos de erro de atualização . . . 119
Migrar ONTAP tools for VMware vSphere 9.xx para 10.4 . . . 123
Migrar das ONTAP tools for VMware vSphere 9.xx para 10.4 . . . 123
Migrar o Provedor VASA e atualizar o SRA . . . 123
Etapas para migrar o provedor VASA . . . 123
Etapas para atualizar o adaptador de replicação de armazenamento (SRA) . . . 126
Automatize usando a API REST . . . 127
Saiba mais sobre as ONTAP tools for VMware vSphere 10 REST API . . . 127
Fundação de serviços web REST . . . 127
Ambiente do gerenciador de ferramentas ONTAP . . . 127
Detalhes de implementação das ONTAP tools for VMware vSphere 10 REST API . . . 128
Como acessar a API REST . . . 128
Detalhes HTTP . . . 129
Autenticação . . . 130

Solicitações síncronas e assíncronas . . . 130
Suas primeiras ONTAP tools for VMware vSphere 10 . . . 130
Antes de começar . . . 131
Etapa 1: Adquira um token de acesso . . . 131
Etapa 2: emitir a chamada da API REST . . . 131
Referência de API para as ONTAP tools for VMware vSphere 10 REST API . . . 132
Avisos legais . . . 133
Direitos autorais . . . 133
Marcas Registradas . . . 133
Patentes . . . 133
Política de Privacidade . . . 133
Código aberto . . . 133

Documentação das ONTAP tools for VMware vSphere

Notas de lançamento

Notas de lançamento

Saiba mais sobre os novos e aprimorados recursos disponíveis nas ONTAP tools for VMware vSphere 10.4.

Para obter uma lista completa de novos recursos e melhorias, consulteNovidades nas ONTAP tools for VMware vSphere 10.4 .

Para saber mais sobre se a migração das ONTAP tools for VMware vSphere 9 para as ferramentas ONTAP 10.4 é adequada para sua implantação, consulteComparação de recursos das ONTAP tools for VMware vSphere 9 e ONTAP tools for VMware vSphere 10 . A migração é suportada das ONTAP tools for VMware vSphere versões 9.12-D e 9.13-D para as ONTAP tools for VMware vSphere 10.4.

Para mais informações, consulte o "Notas de versão das ONTAP tools for VMware vSphere 10.4" . Você deve entrar com sua conta NetApp ou criar uma conta para acessar as Notas de Versão.

Novidades nas ONTAP tools for VMware vSphere 10.4

Saiba mais sobre os novos recursos disponíveis nas ONTAP tools for VMware vSphere 10.4.

Atualizar	Descrição
"Suporte para sistema ASA r2 com 12 nós por cluster"	As ONTAP tools for VMware vSphere 10.4 oferecem suporte a fluxos de trabalho para sistemas de armazenamento ASA r2 com até 12 nós por cluster, melhorando a eficiência e a escalabilidade do gerenciamento de dados. Ele oferece suporte a datastores vVols com protocolos iSCSI e FC, e datastores VMFS com protocolos iSCSI, FC e NVMe, fornecendo opções de armazenamento flexíveis e aprimoradas.
"Melhorias na interface do usuário do gerenciador de ferramentas ONTAP"	Agora você pode habilitar o servidor NTP para sincronização de tempo precisa em todo o ambiente e configurar as definições de telemetria para monitorar e analisar o desempenho do sistema a partir da interface do Gerenciador de ferramentas ONTAP . Essas configurações não estão mais disponíveis no console de manutenção.
Recursos de segurança aprimorados	Os recursos de segurança agora oferecem proteção aprimorada e conformidade com os padrões do setor, proporcionando uma experiência robusta e fácil de usar para ajudar os administradores a gerenciar ambientes VMware de forma mais eficaz.
"Recursos aprimorados de recuperação de desastres SRA"	As ONTAP tools for VMware vSphere 10.4 agora oferecem suporte a operações de recuperação de desastres usando Site Recovery Appliance (SRA) com snapshots com nomes personalizados, além de cópias de snapshots agendadas do SnapMirror .

Comparação de recursos das ONTAP tools for VMware vSphere 9 e ONTAP tools for VMware vSphere 10

Saiba se a migração das ONTAP tools for VMware vSphere 9 para as ONTAP tools for VMware vSphere 10.1 ou versões posteriores é ideal para você.

Para obter as informações de compatibilidade mais atualizadas, consulte "Ferramenta de Matriz de Interoperabilidade da NetApp" .

Recurso	Ferramentas ONTAP 9.13	Ferramentas ONTAP 10.1	Ferramentas ONTAP 10.2 em diante
Proposta de valor chave	Simplifique e otimize as operações do dia 0 ao dia 2 com recursos aprimorados de segurança, conformidade e automação	Evolução das ferramentas ONTAP 10.x em direção à paridade 9.xx, ao mesmo tempo em que estende os limites de alta disponibilidade, desempenho e escala	Suporte expandido para incluir FC para VMFS e vVols, e NVMe-oF/FC, NVMe-oF/TCP somente para VMFS. Facilidade de uso para NetApp SnapMirror, configuração simples para clusters de armazenamento metro vSphere e suporte VMware Live Site Recovery de três sites
Qualificação de liberação ONTAP	ONTAP 9.9.1 para ONTAP 9.16.1	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, 9.16.0 e 9.16.1 para ferramentas ONTAP 10.3. ONTAP 9.14.1, 9.15.1, 9.16.0 e 9.16.1 para ferramentas ONTAP 10.4. ONTAP 9.16.1P3 e posterior é necessário para as ferramentas ONTAP 10.4 ao usar sistemas ASA r2.
Suporte à versão 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
Suporte de protocolo	Armazenamentos de dados NFS e VMFS: NFS (v3 e v4.1), VMFS (iSCSI e FCP) Armazenamentos de dados vVols : iSCSI, FCP, NVMe/FC, NFS v3	Armazenamentos de dados NFS e VMFS: NFS (v3 e v4.1), VMFS (iSCSI) Armazenamentos de dados vVols : iSCSI, NFS v3	Armazenamentos de dados NFS e VMFS: NFS (v3 e v4.1), VMFS (iSCSI/FCP/NVMe-oF) Armazenamentos de dados vVols : iSCSI, FCP, NFS v3
Escalabilidade	Hosts e VMs: 300 hosts, até 10 mil VMs Datastores: 600 NFS, até 50 VMFS, até 250 vVols vVols: até 14.000	Hosts e VMs: 600 Hosts vVols: Até 140.000	Hosts e VMs: 600 Hosts vVols: Até 140.000

Recurso	Ferramentas ONTAP 9.13	Ferramentas ONTAP 10.1	Ferramentas ONTAP 10.2 em diante
Observabilidade	Painéis de desempenho, capacidade e conformidade do host Relatórios dinâmicos de VM e armazenamento de dados	Painéis atualizados de desempenho, capacidade e conformidade do host Relatórios dinâmicos de VM e armazenamento de dados	Painéis atualizados de desempenho, capacidade e conformidade do host Relatórios dinâmicos de VM e armazenamento de dados
Proteção de dados	Replicação SRA para VMFS e NFS Replicação baseada em FlexVols para vVols Integração SCV e interoperável para backup	Replicação SRA para armazenamentos de dados iSCSI VMFS e NFS v3	Replicação SRA para proteção de três sites de datastores iSCSI VMFS e NFS v3 combinando SMAS e VMware Live Site Recovery.
Suporte do provedor VASA	VASA 4.0	VASA 3.0	VASA 3.0

Conceitos

Visão geral das ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere são um conjunto de ferramentas para gerenciamento do ciclo de vida de máquinas virtuais. Ele se integra ao ecossistema VMware para ajudar no provisionamento do armazenamento de dados e fornecer proteção básica para máquinas virtuais. As ONTAP tools for VMware vSphere são uma coleção de microsserviços escaláveis horizontalmente e orientados a eventos, implantados como um Open Virtual Appliance (OVA). Esta versão integra a API REST com o ONTAP.

As ONTAP tools for VMware vSphere consistem no seguinte:

- Funcionalidade da máquina virtual, como proteção básica e recuperação de desastres
- Provedor VASA para gerenciamento granular de VM
- Gerenciamento baseado em políticas de armazenamento
- Adaptador de Replicação de Armazenamento (SRA)

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 oferecem uma solução unificada de hardware e software que cria uma experiência simplificada específica para as necessidades dos clientes somente SAN. "Saiba mais sobre os sistemas de armazenamento ASA r2" .

Autoridade de certificação (AC)

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

Grupo de consistência (GC)

Um grupo de consistência é uma coleção de volumes gerenciados como uma única unidade. Os CGs são sincronizados para consistência de dados em unidades de armazenamento e volumes. No ONTAP, eles fornecem gerenciamento fácil e uma garantia de proteção para uma carga de trabalho de aplicativo abrangendo vários volumes. Saiba mais sobre "grupos de consistência" .

Pilha dupla

Uma rede dual-stack é um ambiente de rede que suporta o uso simultâneo de endereços IPv4 e IPv6.

Alta Disponibilidade (HA)

Os nós do cluster são configurados em pares de HA para operações não disruptivas.

Número da unidade lógica (LUN)

Um LUN é um número usado para identificar uma unidade lógica dentro de uma Rede de Área de Armazenamento (SAN). Esses dispositivos endereçáveis são normalmente discos lógicos acessados por meio do protocolo SCSI (Small Computer System Interface) ou 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 igroup. Um subsistema NVMe pode ser associado a iniciadores para que os iniciadores associados possam acessar namespaces dentro do subsistema.

Gerenciador de ferramentas ONTAP

O ONTAP Tools Manager fornece mais controle às ONTAP tools for VMware vSphere sobre as instâncias gerenciadas do vCenter Server e backends de armazenamento integrados. Ele ajuda a gerenciar instâncias do vCenter Server, backends de armazenamento, certificados, senhas e downloads de pacotes de log.

Dispositivo Virtual Aberto (OVA)

OVA é um padrão aberto para empacotamento e distribuição de dispositivos virtuais ou software que devem ser executados em máquinas virtuais.

Objetivo de Ponto de Recuperação (RPO)

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

Sincronização ativa do SnapMirror

A sincronização ativa do SnapMirror permite que os serviços empresariais continuem operando mesmo com uma falha completa do site, permitindo que os aplicativos façam failover de forma transparente usando uma cópia secundária. Não é necessária intervenção manual ou script personalizado para acionar um failover com a sincronização ativa do SnapMirror . Saiba mais sobre "Sincronização ativa do SnapMirror" .

Backends 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. Eles permitem que o host ESXi acesse e gerencie dados persistentes, fornecendo a capacidade de armazenamento e o desempenho necessários para um ambiente virtualizado.

Cluster global (backend de armazenamento)

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

Backend de armazenamento local

Backends de armazenamento local com credenciais de cluster ou SVM são adicionados por meio da interface

de usuário das ferramentas ONTAP e são limitados a um vCenter. Ao usar credenciais de cluster localmente, os SVMs associados são mapeados automaticamente com o vCenter para gerenciar vVols ou VMFS. Para gerenciamento de VMFS, incluindo SRA, as ferramentas ONTAP oferecem suporte a credenciais SVM sem a necessidade de um cluster global.

Adaptador de Replicação de Armazenamento (SRA)

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

Máquina virtual de armazenamento (SVM)

SVM é a unidade de multilocação no ONTAP. Como uma máquina virtual executada em um hipervisor, o SVM é uma entidade lógica que abstrai recursos físicos. O SVM contém volumes de dados e um 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 dois sites estão conectados a todos os caminhos para clusters de armazenamento em ambos os sites. Caminhos entre locais são estendidos por distâncias.
- **Acesso de host não uniforme** significa que os hosts em cada site estão conectados apenas ao cluster no mesmo site. Caminhos entre sites e caminhos estendidos não estão conectados.

> O acesso uniforme ao host é suportado para qualquer implantação de sincronização ativa do SnapMirror ; o acesso não uniforme ao host é suportado apenas para implantações ativas/ativas simétricas. Saiba mais sobre "Visão geral da sincronização ativa do SnapMirror no ONTAP" .

Sistema de arquivos de máquina virtual (VMFS)

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

Volumes virtuais (vVols)

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

Política de armazenamento de 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 de tipo de armazenamento NetApp vVols .

Recuperação de site VMware Live

O VMware Live Site Recovery, anteriormente conhecido como Site Recovery Manager (SRM), fornece continuidade de negócios, recuperação de desastres, migração de sites e recursos de testes sem interrupções para ambientes virtuais VMware.

APIs do VMware vSphere para reconhecimento de armazenamento (VASA)

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

APIs de armazenamento do VMware vSphere - Integração de matriz (VAAI)

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

Cluster de armazenamento vSphere Metro

O vSphere Metro Storage Cluster (vMSC) é uma arquitetura que habilita e oferece suporte ao vSphere em uma implantação de cluster estendida. As soluções vMSC são compatíveis com o NetApp MetroCluster e o SnapMirror Active Sync (antigo SMBC). Essas soluções proporcionam maior continuidade dos negócios em caso de falha de domínio. O modelo de resiliência é baseado em suas escolhas de configuração específicas. Saiba mais sobre "Cluster de armazenamento VMware vSphere Metro" .

Armazenamento de dados vVols

O armazenamento de dados vVols é uma representação lógica de armazenamento de dados de um contêiner vVols criado e mantido por um provedor VASA.

RPO zero

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

Controle de acesso baseado em função

Saiba mais sobre as ONTAP tools for 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 sua organização.

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

Componentes RBAC

Em um nível mais alto, há vários componentes que geralmente são incluídos em cada implementação do RBAC. Esses componentes são vinculados de diferentes maneiras como parte da definição dos processos de autorização.

Privileges

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

Funções

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

Objetos

Um *objeto* representa um recurso real ou abstrato identificado dentro do ambiente RBAC. As ações definidas por meio dos privilégios são executadas em ou com os objetos associados. Dependendo da implementação, privilégios podem ser concedidos a um tipo de objeto ou a uma instância de objeto específica.

Usuários e grupos

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

Permissões

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

Dois ambientes RBAC

Há dois ambientes RBAC distintos que você precisa considerar ao trabalhar com ONTAP tools for VMware vSphere 10.

Servidor VMware vCenter

A implementação do 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 ONTAP tools for VMware vSphere 10, o ambiente RBAC é estendido para incluir objetos adicionais que representam os recursos das ferramentas ONTAP . O acesso a esses objetos é fornecido por meio do plug-in remoto. Veja"Ambiente RBAC do vCenter Server" para mais informações.

Cluster ONTAP

As ONTAP tools for VMware vSphere 10 se conectam a um cluster ONTAP por meio da API REST ONTAP para executar operações relacionadas ao armazenamento. O acesso aos recursos de armazenamento é controlado por meio de uma função ONTAP associada ao usuário ONTAP fornecido durante a autenticação. Ver "Ambiente ONTAP RBAC" para maiores informações.

RBAC com VMware vSphere

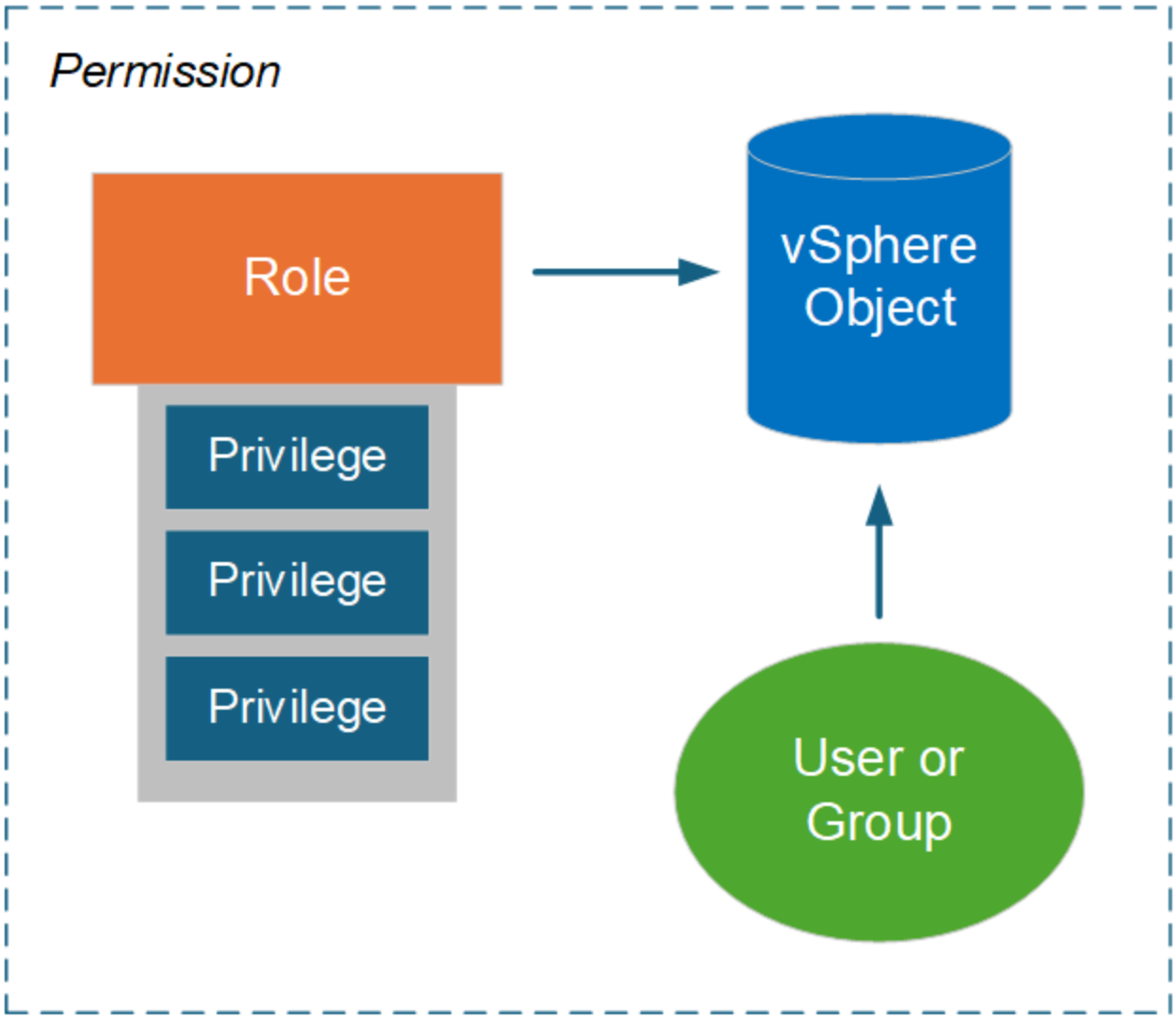
Ambiente RBAC do vCenter Server com ONTAP tools for VMware vSphere 10

O VMware vCenter Server fornece um recurso RBAC que permite controlar o acesso a

objetos do 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 na 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 do vSphere, como o vCenter Server, hosts ESXi, máquinas virtuais, armazenamentos de dados, data centers e pastas. Com base nas permissões atribuídas ao objeto, o vCenter Server determina quais ações ou tarefas podem ser executadas no objeto por cada usuário ou grupo. Para as

tarefas específicas das ONTAP tools for VMware vSphere, todas as permissões são atribuídas e validadas no nível raiz ou da pasta raiz do vCenter Server. Ver "Usar RBAC com o servidor vCenter" para maiores informações.

Privileges e funções

Há dois tipos de privilégios do vSphere usados com ONTAP tools for VMware vSphere 10. Para simplificar o trabalho com o RBAC neste ambiente, as ferramentas ONTAP fornecem funções contendo os privilégios nativos e personalizados necessários. Os privilégios incluem:

- Privilégios nativos do vCenter Server

  Esses são os privilégios fornecidos pelo vCenter Server.

- Privilégios específicos das ferramentas ONTAP

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

Usuários e grupos

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

Use o vCenter Server RBAC com ONTAP tools for VMware vSphere 10

Há vários aspectos das ONTAP tools for VMware vSphere 10 RBAC 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 do vSphere e às tarefas administrativas associadas. Se não for necessário limitar o acesso, você pode 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 ONTAP tools for VMware vSphere 10.

Hierarquia de objetos do vSphere

O inventário de objetos do vSphere é organizado em uma hierarquia. Por exemplo, você pode descer na hierarquia da seguinte maneira:

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

Todas as permissões são validadas na hierarquia de objetos do vSphere, exceto as operações do plug-in VAAI, que são validadas no host ESXi de destino.

Funções incluídas com ONTAP tools for VMware vSphere 10

Para simplificar o trabalho com o vCenter Server RBAC, as ONTAP tools for VMware vSphere fornecem funções predefinidas adaptadas a diversas tarefas de administração.

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

Para visualizar as ONTAP tools for VMware vSphere , selecione **Menu** na parte superior do vSphere Client e clique em **Administração** e depois em **Funções** à esquerda. Há três funções predefinidas, conforme descrito abaixo.

Ferramentas NetApp ONTAP tools for VMware vSphere Administrator

Fornece todos os privilégios nativos do vCenter Server e privilégios específicos das ferramentas ONTAP necessários para executar as principais ONTAP tools for VMware vSphere .

ONTAP tools for VMware vSphere NetApp ONTAP para VMware vSphere somente leitura

Fornece acesso somente leitura às ferramentas ONTAP . Esses usuários não podem executar nenhuma ONTAP tools for VMware vSphere que sejam controladas por acesso.

ONTAP tools for VMware vSphere NetApp ONTAP para VMware vSphere Provision

Fornece alguns dos privilégios nativos do vCenter Server e privilégios específicos das ferramentas ONTAP necessários para provisionar armazenamento. Você pode executar as seguintes tarefas:

- Criar novos armazenamentos de dados
- Gerenciar armazenamentos de dados

Objetos vSphere e backends de armazenamento ONTAP

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

Trabalhando com o vCenter Server RBAC

Há algumas coisas a considerar ao trabalhar com os privilégios e permissões do vCenter Server.

Privilégios necessários

Para acessar a interface de usuário das ONTAP tools for VMware vSphere 10, você precisa ter o privilégio *View* específico das ferramentas ONTAP . Se você entrar no vSphere sem esse privilégio e clicar no ícone do NetApp , as ONTAP tools for VMware vSphere exibirão uma mensagem de erro e impedirão que você acesse a interface do usuário.

O nível de atribuição na hierarquia de objetos do vSphere determina quais partes da interface do usuário você pode acessar. Atribuir o privilégio Exibir ao objeto raiz permite que você acesse as ONTAP tools for 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 os menus das ONTAP tools for VMware vSphere que você pode acessar e usar.

Atribuindo permissões

Você precisa usar permissões do vCenter Server se quiser limitar o acesso aos objetos e tarefas do vSphere.

O local onde você atribui permissão na hierarquia de objetos do vSphere determina as ONTAP tools for VMware vSphere 10 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 ONTAP tools for VMware vSphere 10 se aplicam a objetos personalizados não vSphere, como sistemas de armazenamento. Se possível, você deve atribuir essas permissões às ONTAP tools for VMware vSphere, porque não há nenhum objeto vSphere ao qual você possa atribuí-las. Por exemplo, qualquer permissão que inclua um privilégio "Adicionar/Modificar/Remover sistemas de armazenamento" das ONTAP tools for VMware 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 filhos que substituem as permissões herdadas do pai.

Você pode modificar uma permissão a qualquer momento. Se você alterar qualquer privilégio dentro de uma permissão, os usuários associados à permissão precisarão sair do vSphere e efetuar login novamente para habilitar a alteração.

RBAC com ONTAP

Ambiente ONTAP RBAC com ONTAP tools for VMware vSphere 10

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

Visão geral das opções administrativas

Há várias opções disponíveis ao usar o ONTAP RBAC, dependendo do seu ambiente e objetivos. Uma visão geral das principais decisões administrativas é apresentada abaixo. Veja também "Automação ONTAP : Visão geral da segurança RBAC" para mais informações.

> O ONTAP RBAC é adaptado para um ambiente de armazenamento 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. Não é necessário configurar permissões explícitas, como aquelas usadas com o vCenter Server, com o ONTAP RBAC.

Tipos de funções e privilégios

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

- DESCANSAR

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

- Tradicional

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

ONTAP .

Embora as funções REST tenham sido introduzidas mais recentemente, as funções tradicionais têm algumas vantagens. Por exemplo, parâmetros de consulta adicionais podem ser incluídos opcionalmente para que os privilégios definam com mais precisão os objetos aos quais são aplicados.

Escopo

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

Definições de funções

O ONTAP fornece um conjunto de funções predefinidas no nível do cluster e do SVM. Você também pode definir funções personalizadas.

Trabalhando com funções REST do ONTAP

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

Mapeamento de funções

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

Definindo uma função REST usando privilégios CLI

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

Interface administrativa ao definir funções ONTAP

Você pode criar usuários e funções com o ONTAP CLI e a REST API. No entanto, é mais conveniente usar a interface do System Manager junto com o arquivo JSON disponível através do ONTAP tools Manager. Ver "Use o ONTAP RBAC com ONTAP tools for VMware vSphere 10" para maiores informações.

Use o ONTAP RBAC com ONTAP tools for VMware vSphere 10

Há vários aspectos das ONTAP tools for VMware vSphere 10 RBAC com ONTAP que você deve considerar antes de usá-lo em um ambiente de produção.

Visão geral do processo de configuração

As ONTAP tools for VMware vSphere 10 incluem suporte para criar um usuário ONTAP com uma função personalizada. As definições são empacotadas em um arquivo JSON que você pode carregar no cluster ONTAP . Você pode criar o usuário e adaptar a função ao seu ambiente e às suas necessidades de segurança.

As principais etapas de configuração são descritas detalhadamente abaixo. Consulte"Configurar funções e privilégios de usuário do ONTAP" para mais detalhes.

1. Preparar

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

2. Baixe o arquivo de definição JSON

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

3. Crie um usuário ONTAP com uma função

Após efetuar login no Gerenciador do Sistema, você pode criar o usuário e a função:

1. Selecione **Cluster** à esquerda e depois **Configurações**.
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 na sua estação de trabalho local e carregue-o.

4. Configurar a função

Como parte da definição da função, você precisa tomar diversas decisões administrativas. VerConfigurar a função usando o Gerenciador de Sistema para mais detalhes.

Configurar a função usando o Gerenciador de Sistema

Depois de começar a criar um novo usuário e função com o System Manager e carregar o arquivo JSON, você pode personalizar a função com base no seu ambiente e necessidades.

Configuração de usuário e função principais

As definições do RBAC são agrupadas como vários recursos de produto, incluindo combinações de VSC, VASA Provider e SRA. Você deve selecionar o ambiente ou ambientes onde precisa de suporte 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

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

- Descoberta

  Esta função permite que você adicione sistemas de armazenamento.

- Criar armazenamento

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

- Modificar armazenamento

  Esta função permite que você modifique o armazenamento. Ele também inclui todos os privilégios associados à descoberta e criação de funções de armazenamento.

- Destruir armazenamento

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

Gerar o usuário com uma função

Depois de selecionar as opções de configuração para seu ambiente, clique em **Adicionar** e o ONTAP criará 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 que você selecionou
- Lista dos conjuntos de privilégios.

Exemplo

```
OTV_10_VSC_Discovery_Create
```

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

Alta disponibilidade para ONTAP tools for VMware vSphere

As ONTAP tools for VMware vSphere oferecem suporte a uma configuração de alta disponibilidade (HA) para ajudar a fornecer funcionalidade ininterrupta das ONTAP tools for VMware vSphere durante falhas.

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

- Falha do host

  Somente falhas de nó único são suportadas.

- Falha de rede
- Falha da máquina virtual (falha do sistema operacional convidado)
- Falha no aplicativo (ferramentas ONTAP)

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

As ONTAP tools for VMware vSphere não oferecem suporte ao vCenter HA.

Para habilitar o recurso HA, a adição a quente da CPU e a conexão a quente da memória devem ser habilitadas durante a implantação ou posteriormente nas ONTAP tools for VMware vSphere .

Interface de usuário do gerenciador de ferramentas ONTAP

As ONTAP tools for VMware vSphere são um sistema multilocatário que pode gerenciar várias instâncias do vCenter Server. O ONTAP Tools Manager fornece mais controle ao administrador do ONTAP tools for VMware vSphere sobre as instâncias gerenciadas do vCenter Server e os backends de armazenamento integrados.

O Gerenciador de ferramentas ONTAP ajuda em:

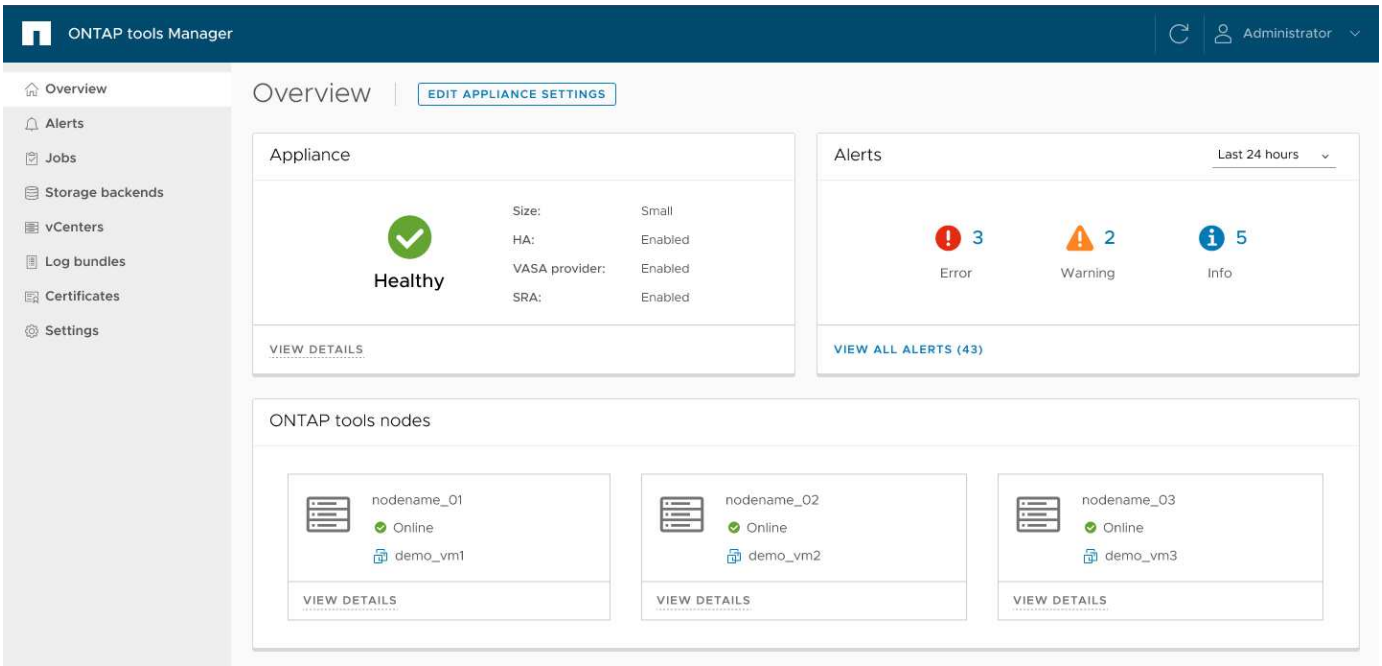
- Gerenciamento de instâncias do vCenter Server - Adicione e gerencie instâncias do vCenter Server às

ferramentas ONTAP .

- Gerenciamento de backend de armazenamento - Adicione e gerencie clusters de armazenamento ONTAP às ONTAP tools for VMware vSphere e mapeie-os para instâncias integradas do vCenter Server globalmente.
- Downloads de pacotes de log - Colete arquivos de log para ONTAP tools for VMware vSphere.
- Gerenciamento de certificados - Altere o certificado autoassinado para um certificado de CA personalizado e renove ou atualize todos os certificados do VASA Provider e das ferramentas ONTAP .
- Gerenciamento de senhas - Redefina a senha do aplicativo OVA do usuário.

Para acessar o Gerenciador de ferramentas ONTAP , inicie `https://<ONTAPtoolsIP>:8443/virtualization/ui/` no navegador e faça login com as credenciais de administrador das ONTAP tools for VMware vSphere fornecidas durante a implantação.

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



Cartão	Descrição
Cartão de eletrodomésticos	O cartão do dispositivo fornece o status geral do dispositivo ONTAP Tools. Ele mostra os detalhes da configuração do dispositivo e o status dos serviços habilitados. Para obter informações adicionais sobre o dispositivo ONTAP Tools, selecione o link **Exibir detalhes**. Quando uma ação de edição de configuração do dispositivo está em andamento, o portlet do dispositivo mostra o status e os detalhes do trabalho.

Cartão	Descrição
Cartão de alertas	O cartão Alertas lista os alertas das ferramentas ONTAP por tipo, incluindo os alertas no nível do nó HA. Você pode visualizar a lista de alertas selecionando o texto de contagem (hiperlink). O link direciona você para a página de visualização de alertas filtrada pelo tipo selecionado.
vCenters	O cartão vCenter mostra o status de integridade dos vCenters no sistema.
Backends de armazenamento	O cartão Backends de armazenamento mostra o status de integridade dos backends de armazenamento no sistema.
Cartão de nós de ferramentas ONTAP	O cartão de nós das ferramentas 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 **Exibir detalhes** para visualizar detalhes adicionais relacionados ao nó selecionado. [NOTA] Em uma configuração não HA, apenas um nó é mostrado. Na configuração do HA, três nós são mostrados.

Implantar ONTAP tools for VMware vSphere

Início rápido para ONTAP tools for VMware vSphere

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

Inicialmente, você implantará ONTAP tools for 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 precisar expandir sua configuração para usar datastores vVols e alta disponibilidade (HA), você fará isso depois de concluir este fluxo de trabalho. Para mais informações, consulte o "Fluxo de trabalho de implantação de HA" .

1 Planeje sua implantação

Verifique se as versões do seu host vSphere, ONTAP e ESXi são compatíveis com a versão das ferramentas ONTAP . Aloque CPU, memória e espaço em disco suficientes. Com base nas suas regras de segurança, pode ser necessário configurar firewalls ou outras ferramentas de segurança para permitir o tráfego de rede.

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

- "Ferramenta de Matriz de Interoperabilidade"
- "ONTAP tools for VMware vSphere"
- "Antes de começar"

2 Implantar ONTAP tools for VMware vSphere

Inicialmente, você implantará as ONTAP tools for VMware vSphere como uma configuração de nó único de pequeno porte que fornece serviços essenciais para oferecer suporte a datastores NFS e VMFS. Se você planeja expandir sua configuração para usar datastores vVols e alta disponibilidade (HA), faça isso após concluir este fluxo de trabalho. Para expandir para uma configuração de HA, certifique-se de que a adição a quente de CPU e a conexão a quente de memória estejam habilitadas.

- "Implantar ONTAP tools for VMware vSphere"

3 Adicionar instâncias do vCenter Server

Adicione instâncias do vCenter Server às ONTAP tools for VMware vSphere para configurar, gerenciar e proteger armazenamentos de dados virtuais no ambiente do vCenter Server.

- "Adicionar instâncias do vCenter Server"

4 Configurar funções e privilégios de usuário do ONTAP

Configure novas funções e privilégios de usuário para gerenciar backends de armazenamento usando o arquivo JSON fornecido com as ONTAP tools for VMware vSphere.

- "Configurar funções e privilégios de usuário do ONTAP"

5 Configurar os backends de armazenamento

Adicione um backend de armazenamento a um cluster ONTAP . Para configurações de multilocação em que o vCenter atua como locatário com um SVM associado, use o Gerenciador de ferramentas ONTAP para adicionar o cluster. Associe o backend de armazenamento ao vCenter Server para mapeá-lo globalmente à instância integrada do vCenter Server.

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

- "Adicionar um backend de armazenamento"
- "Associar o backend de armazenamento 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) Configurar proteção SRA

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

- "Habilitar ONTAP tools for VMware vSphere"
- "Configurar SRA no dispositivo VMware Live Site Recovery"

8 (Opcional) Habilitar a proteção de sincronização ativa do SnapMirror

Configure ONTAP tools for VMware vSphere para gerenciar a proteção do cluster de host para sincronização ativa do SnapMirror . Execute o cluster ONTAP e o peering SVM em sistemas ONTAP para usar a sincronização ativa do SnapMirror . Isso se aplica somente aos armazenamentos de dados VMFS.

- "Proteger usando proteção de cluster de host"

9 Configure backup e recuperação para suas ONTAP tools for VMware vSphere

Agende backups das suas ONTAP tools for VMware vSphere , que você pode usar para recuperar a configuração em caso de falha.

- "Crie um backup e recupere a configuração das ferramentas ONTAP"

Fluxo de trabalho de implantação de alta disponibilidade (HA)

Se estiver usando datastores vVols , você precisará expandir a implantação inicial das ferramentas ONTAP para uma configuração de alta disponibilidade (HA) e habilitar os serviços do Provedor VASA.

1 **Amplie a implantação**

Você pode ampliar as ONTAP tools for VMware vSphere para aumentar o número de nós na implantação e alterar a configuração para uma configuração de HA.

- "Alterar ONTAP tools for VMware vSphere"

2 **Habilitar serviços**

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

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

- "Habilitar serviços de provedor VASA e SRA"

3 **Atualizar os certificados**

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

- "Gerenciar certificados"

ONTAP tools for VMware vSphere

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

Você pode usar ONTAP tools for VMware vSphere com o VMware vCenter Server Virtual Appliance (vCSA). Você deve implantar ONTAP tools for 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 fino
  - 348 GB para instalações com provisionamento espesso

- **Requisitos de dimensionamento do sistema host** A memória recomendada de acordo com o tamanho da implantação é mostrada na tabela abaixo. Para implantar alta disponibilidade (HA), você precisará de três vezes o tamanho do dispositivo especificado na tabela.

Tipo de implantação	CPUs por nó	Memória (GB) por nó	Espaço em disco (GB) provisionado por nó
Pequeno	9	18	350
Médio	13	26	350
NOTA grande: A implantação grande é somente para configuração de HA.	17	34	350

Quando o backup está habilitado, cada cluster de ferramentas ONTAP precisa de mais 50 GB de espaço no armazenamento de dados onde as VMs são implantadas. Portanto, o não-HA requer 400 GB, e o HA requer 1100 GB de espaço no total.

Requisitos mínimos de armazenamento e aplicação

Armazenamento, host e aplicativos	Requisitos de versão
ONTAP	9.14.1, 9.15.1, 9.16.0, 9.16.1 e 9.16.1P3 FAS, ASA Série A, ASA Série C, AFF Série A, AFF Série C e ASA r2.
Ferramentas ONTAP suportam hosts ESXi	7.0.3 em diante
Ferramentas ONTAP suportadas pelo vCenter Server	7.0U3 em diante
Provedor VASA	3,0
Aplicação OVA	10,4
Host ESXi para implantar máquina virtual de ferramentas ONTAP	7.0U3 e 8.0U3
vCenter Server para implantar ferramentas ONTAP em máquinas virtuais	7.0 e 8.0

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

A Interoperability Matrix Tool (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"

Requisitos portuários

A tabela a seguir descreve as portas de rede utilizadas pela NetApp e suas finalidades. Certifique-se de que essas portas estejam abertas e acessíveis para facilitar a operação e a comunicação adequadas dentro do sistema. Certifique-se de que as configurações de rede necessárias estejam implementadas para permitir o tráfego nessas portas e o funcionamento correto dos serviços associados. Dependendo das suas políticas de

segurança, pode ser necessário configurar firewalls ou outros dispositivos de segurança para permitir esse tráfego na sua rede.

Porta	Protocolo	Descrição
8143	TCP	Conexões HTTP/HTTPS para ferramentas ONTAP .
8043	TCP	Conexões HTTP/HTTPS para ferramentas ONTAP .
9060	TCP	Conexões HTTP/HTTPS para ferramentas ONTAP .
22	TCP	O Ansible usa essa porta SSH para comunicação durante o provisionamento do cluster. Esta porta é necessária para funcionalidades como alteração de senha do usuário de manutenção, mensagens de status e para atualizar valores em todos os três nós no caso de configuração de HA.
443	TCP	Esta é a porta de passagem para comunicação de entrada para o serviço do Provedor VASA. O certificado autoassinado do provedor VASA e o certificado CA personalizado são hospedados nesta porta.
8443	TCP	Esta 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 do etcd.
2380	TCP	Esta é a porta padrão para comunicação de servidor para servidor para o cluster etcd usada para o algoritmo de consenso raft, no qual o etcd se baseia para replicação e consistência de dados.
7472	TCP/UDP	Esta é a porta de serviço de métricas do Prometheus.
7946	TCP/UDP	Esta porta é usada para descoberta de rede de contêineres do Docker.

9083	TCP	Esta porta é uma porta de serviço usada internamente para o serviço do Provedor VASA.
1162	UDP	Esta é a porta de pacotes de trap SNMP.
6443	TCP	Fonte: nós de agentes RKE2. Destino: nós do servidor REK2. Descrição: API do Kubernetes
9345	TCP	Fonte: nós de agentes RKE2. Destino: nós do servidor REK2. Descrição: API do supervisor REK2
8472	TCP+UDP	Todos os nós precisam ser capazes de alcançar outros nós pela porta UDP 8472 quando o Flannel VXLAN for usado. Fonte: todos os nós RKE2. Destino: todos os nós REK2. Descrição: Canal CNI com VXLAN
10250	TCP	Fonte: todos os nós RKE2. Destino: todos os nós REK2. Descrição: Métricas do Kubelet
30000-32767	TCP	Fonte: todos os nós RKE2. Destino: todos os nós REK2. Descrição: Intervalo de portas NodePort
123	TCP	O Ntpd usa esta porta para realizar a validação do servidor NTP.
137-139	TCP/UDP	Pacotes de compartilhamento SMB/Windows.
6789	TCP	Monitor Ceph (MON)
3300	TCP	Monitor Ceph (MON)
6800-7300	TCP	Gerenciadores Ceph, OSDs e Sistema de Arquivos (MDS).
80	TCP	Gateway Ceph RADOS (RGW)
9080	TCP	Conexões VP HTTP/HTTPS (somente de 127.0.0.0/8 para IPv4 ou ::1/128 para IPv6).

Limites de configuração para implantar ONTAP tools for VMware vSphere

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

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

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

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

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

Tamanho da implantação do vCenter	**Pequeno**	**Médio**
Número total de máquinas virtuais configuradas para proteção usando replicação baseada em matriz	2000	5000
Número total de grupos de proteção de replicação baseados em matriz	250	250
Número total de grupos de proteção por plano de recuperação	50	50
Número de armazenamentos de dados replicados	255	255
Número de VMs	4000	7000

A tabela a seguir mostra o número de VMware Live Site Recovery e as ONTAP tools for VMware vSphere .

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

Para obter mais informações, consulte "Limites operacionais do VMware Live Site Recovery" .

Antes de começar…

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

Requisitos	Seu status
As versões do vSphere, do ONTAP e do host ESXi são compatíveis com a versão das ferramentas ONTP.	☐ Sim ☐ Não
O ambiente do vCenter Server está configurado e configurado	☐ Sim ☐ Não
O cache do navegador foi 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 ONTAP tools for VMware vSphere se conectarão após a implantação para registro	☐ Sim ☐ Não
O nome de domínio no qual o certificado é emitido é mapeado para o endereço IP virtual em uma implantação multi-vCenter, onde certificados de CA personalizados são obrigatórios.	☐ Sim ☐ Não
Você executou a verificação nslookup no nome de domínio para verificar se o domínio está sendo resolvido para o endereço IP pretendido.	☐ Sim ☐ Não
O certificado é criado com o nome de domínio e o endereço IP das ferramentas ONTAP .	☐ Sim ☐ Não
O aplicativo de ferramentas ONTAP e os serviços internos podem ser acessados pelo vCenter Server.	☐ Sim ☐ Não
Ao usar SVMs multilocatários, você tem um LIF de gerenciamento de SVM em cada SVM.	☐ Sim ☐ Não

Planilha de implantação

Para implantação de nó único

Use a planilha a seguir para reunir as informações necessárias para as ONTAP tools for VMware vSphere :

Exigência	Seu valor
Endereço IP para o aplicativo de ferramentas ONTAP . Este é o endereço IP para acessar a interface web das ferramentas ONTAP	
Ferramentas ONTAP endereço IP virtual para comunicação interna. Este endereço IP é usado para comunicação interna em uma configuração com várias instâncias de ferramentas ONTAP . Este endereço IP não deve ser o mesmo que o endereço IP do aplicativo de ferramentas ONTAP .	
Nome do host DNS para o primeiro nó	
Servidor DNS primário	

Exigência	Seu valor
Servidor DNS secundário	
Domínio de pesquisa DNS	
Endereço IPv4 para o primeiro nó. É um endereço IPv4 exclusivo para a interface de gerenciamento de nós 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 livres no DNS. Todos os endereços IP devem estar na mesma VLAN selecionada para implantação.

Para implantação de alta disponibilidade (HA)

Além dos requisitos de implantação de nó único, você precisará das seguintes informações para implantação de HA:

Exigência	Seu valor
Servidor DNS primário	
Servidor DNS secundário	
Domínio de pesquisa DNS	
Nome do host DNS para o segundo nó	
Endereço IP para o segundo nó	
Nome do 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 seu firewall de rede. As ferramentas ONTAP devem conseguir acessar esse LIF pela porta 443. Consulte"Requisitos portuários" para atualizações mais recentes.

Configurações de armazenamento ONTAP

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

- Se você estiver usando o Fibre Channel (FC) para conectividade de armazenamento, configure o zoneamento em seus switches FC para conectar os hosts ESXi com os LIFs FC do SVM. "Aprenda sobre zoneamento FC e FCoE com sistemas ONTAP"

- Para usar a replicação SnapMirror gerenciada por ferramentas ONTAP , o administrador de armazenamento ONTAP deve criar "Relacionamentos de pares de cluster ONTAP" e "Relações de pares SVM intercluster ONTAP" no ONTAP antes de usar o SnapMirror.

Implantar ONTAP tools for VMware vSphere

O dispositivo ONTAP tools for VMware vSphere é implantado como um nó único de pequeno porte com serviços principais para oferecer suporte a datastores NFS e VMFS. O processo de implantação do ONTAP Tools pode levar até 45 minutos.

Antes de começar

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

> Você deve armazenar a biblioteca de conteúdo em um armazenamento de dados 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 habilitar a implantação de HA posteriormente, não implante a máquina virtual que hospeda as ferramentas 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 Se você planeja usar apenas uma pequena implantação de nó único, não é necessário criar uma biblioteca de conteúdo.

1. Baixe o arquivo que contém os binários (*.ova*) e os certificados assinados para as ONTAP tools for VMware vSphere do "Site de suporte da NetApp" .
2. Efetue 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 mais informações, consulte "Criação e uso da biblioteca de conteúdo" blog.

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

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

Passos

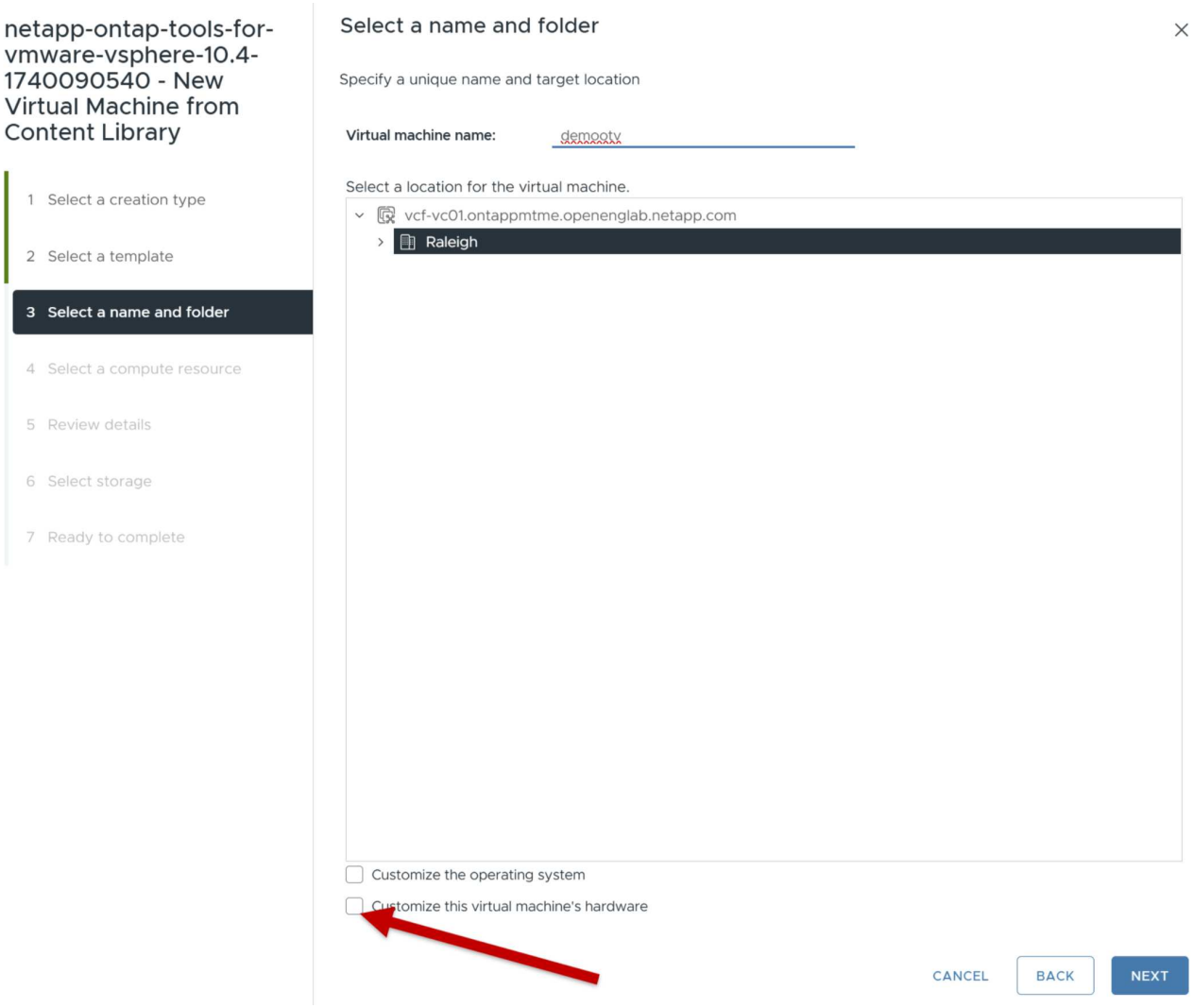
1. Baixe o arquivo que contém os binários (*.ova*) e os certificados assinados para as ONTAP tools for VMware vSphere do "Site de suporte da NetApp" . Se você importou o OVA para a biblioteca de conteúdo, pode pular esta etapa e prosseguir para a próxima.
2. Efetue login no servidor vSphere.
3. Navegue até o pool de recursos, cluster ou host onde você pretende implantar o OVA.

   Nunca armazene ONTAP tools for VMware vSphere em armazenamentos de dados vVols que ela gerencia.

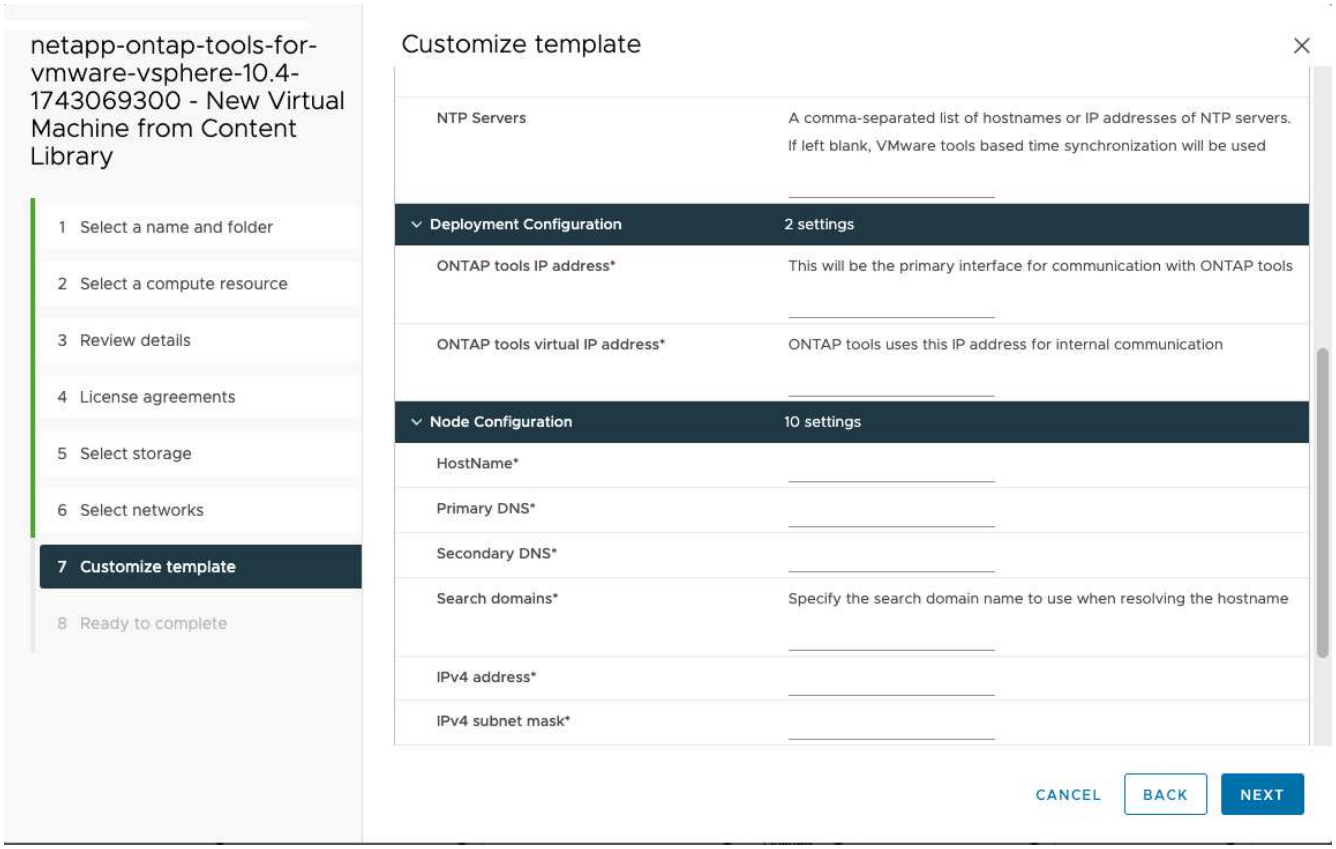
4. Você pode implantar o OVA da biblioteca de conteúdo ou do sistema local.

Do sistema local	Da biblioteca de conteúdo
a. Clique com o botão direito e selecione **Implantar modelo OVF…**. b. Escolha o arquivo OVA na URL ou navegue até seu local e selecione **Avançar**.	a. Acesse sua biblioteca de conteúdo e selecione o item de biblioteca que deseja implantar. b. Selecione **Ações** > **Nova VM deste modelo**

5. No campo **Selecione um nome e uma pasta**, insira o nome da máquina virtual e escolha seu local.
   - Se você estiver usando a versão vCenter Server 8.0.3, selecione a opção **Personalizar o hardware desta máquina virtual**, que ativará uma etapa adicional chamada **Personalizar hardware** antes de prosseguir para a janela **Pronto para concluir**.
   - Se você estiver usando a versão vCenter Server 7.0.3, siga as etapas na seção **o que vem a seguir?** no final da
     implantação.



6. Selecione um recurso do computador e selecione **Avançar**. Opcionalmente, marque a caixa para **Ligar automaticamente a VM implantada**.
7. Revise os detalhes do modelo e selecione **Avançar**.
8. Leia e aceite o contrato de licença e selecione **Avançar**.
9. Selecione o armazenamento para a configuração e o formato do disco e selecione **Avançar**.
10. Selecione a rede de destino para cada rede de origem e selecione **Avançar**.
11. Na janela **Personalizar modelo**, preencha os campos obrigatórios e selecione **Avançar**
    .

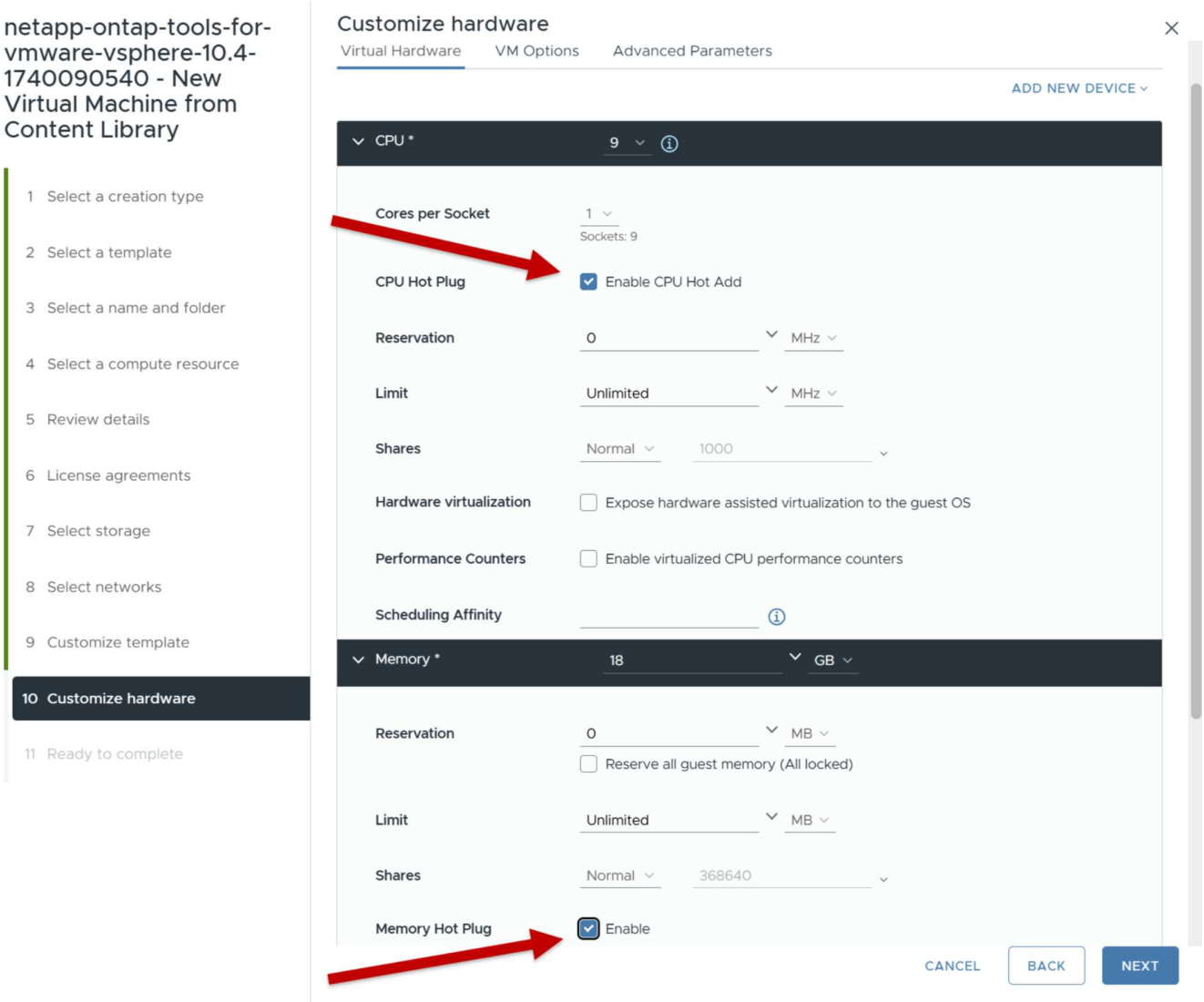


- As informações são validadas durante a instalação. Se houver alguma discrepância, uma mensagem de erro será exibida no console da web e você será solicitado a corrigi-la.
- Os nomes de host devem incluir letras (AZ, az), dígitos (0-9) e hifens (-). Para configurar a pilha dupla, especifique o nome do host mapeado para o endereço IPv6.

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

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

12. Ao usar a versão vCenter Server 8.0.3, na janela **Personalizar hardware**, ative as opções **CPU hot add** e **Memory hot plug** para permitir a funcionalidade
HA.



13. Revise os detalhes na janela **Pronto para concluir** e 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 concluir a tarefa se a opção para ligar a VM automaticamente não tiver sido selecionada.

Você pode acompanhar o progresso da instalação no console web da VM.

Se houver discrepâncias no formulário OVF, uma caixa de diálogo solicitará uma ação corretiva. Use o botão tab para navegar, faça as alterações necessárias e selecione **OK**. Você tem três tentativas para resolver qualquer problema. Se os problemas persistirem 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 ONTAP tools for VMware vSphere com vCenter Server 7.0.3, siga estas etapas após a implantação.

1. Efetue login no cliente vCenter
2. Desligue o nó de ferramentas ONTAP .
3. Navegue até as ONTAP tools for VMware vSphere em **Inventários** e selecione a opção **Editar configurações**.

4. Nas opções **CPU**, marque a caixa de seleção **Habilitar adição a quente da CPU**
5. Nas opções de **Memória**, marque a caixa de seleção **Ativar** em **Memória hot plug**.

Códigos de erro de implantação

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

Todos os logs de erros são registrados no arquivo ansible-perl-errors.log para facilitar o rastreamento e a resolução de problemas. Este arquivo de log contém o código de erro e a tarefa Ansible 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 nenhuma solução for mencionada.

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

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

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

Código de erro de implantação	Fluxo de trabalho	Resolução
049	Para rede e validação, o script Perl também os atribuirá em breve	-
050	Falha na geração da chave SSH	Reinicie a máquina virtual primária (VM).
053	Falha na instalação do RKE2	Execute o seguinte e reinicie a VM primária ou reimplante: sudo rke2-killall.sh (todas as VMs) sudo rke2-uninstall.sh (todas as VMs).

054	Falha ao definir o kubeconfig	Redistribuir
055	Falha na implantação do registro	Se o pod de registro estiver presente, aguarde até que ele esteja pronto e reinicie a VM primária ou reimplante-a.
059	A implantação do KubeVip falhou	Garanta que o endereço IP virtual para o plano de controle do Kubernetes e os endereços IP das ferramentas ONTAP fornecidos durante a implantação pertençam à mesma VLAN e sejam endereços IP livres. Reinicie se todos os pontos anteriores estiverem corretos. Caso contrário, redistribua.
060	A implantação do operador falhou	Reiniciar
061	A implantação dos serviços falhou	Execute a depuração básica do Kubernetes, como obter pods, obter rs, obter svc e assim por diante no namespace ntv-system para obter mais detalhes e logs de erros em /var/log/ansible-perl-errors.log e /var/log/ansible-run.log e reimplantar.
062	A implantação dos serviços das ferramentas ONTAP falhou	Consulte os logs de erros em /var/log/ansible-perl-errors.log para obter mais detalhes e reimplantar.
065	URL da página do Swagger não está acessível	Redistribuir
066	As etapas de pós-implantação para o certificado de gateway falharam	Faça o seguinte para recuperar/concluir a atualização: * Habilite o shell de diagnóstico. * Execute o comando 'sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postDeploy'. * Verifique os logs em /var/log/post-deploy-upgrade.log.
088	A configuração da rotação de log para journald falhou	Verifique se as configurações de rede da VM são compatíveis com o host no qual a VM está hospedada. Você pode tentar migrar para outro host e reiniciar a VM.
089	Falha na alteração da propriedade do arquivo de configuração de rotação do log de resumo	Reinicie a VM primária.
096	Instalar provisionador de armazenamento dinâmico	-

108	Falha no script de semeadura	-

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

Configurar ONTAP tools for VMware vSphere

Adicionar instâncias do vCenter Server

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

Sobre esta tarefa

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

Passos

1. Abra um navegador da web e navegue até o URL: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Efetue login com as credenciais de administrador das ONTAP tools for VMware vSphere fornecidas durante a implantação.
3. Selecione **vCenters** > **Adicionar** 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 ONTAP . Você pode criar uma função personalizada sem a conta de administrador com permissões limitadas. Consulte"Use o vCenter Server RBAC com ONTAP tools for VMware vSphere 10" para mais detalhes.

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

- O plug-in do cliente vCenter é registrado como um plug-in remoto.
- Privilégios personalizados para 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 VASA Provider com uma instância do vCenter Server usando ONTAP tools for 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. Efetue login no cliente vSphere.
2. Selecione **Atalhos** > *Ferramentas NetApp ONTAP * na seção de plug-ins.
3. Selecione **Configurações** > **Configurações do provedor VASA**. O status de registro do Provedor VASA será exibido como não registrado.
4. Selecione o botão **Registrar** para registrar o Provedor VASA.
5. Insira um nome e credenciais para o Provedor VASA. O nome de usuário só pode conter letras, números e sublinhados. O comprimento da senha deve ter entre 8 e 256 caracteres.
6. Selecione **Registrar**.
7. Após um registro bem-sucedido e atualização da página, o status, o nome e a versão do Provedor VASA registrado são exibidos. Após o registro, a ação de cancelamento de registro é ativada.

O que vem a seguir

Verifique se o Provedor VASA integrado está listado em Provedor VASA do cliente vCenter:

Passos

1. Navegue até a instância do vCenter Server.
2. Efetue login com as credenciais de administrador.
3. Selecione **Provedores de armazenamento** > **Configurar**. Verifique se o Provedor VASA integrado está listado corretamente.

Instalar o plug-in NFS VAAI

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

Antes de começar

- Baixe o "Plug-in NetApp NFS para VMware VAAI" pacote de instalação.
- Certifique-se de ter o host ESXi e o patch mais recente do vSphere 7.0U3 ou versões posteriores e o ONTAP 9.14.1 ou versões posteriores.
- Monte um armazenamento de dados NFS.

Passos

1. Efetue login no cliente vSphere.
2. Selecione **Atalhos** > *Ferramentas NetApp ONTAP * na seção de plug-ins.
3. Selecione **Configurações** > **Ferramentas NFS VAAI**.
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 no vCenter Server, selecione o botão **Upload**.
5. Navegue e selecione o `.vib` arquivo e selecione **Upload** para enviar o arquivo para as ferramentas 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 qualificados para a instalação do plug-in são exibidos. Você pode monitorar o progresso da instalação na seção de 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 ONTAP tools for VMware vSphere detectam e ativam automaticamente o plug-in NFS VAAI.

O que vem a seguir?

Depois de instalar o plug-in NFS VAAI e reinicializar seu host ESXi, você precisa configurar as políticas de exportação NFS corretas para o descarregamento de cópias 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 root deve permanecer como root e o NFSv4 deve ser permitido em todos os volumes pais de junção.
- A opção de suporte VAAI precisa ser definida no servidor NFS relevante.

Para mais informações sobre o procedimento, consulte "Configurar as políticas de exportação NFS corretas para descarregamento de cópias VAAI" Artigo da KB.

Informações relacionadas

"Suporte para VMware vStorage sobre NFS"

"Habilitar ou desabilitar o NFSv4.0"

"Suporte ONTAP para NFSv4.2"

Configurar as definições do host ESXi

A configuração de multicaminhos e tempo limite do servidor ESXi garante alta disponibilidade e integridade de dados, permitindo alternar facilmente para um caminho de armazenamento de backup se um caminho primário falhar.

Configurar configurações de multicaminho e tempo limite do servidor ESXi

As ONTAP tools for VMware vSphere verificam e definem as configurações de multicaminho 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 sua 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 cliente VMware vSphere Web, selecione **Hosts e Clusters**.
2. Clique com o botão direito do mouse em um host e selecione * Ferramentas NetApp ONTAP * > **Atualizar**

dados do host.

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

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

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

Definir valores do host ESXi

Usando ONTAP tools for VMware vSphere, você pode definir tempos limite e outros valores nos hosts ESXi para garantir o melhor desempenho e failover bem-sucedido. Os valores que as ONTAP tools for VMware vSphere definem são baseados em testes internos da NetApp .

Você pode definir os seguintes valores em um host ESXi:

Configurações do adaptador HBA/CNA

Define os seguintes parâmetros para valores padrão:

- Disco.QFullSampleSize
- Disco.QFullThreshold
- Tempo limite do Emulex FC HBA
- Tempo limite do QLogic FC HBA

Configurações do MPIO

As configurações de MPIO definem os caminhos preferenciais para sistemas de armazenamento NetApp . Eles determinam quais dos caminhos disponíveis são otimizados (em oposição aos caminhos não otimizados que atravessam o cabo de interconexão) e definem o caminho preferencial 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) round-robin (VMW_PSP_RR) da configuração IOPS padrão de 1000 para um valor de 1.

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

Configurações NFS

Parâmetro	Defina este valor como…

Tamanho líquido do heap Tcpip	32
Rede.TcpipHeapMax	1024 MB
NFS.Volumes Máximos	256
NFS41.MaxVolumes	256
NFS.MaxQueueDepth	128 ou superior
NFS.HeartbeatMaxFalhas	10
NFS.Frequência de batimentos cardíacos	12
NFS.Tempo limite de pulsação	5

Configurar funções e privilégios de usuário do ONTAP

Você pode configurar novas funções e privilégios de usuário para gerenciar backends de armazenamento usando o arquivo JSON fornecido com as ONTAP tools for VMware vSphere e ONTAP System Manager.

Antes de começar

- Você deve ter baixado o arquivo de privilégios ONTAP das ONTAP tools for VMware vSphere usando *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip*.
- Você deve ter baixado o arquivo de Privileges ONTAP das ferramentas ONTAP usando `https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip`.

> Você pode criar usuários no nível do cluster ou diretamente no nível das máquinas virtuais de armazenamento (SVMs). Você também pode criar usuários sem usar o arquivo user_roles.json e, para isso, você precisa ter um conjunto mínimo de privilégios no nível SVM.

- Você deve ter feito login com privilégios de administrador para o backend de armazenamento.

Passos

1. Extraia o arquivo *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip* baixado.
2. Acesse o ONTAP System Manager usando o endereço IP de gerenciamento do cluster.
3. Efetue login no cluster com privilégios de administrador. Para configurar um usuário, execute as seguintes etapas:
   a. Para configurar o usuário das ferramentas ONTAP do cluster, selecione **Cluster** > **Configurações** > painel **Usuários e funções**.
   b. Para configurar o usuário das ferramentas SVM ONTAP , selecione **Storage SVM** > **Settings** > painel **Users and Roles**.
   c. Selecione **Adicionar** em Usuários.
   d. Na caixa de diálogo **Adicionar usuário**, selecione **Produtos de virtualização**.
   e. **Navegue** para selecionar e carregar o arquivo JSON de Privileges do ONTAP .

      O campo Produto é preenchido automaticamente.

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

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

g. Digite o nome de usuário e a senha necessários.

h. Selecione os privilégios (Descoberta, Criar armazenamento, Modificar armazenamento, Destruir armazenamento, Função NAS/SAN) necessários para o usuário e, em seguida, selecione **Adicionar**.

A nova função e usuário são adicionados, e você pode ver os privilégios detalhados da função que configurou.

Requisitos de mapeamento agregado de SVM

Para usar credenciais de usuário do SVM para provisionar datastores, internamente as ONTAP tools for VMware vSphere criam volumes no agregado especificado na API POST dos datastores. O ONTAP não permite a criação de volumes em agregados não mapeados em um SVM usando credenciais de usuário do SVM. Para resolver isso, você precisa mapear as 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 ONTAP :

```
sti115_vsim_ucs630f_aggr1 vserver show-aggregates
AvailableVserver        Aggregate      State         Size Type    SnapLock
Type-------------- -------------- ------- ---------- -------
--------------svm_test       sti115_vsim_ucs630f_aggr1
online     10.11GB vmdisk  non-snaplock
```

Crie o usuário e a função ONTAP manualmente

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

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

      Adicione o **Caminho da API REST** e o respectivo acesso no menu suspenso.

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

4. Criar usuários:
   a. Selecione **Adicionar** na tabela **Usuários**.
   b. Na caixa de diálogo **Adicionar usuário**, selecione **Gerenciador do sistema**.
   c. Digite o **Nome de usuário**.
   d. Selecione **Função** nas opções criadas na etapa **Criar funções** acima.
   e. Insira os aplicativos aos quais deseja dar acesso e o método de autenticação. ONTAPI e HTTP são os aplicativos necessários, e o tipo de autenticação é **Senha**.
   f. Defina a **Senha para o usuário** e **Salve** o usuário.

Lista de privilégios mínimos necessários para usuários de cluster com escopo global não administrativo

Os privilégios mínimos necessários para usuários de cluster com escopo global não administrativo, criados sem usar o arquivo JSON dos usuários, estão listados nesta seção. Se um cluster for adicionado no escopo local, é recomendável usar o arquivo JSON para criar os usuários, pois as ONTAP tools for VMware vSphere exigem mais do que apenas os privilégios de leitura para provisionamento no ONTAP.

Usando APIs:

API	Nível de acesso	Usado para
/api/cluster	Somente leitura	Descoberta de configuração de cluster
/api/cluster/licenciamento/licenças	Somente leitura	Verificação de licença para licenças específicas de protocolo
/api/cluster/nós	Somente leitura	Descoberta de tipo de plataforma
/api/segurança/contas	Somente leitura	Descoberta de privilégios
/api/segurança/funções	Somente leitura	Descoberta de privilégios
/api/armazenamento/agregados	Somente leitura	Verificação de espaço agregado durante o provisionamento de Datastore/Volume
/api/armazenamento/cluster	Somente leitura	Para obter os dados de espaço e eficiência do nível do cluster
/api/armazenamento/discos	Somente leitura	Para obter os discos associados em um agregado
/api/armazenamento/qos/políticas	Ler/Criar/Modificar	Gerenciamento de políticas de QoS e VM
/api/svm/svms	Somente leitura	Para obter a configuração do SVM caso o Cluster seja adicionado localmente.
/api/rede/ip/interfaces	Somente leitura	Adicionar backend de armazenamento - Para identificar o escopo do LIF de gerenciamento é Cluster/SVM

/api/armazenamento/zonas-de-disponibilidade	Somente leitura	Descoberta SAZ. Aplicável à versão ONTAP 9.16.1 em diante e aos sistemas ASA r2.

Crie ONTAP tools for VMware vSphere ONTAP

> Você precisa descobrir, criar, modificar e destruir Privileges para executar operações PATCH e reversão automática em caso de falha em armazenamentos de dados. A falta de todos esses privilégios juntos leva a interrupções no fluxo de trabalho e problemas de limpeza.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```
/api/storage/quota/reports -access readonly

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

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

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

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

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

Para sistemas ASA r2 no ONTAP versões 9.16.1 e superiores, execute o seguinte comando:

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

Crie ONTAP tools for VMware vSphere ONTAP

Para criar um usuário com escopo SVM com todos os privilégios, 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/snapmirror/policies -access read_create -vserver <vserver-name>

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Além disso, para as versões 9.16.0 e superiores do ONTAP , 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 C1_sti160-cluster_
```

Para desbloquear a conta e 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 C1_sti160-cluster
```

Atualizar ONTAP tools for VMware vSphere 10.1 para 10.3

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

Para recursos do produto:

- VSC
- Provedor VSC e VASA
- VSC e SRA
- VSC, provedor VASA e SRA.

Privilégios de cluster:

criação de função de login de segurança -role <nome-da-função-existente> -cmddirname "vserver nvme namespace show" -access all

função de login de segurança criar -role <nome-da-função-existente> -cmddirname "vserver nvme subsystem show" -access all

função de login de segurança criar -role <nome-da-função-existente> -cmddirname "vserver nvme subsystem host show" -access all

criação de função de login de segurança -role <nome da função existente> -cmddirname "mostrar mapa do subsistema vserver nvme" -access all

função de login de segurança criar -role <nome-da-função-existente> -cmddirname "vserver nvme show-interface" -access read

criação de função de login de segurança -role <nome-da-função-existente> -cmddirname "host do subsistema vserver nvme adicionar" -access all

criação de função de login de segurança -role <nome-da-função-existente> -cmddirname "mapa do subsistema vserver nvme adicionar" -access all

criação de função de login de segurança -role <nome-da-função-existente> -cmddirname "vserver nvme namespace delete" -access all

criação de função de login de segurança -role <nome-da-função-existente> -cmddirname "subsistema vserver nvme delete" -access all

criação de função de login de segurança -role <nome da função existente> -cmddirname "remoção do host do subsistema vserver nvme" -access all

criação de função de login de segurança -role <nome-da-função-existente> -cmddirname "remoção do mapa do subsistema vserver nvme" -access all

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

Privilégios SVM:

criação de função de login de segurança -role <nome da função existente> -cmddirname "vserver nvme namespace show" -access all -vserver <nome do vserver>

criação de função de login de segurança -role <nome da função existente> -cmddirname "vserver nvme subsystem show" -access all -vserver <nome do vserver>

criação de função de login de segurança -role <nome da função existente> -cmddirname "host do subsistema vserver nvme show" -access all -vserver <nome do vserver>

criação de função de login de segurança -role <nome da função existente> -cmddirname "mostrar mapa do subsistema vserver nvme" -access all -vserver <nome do vserver>

função de login de segurança criar -role <nome-da-função-existente> -cmddirname "vserver nvme show-interface" -access read -vserver <nome-do-vserver>

criação de função de login de segurança -role <nome da função existente> -cmddirname "host do subsistema

vserver nvme adicionar" -access all -vserver <nome do vserver>

criação de função de login de segurança -role <nome da função existente> -cmddirname "mapa do subsistema vserver nvme adicionar" -access all -vserver <nome do vserver>

criação de função de login de segurança -role <nome da função existente> -cmddirname "vserver nvme namespace delete" -access all -vserver <nome do vserver>

criação de função de login de segurança -role <nome da função existente> -cmddirname "subsistema vserver nvme delete" -access all -vserver <nome do vserver>

criação de função de login de segurança -role <nome da função existente> -cmddirname "remoção do host do subsistema vserver nvme" -access all -vserver <nome do vserver>

criação de função de login de segurança -role <nome da função existente> -cmddirname "remoção do mapa do subsistema vserver nvme" -access all -vserver <nome do vserver>

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

```
vserver nvme namespace create

vserver nvme namespace modify

vserver nvme subsystem create

vserver nvme subsystem modify
```

Atualizar ONTAP tools for VMware vSphere 10.3 para 10.4

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

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

Para recursos do produto:

- VSC
- Provedor VSC e VASA
- VSC e SRA
- VSC, provedor VASA e SRA.

Privilégios de cluster:

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

Adicionar um backend de armazenamento

Adicionar um backend de armazenamento permite que você integre um cluster ONTAP .

Sobre esta tarefa

No caso de configurações de multilocação em que o vCenter atua como locatário com um SVM associado, use o Gerenciador de ferramentas ONTAP para adicionar o cluster. Associe o backend de armazenamento ao vCenter Server para mapeá-lo globalmente à instância integrada do vCenter Server. O locatário do vCenter deve integrar as Máquinas Virtuais de Armazenamento (SVMs) desejadas. Isso permite que um usuário SVM provisione armazenamentos de dados vVols . Você pode adicionar armazenamento no vCenter usando o SVM.

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

Usando o Gerenciador de ferramentas ONTAP

> Em uma configuração multilocatário, você pode adicionar um cluster de backend de armazenamento globalmente e um SVM localmente para usar credenciais de usuário do SVM.

Passos

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

   > LIFs de gerenciamento de endereços IPv4 e IPv6 são suportados.

Usando a interface de usuário do cliente vSphere

> Ao configurar um backend de armazenamento por meio da interface de usuário do cliente vSphere, é importante observar que os datastores vVols não oferecem suporte à adição direta de um usuário SVM.

1. Efetue login no cliente vSphere.
2. Na página de atalhos, selecione * Ferramentas NetApp ONTAP * na seção de plug-ins.
3. Selecione **Backends de armazenamento** na barra lateral.
4. Adicione o backend 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 SVM.

O que vem a seguir?

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

Associar um backend de armazenamento a uma instância do vCenter Server

Associe um backend de armazenamento ao vCenter Server para criar um mapeamento entre o backend de armazenamento e a instância do vCenter Server integrada globalmente.

Passos

1. Inicie o ONTAP Tools Manager em um navegador da web:

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

2. Efetue login com as credenciais de administrador das ONTAP tools for 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 backend de armazenamento no menu suspenso para associar a instância do vCenter Server ao backend de armazenamento necessário.

Configurar acesso à rede

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

   Para adicionar vários endereços IP, separe a lista com vírgulas, intervalo, roteamento entre domínios sem classes (CIDR) ou uma combinação dos três.

4. Selecione **Salvar**.

Criar um armazenamento de dados

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

*Interoperabilidade entre datastores nativos com vCenter Server e datastores gerenciados por ferramentas ONTAP *

As ONTAP tools for VMware vSphere 10 criam igroups aninhados para datastores, com igroups pais específicos para datastores e igroups filhos mapeados para os hosts. Você pode criar igroups simples a partir do gerenciador de sistemas ONTAP e usá-los para criar armazenamentos de dados VMFS sem usar ferramentas ONTAP . Consulte "Gerenciar iniciadores SAN e igroups" para maiores informações.

Quando o armazenamento é integrado às ferramentas ONTAP e a descoberta do armazenamento de dados é executada, os igroups simples e os armazenamentos de dados VMFS se tornam gerenciados pelas ferramentas ONTAP e são convertidos em igroups aninhados. Não é possível usar os igroups simples anteriores para criar novos armazenamentos de dados; você deve usar a interface de usuário das ferramentas ONTAP ou a API REST para reutilizar os igroups aninhados.

Criar um armazenamento de dados vVols

Começando com as ONTAP tools for VMware vSphere 10.3, você pode criar um armazenamento de dados vVols em sistemas ASA r2 com eficiência de espaço como thin.vVol. O provedor VASA cria um contêiner e os pontos de extremidade de protocolo desejados ao criar o armazenamento de dados vVol. Este contêiner não terá nenhum volume de apoio.

Antes de começar

- Certifique-se de que os agregados raiz não sejam mapeados para SVM.
- Certifique-se de que o Provedor VASA esteja registrado no vCenter selecionado.
- No sistema de armazenamento ASA r2, o SVM deve ser mapeado para agregar para o usuário do SVM.

Passos

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

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

5. Selecione a VM de armazenamento onde você deseja criar o armazenamento de dados.
6. Em opções avançadas:
   - Se você selecionar a **Política de exportação personalizada**, certifique-se de executar a descoberta no vCenter para todos os objetos. É recomendável que você não use esta opção.
   - Você pode selecionar o nome do **Grupo de iniciadores personalizados** para os protocolos iSCSI e FC.

     No sistema de armazenamento ASA r2 tipo SVM, as unidades de armazenamento (LUN/namespace) não são criadas porque 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 armazenamento de dados vVols .

   Ao criar um novo volume, você pode habilitar o QoS no armazenamento de dados. Por padrão, um volume é criado para cada solicitação criada por LUN. Esta etapa não é aplicável para datastores vVols que usam os sistemas de armazenamento ASA r2.

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

Criar um armazenamento de dados NFS

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

Passos

1. Efetue login no cliente vSphere.
2. Clique com o botão direito do mouse em um sistema host, cluster de host ou data center e selecione * Ferramentas NetApp ONTAP * > **Criar armazenamento de dados**.
3. Selecione NFS no campo **Tipo de armazenamento de dados**.
4. Insira o nome, o tamanho e as informações do protocolo do armazenamento de dados no painel **Nome e protocolo**. Selecione **Cluster de armazenamento de dados** e **Autenticação Kerberos** nas opções avançadas.

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

5. Selecione **Plataforma** e **VM de armazenamento** no painel **Armazenamento**.
6. Se você selecionar **Política de exportação personalizada** nas opções avançadas, execute a descoberta no vCenter para todos os objetos. É recomendável que você não use esta opção.

   > Não é possível 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 somente se desempenho ou capacidade for selecionado no menu suspenso da plataforma.
   - Ao escolher a opção **Qualquer** no menu suspenso da plataforma, você pode ver as 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 **Resumo** e selecione **Concluir**.

O armazenamento de dados NFS é criado e montado em todos os hosts.

Criar um armazenamento de dados VMFS

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

Em um cluster protegido:

- Você pode criar somente datastores VMFS. Quando você adiciona um armazenamento de dados VMFS a um cluster protegido, o armazenamento de dados fica protegido automaticamente.
- Não é possível criar um armazenamento de dados em um data center com um ou mais clusters de hosts protegidos.
- Não é possível criar um armazenamento de dados no host ESXi se o cluster do host pai estiver protegido com um relacionamento do tipo "Política de Failover Duplex Automatizado" (configuração uniforme/não uniforme).
- Você pode criar um armazenamento de dados VMFS somente em um host ESXi protegido por um relacionamento assíncrono. Não é possível criar e montar um armazenamento de dados em um host ESXi que faça parte de um cluster de host protegido pela política "Automated Failover Duplex".

Antes de começar

- Habilite serviços e LIFs para cada protocolo no lado de armazenamento ONTAP .
- Mapear SVM para agregar para usuário SVM no sistema de armazenamento ASA r2.
- Configure o host ESXi se estiver usando o protocolo NVMe/TCP:
  a. Revise o "Guia de compatibilidade do VMware"

  > O VMware vSphere 7.0 U3 e versões posteriores oferecem suporte ao protocolo NVMe/TCP. No entanto, o VMware vSphere 8.0 e versões posteriores são recomendados.

  b. Valide se o fornecedor da placa de interface de rede (NIC) oferece suporte à NIC ESXi com o protocolo NVMe/TCP.
  c. Configure a placa de rede ESXi para NVMe/TCP de acordo com as especificações do fornecedor da placa de rede.
  d. Ao usar a versão VMware vSphere 7, siga as instruções no site da VMware "Configurar a vinculação do VMkernel para o adaptador NVMe sobre TCP" para configurar a vinculação de porta NVMe/TCP. Ao usar a versão VMware vSphere 8, siga "Configurando NVMe sobre TCP no ESXi" , para configurar a ligação da porta NVMe/TCP.
  e. Para a versão VMware vSphere 7, siga as instruções na página "Habilitar adaptadores de software NVMe sobre RDMA ou NVMe sobre TCP" para configurar adaptadores de software NVMe/TCP. Para o lançamento do VMware vSphere 8, siga "Adicionar software NVMe sobre adaptadores RDMA ou NVMe sobre TCP" para configurar os adaptadores de software NVMe/TCP.
  f. Correr"Descubra sistemas de armazenamento e hosts" ação no host ESXi. Para obter mais informações, consulte "Como configurar NVMe/TCP com vSphere 8.0 Update 1 e ONTAP 9.13.1 para datastores VMFS" .
- Se você estiver usando o protocolo NVME/FC, execute as seguintes etapas para configurar o host ESXi:
  a. Se ainda não estiver habilitado, habilite o NVMe sobre Fabrics (NVMe-oF) em seu(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 ONTAP SVM para o protocolo FC, consulte "Configurar um SVM para FC" .

Para obter mais informações sobre o uso do protocolo NVMe/FC com o VMware vSphere 8.0, consulte "Configuração de host NVMe-oF para ESXi 8.x com ONTAP" .

Para obter mais informações sobre o uso de NVMe/FC com VMware vSphere 7.0, consulte "Guia de configuração do host ONTAP NVMe/FC" e "TR-4684" .

Passos

1. Efetue login no cliente vSphere.
2. Clique com o botão direito do mouse em um sistema host, cluster de host ou data center e selecione * Ferramentas NetApp ONTAP * > **Criar armazenamento de dados**.
3. Selecione o tipo de armazenamento de dados VMFS.
4. Insira o nome, o tamanho e as informações de protocolo do armazenamento de dados no painel

Nome e Protocolo. Se você optar por adicionar o novo armazenamento de dados a um cluster de armazenamento de dados VMFS existente, selecione o seletor de cluster de armazenamento de dados em Opções avançadas.

5. Selecione a VM de armazenamento no painel **Armazenamento**. Forneça o **Nome do grupo iniciador personalizado** na seção **Opções avançadas**, conforme necessário. Você pode escolher um igroup existente para o armazenamento de dados ou criar um novo igroup com um nome personalizado.

   Quando o protocolo NVMe/FC ou NVMe/TCP é selecionado, um novo subsistema de namespace é criado e usado para mapeamento de namespace. O subsistema de namespace é criado usando o nome gerado automaticamente que inclui o nome do armazenamento de dados. 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 **Agregar** não é exibida porque o armazenamento ASA r2 é desagregado. Ao escolher um sistema de armazenamento ASA r2 do tipo SVM, a página de atributos de armazenamento mostra as opções para habilitar 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.

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

   c. Selecione o **Nível de serviço de desempenho** para sistemas de armazenamento ASA r2 com SVM de 12 nós que é um cluster heterogêneo. Esta opção não estará disponível se o SVM selecionado for um cluster homogêneo ou usar um usuário SVM.

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

   d. Selecione **Usar volume existente**, **Ativar opções de 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.

   > Não é possível usar o volume existente para criar um armazenamento de dados VMFS com protocolo NVMe/FC ou NVMe/TCP; você deve criar um novo volume.

7. Revise os detalhes do armazenamento de dados no painel **Resumo** e selecione **Concluir**.

   > Se você criar o armazenamento de dados em um cluster protegido, poderá ver uma mensagem somente leitura: "O armazenamento de dados está sendo montado em um cluster protegido".

Resultado

O armazenamento de dados VMFS é criado e montado em todos os hosts.

Proteja datastores e máquinas virtuais

Proteger usando proteção de cluster de host

As ONTAP tools for VMware vSphere gerenciam a proteção de clusters de host. Todos os datastores pertencentes ao SVM selecionado e montados em um ou mais hosts do cluster são protegidos por um cluster de host.

Antes de começar

Certifique-se de que os seguintes pré-requisitos sejam atendidos:

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

Passos

1. Efetue login no cliente vSphere.
2. Clique com o botão direito do mouse em um cluster de host e selecione * Ferramentas NetApp ONTAP * > **Proteger Cluster**.
3. Na janela de proteção do cluster, os detalhes do tipo de armazenamento de dados e da máquina virtual (VM) de armazenamento de origem são preenchidos automaticamente. Selecione o link dos armazenamentos de dados para visualizar os armazenamentos de dados protegidos.
4. Digite o **nome do grupo de consistência**.
5. Selecione **Adicionar Relacionamento**.
6. Na janela **Adicionar relacionamento SnapMirror *, selecione a *VM de armazenamento de destino** e o tipo de **Política**.

   O tipo de política pode ser Assíncrono ou AutomatedFailOverDuplex.

   Ao adicionar o relacionamento SnapMirror como uma política do tipo AutomatedFailOverDuplex, você deve adicionar a VM de armazenamento de destino como backend de armazenamento ao mesmo vCenter onde as ONTAP tools for VMware vSphere estão implantadas.

   No tipo de política AutomatedFailOverDuplex, há configurações de host uniformes e não uniformes. Quando você seleciona o botão de alternância **configuração uniforme do host**, a configuração do grupo iniciador do host é replicada implicitamente no site de destino. Para mais detalhes, consulte"Principais conceitos e termos" .

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

8. Selecione **Adicionar**.
9. Na janela **Proteger cluster**, você não pode editar o cluster protegido durante a operação de criação. 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 os relacionamentos usando as opções do menu de reticências.
10. Selecione o botão **Proteger**.

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

11. Para visualizar os clusters de host protegidos, navegue até * Ferramentas NetApp ONTAP * > * Proteção * > * Relacionamentos de cluster de host *.

Proteja usando proteção SRA

Configurar SRA para proteger armazenamentos de dados

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

Antes de começar

- Você deve ter configurado sua instância do vCenter Server e configurado o host ESXi.
- Você deve ter implantado ONTAP tools for VMware vSphere.
- Você deve ter baixado o adaptador SRA `.tar.gz` arquivo do "Site de suporte da NetApp" .
- Os clusters ONTAP de origem e destino devem ter os mesmos agendamentos SnapMirror personalizados criados antes de executar os fluxos de trabalho SRA.
- "Habilitar ONTAP tools for VMware vSphere" para habilitar a capacidade SRA.

Passos

1. Efetue login na interface de gerenciamento do dispositivo VMware Live Site Recovery usando o URL: `https://:<srm_ip>:5480` e, em seguida, vá para Adaptadores de replicação de armazenamento na interface de gerenciamento do dispositivo VMware VMware Live Site Recovery.
2. Selecione **Novo Adaptador**.
3. Carregue o instalador *.tar.gz* do plug-in SRA no VMware Live Site Recovery.
4. Examine novamente os adaptadores para verificar se os detalhes estão atualizados na página Adaptadores de replicação de armazenamento do VMware Live Site Recovery.

Configurar SRA para ambientes SAN e NAS

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

Configurar SRA para ambientes SAN

Antes de começar

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

- Recuperação de site VMware Live

  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 site protegido.
2. Verifique se os LUNS estão em igroups que têm o `ostype` opção definida como *VMware* no sistema de armazenamento primário.
3. Verifique se os hosts ESXi no site de recuperação têm conectividade iSCSI apropriada com a máquina virtual de armazenamento (SVM). Os hosts ESXi do site secundário devem ter acesso ao armazenamento do site secundário, e os hosts ESXi do site primário devem ter acesso ao armazenamento do site primário.

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

Configurar SRA para ambientes NAS

Antes de começar

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

- Recuperação de site VMware Live

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

Configurar SRA para ambientes altamente escalonados

Você deve configurar os intervalos de tempo limite de armazenamento de acordo com as configurações recomendadas para que o Adaptador de Replicação de Armazenamento (SRA) tenha um desempenho ideal em ambientes altamente escalonados.

Configurações do provedor 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
`StorageProvider.resignatureTimeout`	Aumente o valor da configuração de 900 segundos para 12.000 segundos.
`storageProvider.hostRescanDelaySec`	60
`storageProvider.hostRescanRepeatCnt`	20
`storageProvider.hostRescanTimeoutSec`	Defina um valor alto (por exemplo: 99999)

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

Consulte "Alterar configurações do provedor de armazenamento" para obter mais informações sobre como modificar as configurações do Provedor de Armazenamento.

Configurações de armazenamento

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

> O intervalo de tempo limite especificado é o valor máximo. Você não precisa esperar que o tempo limite máximo seja atingido. A maioria dos comandos termina dentro do intervalo de tempo limite máximo definido.

Consulte "Alterar configurações de armazenamento" para modificar as configurações do Provedor SAN.

Configurar SRA no dispositivo VMware Live Site Recovery

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

Configurar o SRA no dispositivo VMware Live Site Recovery salva as ONTAP tools for VMware vSphere no dispositivo, permitindo a comunicação entre o VMware Live Site Recovery e o SRA.

Antes de começar

- Baixe o arquivo *.tar.gz* do "Site de suporte da NetApp" .
- Habilite serviços SRA no Gerenciador de ferramentas ONTAP . Para obter mais informações, consulte

"Habilitar serviços" seção.

- Adicione servidores vCenter às ferramentas ONTATP para o dispositivo VMware vSphere. Para obter mais informações, consulte "Adicionar servidores vCenter" seção.
- Adicione backends de armazenamento às ONTAP tools for VMware vSphere. Para obter mais informações, consulte "Adicionar backends de armazenamento" seção.

Passos

1. Na tela do dispositivo VMware Live Site Recovery, selecione **Adaptador de replicação de armazenamento** > **Novo adaptador**.
2. Carregue o arquivo *.tar.gz* no VMware Live Site Recovery.
3. Efetue login no dispositivo VMware Live Site Recovery usando uma conta de administrador por meio de um cliente SSH, como o PuTTY.
4. Mude para o usuário root usando o comando: `su root`
5. Execute o comando `cd /var/log/vmware/srm` para navegar até o diretório de log.
6. No local do log, insira o comando para obter o ID do docker usado pelo SRA: `docker ps -l`
7. Para efetuar login no ID do contêiner, digite o comando: `docker exec -it -u srm <container id> sh`
8. Configure o VMware Live Site Recovery com ONTAP tools for VMware vSphere usando o comando: `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`
   - Forneça a senha entre aspas simples para que o script Perl trate caracteres especiais como parte da senha, não como delimitadores.
   - Você pode definir o nome de usuário e a senha do aplicativo (Provedor VASA/SRA) no Gerenciador de ferramentas ONTAP ao habilitar esses serviços pela primeira vez. Use essas credenciais para registrar o SRA com o VMware Live Site Recovery.
   - Para localizar o GUID do vCenter, acesse a página do vCenter Server no Gerenciador de ferramentas ONTAP depois de adicionar sua instância do vCenter. Consulte"Adicionar servidores vCenter" seção.
9. Examine novamente os adaptadores para confirmar se os detalhes atualizados aparecem na página Adaptadores de replicação de armazenamento do VMware Live Site Recovery.

Resultados

Uma mensagem de confirmação é exibida indicando que as credenciais de armazenamento foram salvas. O SRA agora pode se comunicar com o servidor SRA usando o endereço IP, a porta e as credenciais especificados.

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 os passos mencionados no tópico"Configurando SRA no dispositivo VMware Live Site Recovery" .

Passos

1. Execute os seguintes comandos para excluir a pasta da máquina VMware Live Site Recovery armazenada em cache nas ferramentas ONTAP nome de usuário senha:
   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 -l --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv -password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>`Você precisa colocar o valor da senha entre aspas simples.

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

Configurar sites protegidos e de recuperação

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

Ao adicionar um novo repositório de dados, você pode incluí-lo no grupo de repositórios de dados existente ou adicionar um novo repositório de dados e criar um novo volume ou grupo de consistência para proteção. Após adicionar um novo repositório de dados a um grupo de consistência ou volume protegido, atualize o SnapMirror e execute a descoberta de armazenamento nos sites protegido e de recuperação. Você pode executar a descoberta manualmente ou de acordo com uma programação para garantir que o novo repositório de dados seja detectado e protegido.

Emparelhar locais protegidos e de recuperação

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

> O Adaptador de Replicação de Armazenamento (SRA) oferece suporte a fan-out com um relacionamento de sincronização do tipo Automated Failover Duplex e relacionamento assíncrono SnapMirror no grupo de consistência. No entanto, o fan-out com dois SnapMirror assíncronos no grupo de consistência ou fan-out de SnapMirrors no volume não é suportado.

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 **Objetos** > **Ações** > **Emparelhar sites**.

3. Na caixa de diálogo **Emparelhar servidores do Site Recovery Manager**, insira o endereço do Platform Services Controller do site protegido e selecione **Avançar**.
4. Na seção Selecionar vCenter Server, faça o seguinte:
   a. Verifique se o vCenter Server do site protegido aparece como um candidato correspondente ao pareamento.
   b. Insira as credenciais administrativas do SSO e selecione **Concluir**.
5. Se solicitado, selecione **Sim** para aceitar os certificados de segurança.

Resultado

Os sites protegidos e de recuperação aparecerão na caixa de diálogo Objetos.

Configurar grupos de proteção

Antes de começar

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

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

Passos

1. Faça login no vCenter Server e selecione **Site Recovery** > **Grupos de proteção**.
2. No painel **Grupos de proteção**, selecione **Novo**.
3. Especifique um nome e uma descrição para o grupo de proteção, direção e selecione **Avançar**.
4. No campo **Tipo**, selecione a opção **Campo Tipo…** como grupos de armazenamento de dados (replicação baseada em matriz) para armazenamento de dados NFS e VMFS. O domínio de falha nada mais é do que SVMs com replicação habilitada. As SVMs que possuem apenas peering implementado e não apresentam problemas são exibidas.
5. Na guia Grupos de replicação, selecione o par de matrizes habilitado ou os grupos de replicação que têm a máquina virtual que você configurou e selecione **Avançar**.

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

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

Configurar recursos de 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 permitir o mapeamento de cada recurso do site protegido para o recurso apropriado no site de recuperação.

Você deve concluir as seguintes configurações de recursos:

- Mapeamentos de rede
- Mapeamentos de pastas
- Mapeamentos de recursos
- Armazenamentos de dados de espaço reservado

Antes de começar

Você deve ter conectado os sites protegidos e de recuperação.

Passos

1. Faça login 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 **Preparar automaticamente mapeamentos para redes com nomes correspondentes** e selecione **Avançar**.
   b. Selecione os objetos de data center necessários para os sites protegidos e de recuperação e selecione **Adicionar mapeamentos**.
   c. Selecione **Avançar** depois que os mapeamentos forem criados com sucesso.
   d. Selecione o objeto usado anteriormente para criar o mapeamento reverso e selecione **Concluir**.

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. Faça login no vCenter Server e selecione **Site Recovery** > **Sites**.
2. Selecione seu site protegido e selecione **Gerenciar**.
3. Selecione **Mapeamentos de pastas** > ícone **Pasta** na guia Gerenciar para criar um novo mapeamento de pastas.
4. No assistente Criar mapeamento de pasta, faça o seguinte:
   a. Selecione **Preparar automaticamente mapeamentos para pastas com nomes correspondentes** e selecione **Avançar**.
   b. Selecione os objetos de data center necessários para os sites protegidos e de recuperação e selecione **Adicionar mapeamentos**.
   c. Selecione **Avançar** depois que os mapeamentos forem criados com sucesso.

d. Selecione o objeto usado anteriormente para criar o mapeamento reverso e selecione **Concluir**.

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. Faça login 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 **Preparar automaticamente mapeamentos para recursos com nomes correspondentes** e selecione **Avançar**.
   b. Selecione os objetos de data center necessários para os sites protegidos e de recuperação e selecione **Adicionar mapeamentos**.
   c. Selecione **Avançar** depois que os mapeamentos forem criados com sucesso.
   d. Selecione o objeto usado anteriormente para criar o mapeamento reverso e selecione **Concluir**.

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 armazenamentos de dados de espaço reservado

Você deve configurar um repositório de dados de espaço reservado para armazenar um espaço no inventário do vCenter no local de recuperação da máquina virtual (VM) protegida. O repositório de dados de espaço reservado não precisa ser grande, pois as VMs de espaço reservado são pequenas e ocupam apenas algumas centenas de quilobytes ou menos.

Antes de começar

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

Passos

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

> Os armazenamentos de dados de espaço reservado podem ser locais ou remotos e não devem ser replicados.

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

Configurar SRA usando o gerenciador de matriz

Você pode configurar o Adaptador de Replicação de Armazenamento (SRA) usando o assistente do Array Manager do VMware Live Site Recovery para permitir interações entre o VMware Live Site Recovery e as máquinas virtuais de armazenamento (SVMs).

Antes de começar

- Você deve ter pareado os sites protegidos e os sites de recuperação no VMware Live Site Recovery.
- Você deve ter configurado seu armazenamento integrado antes de configurar o gerenciador de matriz.
- Você deve ter configurado e replicado os relacionamentos do SnapMirror entre os sites protegidos e os sites de recuperação.
- Você deve ter habilitado os LIFs de gerenciamento do SVM para habilitar a multilocação.

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

Passos

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

      > Ao configurar o gerenciador de matriz, você deve usar a mesma conexão (endereço IP) para o sistema de armazenamento que foi usada para integrar o sistema de armazenamento nas ONTAP tools for VMware vSphere. Por exemplo, se a configuração do gerenciador de matriz tiver escopo SVM, o armazenamento nas ONTAP tools for VMware vSphere deverá ser adicionado no nível SVM.

   d. Se estiver se conectando a um cluster, especifique o nome da SVM no campo **Nome da SVM** ou

deixe-o em branco para gerenciar todas as SVMs no cluster.

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

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

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

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

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

Por exemplo, se você quiser excluir o volume *src_vol1* que está em um relacionamento SnapMirror com o volume *dst_vol1*, você deve especificar *src_vol1* no campo de site protegido e *dst_vol1* no campo de site de recuperação.

3. Selecione **Avançar**.
4. Verifique se o array foi descoberto e exibido na parte inferior da janela Adicionar Gerenciador de Array e selecione **Concluir**.

Você pode seguir as mesmas etapas para o site de recuperação usando os endereços IP e credenciais de gerenciamento de SVM apropriados. Na tela Habilitar pares de matrizes do assistente Adicionar gerenciador de matrizes, você deve verificar se o par de matrizes correto está selecionado e se ele aparece como pronto para ser habilitado.

Verificar sistemas de armazenamento replicados

Você deve verificar se o site protegido e o site de recuperação estão pareados com sucesso após configurar o Adaptador de Replicação de Armazenamento (SRA). O sistema de armazenamento replicado deve ser detectável tanto pelo site protegido quanto pelo site de recuperação.

Antes de começar

- Você deve ter configurado seu sistema de armazenamento.
- Você deve ter pareado 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. Efetue login no seu vCenter Server.
2. Navegue até **Recuperação de Site** > **Replicação Baseada em Matriz**.
3. Selecione o Par de Matriz necessário e verifique os detalhes correspondentes.

   Os sistemas de armazenamento devem ser descobertos no site protegido e no site de recuperação com o

status “Habilitado”.

Proteção contra dispersão

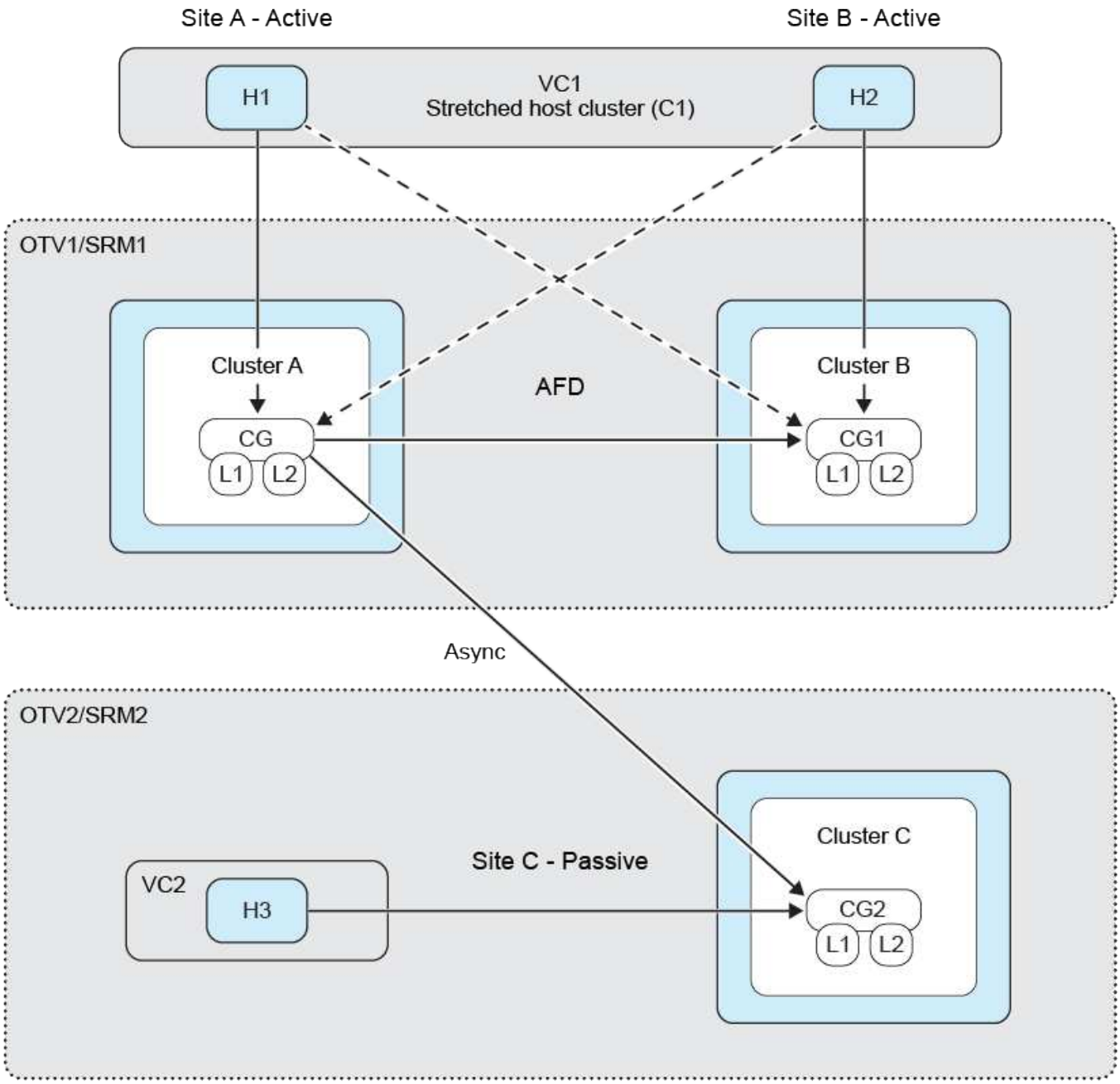
Em uma proteção de fan out, o grupo de consistência é duplamente protegido com relacionamento síncrono no primeiro cluster ONTAP de destino e com relacionamento assíncrono no segundo cluster ONTAP de destino. Os fluxos de trabalho de criação, edição e exclusão da proteção de sincronização ativa do SnapMirror mantêm a proteção síncrona. Os fluxos de trabalho de failover e reproteção do SRM mantêm a proteção assíncrona.

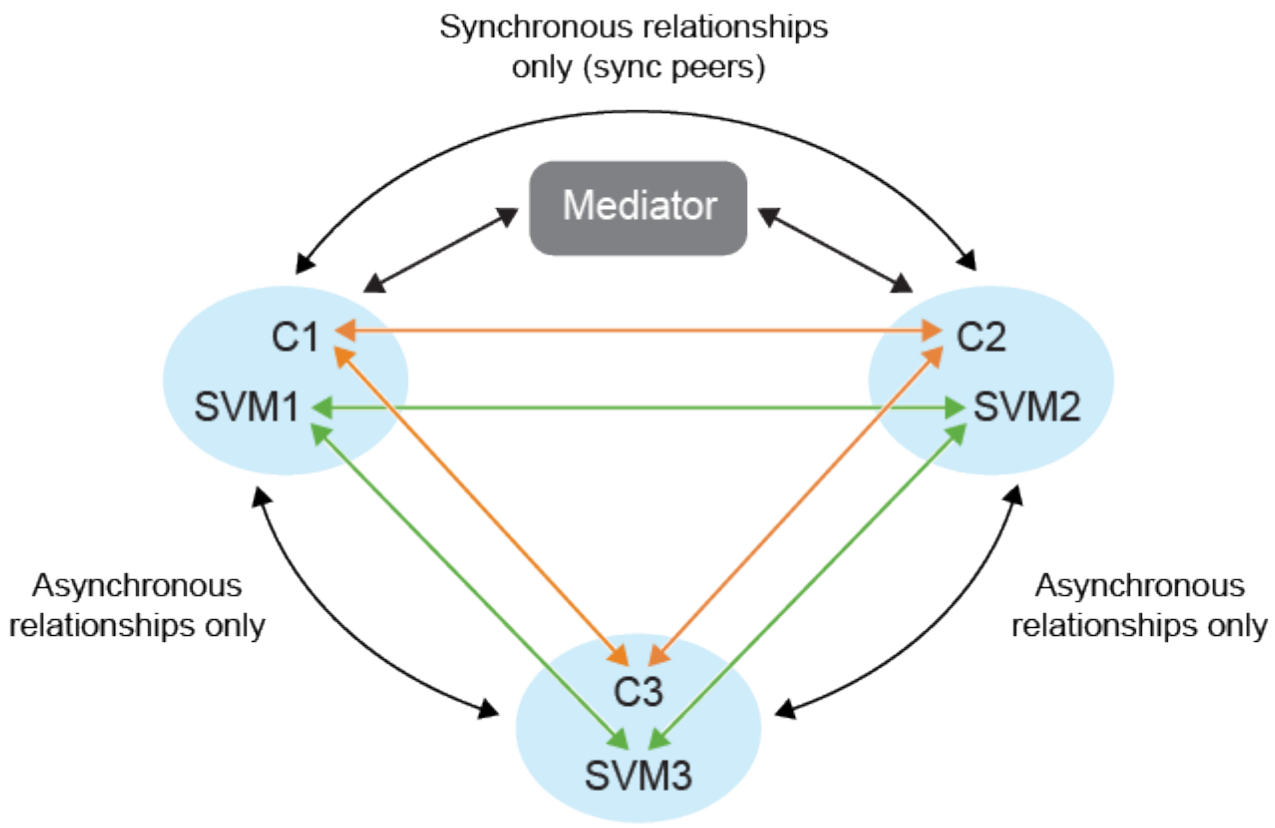
Para estabelecer a proteção de fan out, você precisa conectar três clusters de sites e SVMs.

Exemplo:

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

O diagrama a seguir mostra a configuração da proteção fan out:


Site A - Active
Site B - Active
VC1
Stretched host cluster (C1)
H1
H2
OTV1/SRM1
Cluster A
Cluster B
AFD
CG
CG1
L1
L2
L1
L2
Async
OTV2/SRM2
Cluster C
Site C - Passive
VC2
H3
CG2
L1
L2



Passos

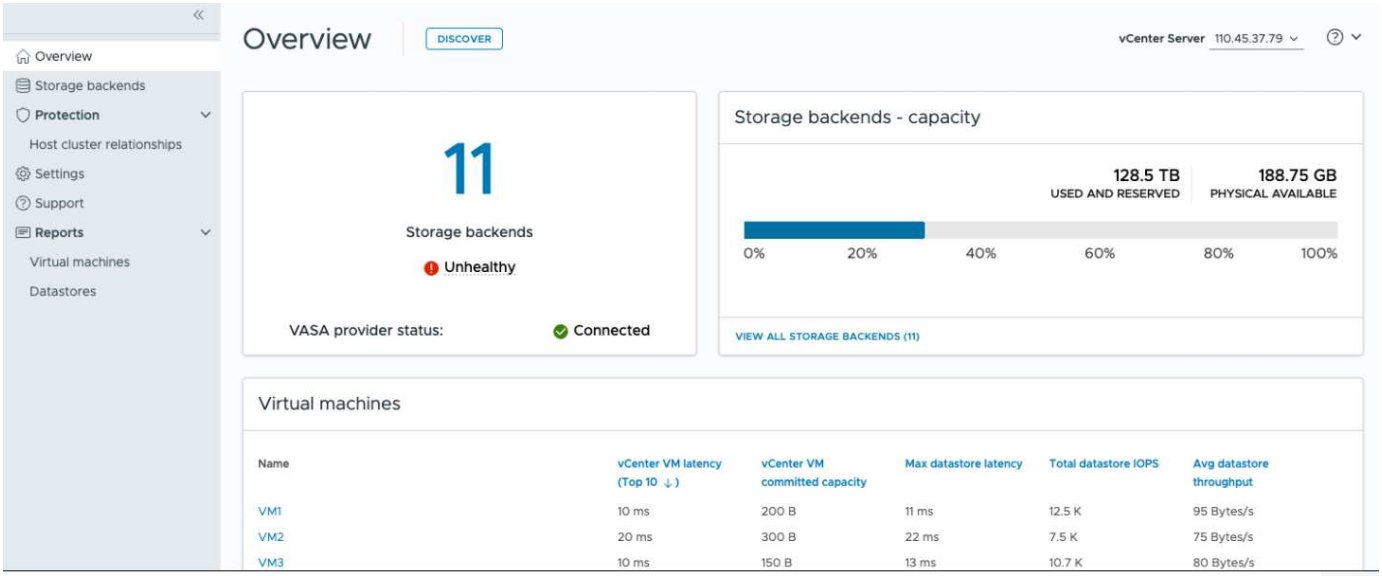
1. Crie um novo repositório de dados de espaço reservado. Referir "Selecione um repositório de dados de espaço reservado"
2. Adicionar armazenamento de dados para hospedar a proteção do cluster"Modificar cluster de host protegido" . Você precisa adicionar tipos de políticas assíncronas e síncronas.

Gerenciar ONTAP tools for VMware vSphere

Visão geral do painel de ONTAP tools for VMware vSphere

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

No caso da configuração do Modo Vinculado Aprimorado (ELM), o menu suspenso de seleção do vCenter Server aparece e você pode selecionar um vCenter Server desejado para ver os dados relevantes a ele. Este menu suspenso está disponível para todas as outras visualizações de listagem do plug-in. A seleção do vCenter Server feita em uma página persiste em todas as guias do plug-in.



Na página de visão geral, você pode executar a ação **Descoberta**. A ação de descoberta executa a descoberta no nível do vCenter para detectar quaisquer backends de armazenamento, hosts, armazenamentos de dados e status/relacionamentos de proteção adicionados ou atualizados recentemente. Você pode executar uma descoberta de entidades sob demanda sem precisar esperar pela descoberta agendada.

> O botão de ação será habilitado somente se você tiver o privilégio de executar a ação de descoberta.

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

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

Cartão	Descrição

Status	O cartão Status mostra o número de backends de armazenamento e o status geral de integridade dos backends de armazenamento e do Provedor VASA. O status dos backends de armazenamento mostra **Íntegro** quando o status de todos os backends de armazenamento é normal e mostra **Não íntegro** se qualquer um dos backends de armazenamento tiver um problema (status Desconhecido/Inacessível/Degradado). Selecione a dica de ferramenta para abrir os detalhes de status dos backends de armazenamento. Você pode selecionar qualquer backend de armazenamento para obter mais detalhes. O link **Outros estados do provedor VASA** mostra o estado atual do provedor VASA registrado no vCenter Server.
Backends de armazenamento - Capacidade	Este cartão mostra a capacidade agregada utilizada e disponível de todos os backends de armazenamento para a instância selecionada do vCenter Server. No caso de sistemas de armazenamento ASA r2, os dados de capacidade não são exibidos por se tratar de um sistema desagregado.
Máquinas virtuais	Este cartão 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, classificadas em ordem crescente ou decrescente. As alterações de classificação e filtragem feitas no cartão persistem até que você altere ou limpe o cache do navegador.
Armazenamentos de dados	Este cartão mostra os 10 principais armazenamentos de dados classificados por uma métrica de desempenho. Você pode selecionar o cabeçalho para obter os 10 principais armazenamentos de dados para a métrica selecionada, classificados em ordem crescente ou decrescente. As alterações de classificação e filtragem feitas no cartão persistem até que você altere ou limpe o cache do navegador. Há um menu suspenso Tipo de armazenamento de dados para selecionar o tipo de armazenamento de dados - NFS, VMFS ou vVols.
Cartão de conformidade do host ESXi	Este cartão mostra o status geral de conformidade de todas as configurações de hosts ESXi (para o vCenter selecionado) com relação às configurações recomendadas do host NetApp por grupo/categoria de configurações. Você pode selecionar o link **Aplicar configurações recomendadas** para aplicar as configurações recomendadas. Você pode selecionar o status de conformidade dos hosts para ver a lista de hosts.

Interface de usuário do gerenciador de ferramentas ONTAP

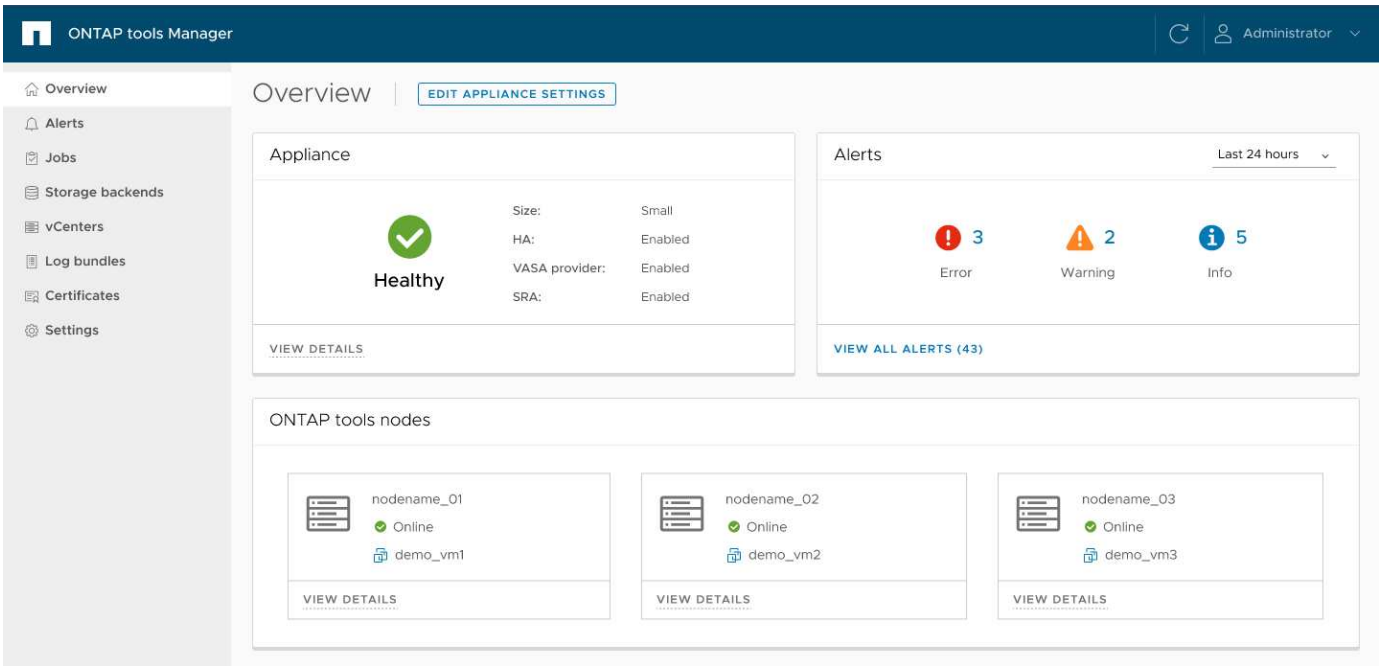
As ONTAP tools for VMware vSphere são um sistema multilocatário que pode gerenciar várias instâncias do vCenter Server. O ONTAP Tools Manager fornece mais controle ao administrador do ONTAP tools for VMware vSphere sobre as instâncias gerenciadas do vCenter Server e os backends de armazenamento integrados.

O Gerenciador de ferramentas ONTAP ajuda em:

- Gerenciamento de instâncias do vCenter Server - Adicione e gerencie instâncias do vCenter Server às ferramentas ONTAP .
- Gerenciamento de backend de armazenamento - Adicione e gerencie clusters de armazenamento ONTAP às ONTAP tools for VMware vSphere e mapeie-os para instâncias integradas do vCenter Server globalmente.
- Downloads de pacotes de log - Colete arquivos de log para ONTAP tools for VMware vSphere.
- Gerenciamento de certificados - Altere o certificado autoassinado para um certificado de CA personalizado e renove ou atualize todos os certificados do VASA Provider e das ferramentas ONTAP .
- Gerenciamento de senhas - Redefina a senha do aplicativo OVA do usuário.

Para acessar o Gerenciador de ferramentas ONTAP , inicie `https://<ONTAPtoolsIP>:8443/virtualization/ui/` no navegador e faça login com as credenciais de administrador das ONTAP tools for VMware vSphere fornecidas durante a implantação.

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



Cartão	Descrição
Cartão de eletrodomésticos	O cartão do dispositivo fornece o status geral do dispositivo ONTAP Tools. Ele mostra os detalhes da configuração do dispositivo e o status dos serviços habilitados. Para obter informações adicionais sobre o dispositivo ONTAP Tools, selecione o link **Exibir detalhes**. Quando uma ação de edição de configuração do dispositivo está em andamento, o portlet do dispositivo mostra o status e os detalhes do trabalho.
Cartão de alertas	O cartão Alertas lista os alertas das ferramentas ONTAP por tipo, incluindo os alertas no nível do nó HA. Você pode visualizar a lista de alertas selecionando o texto de contagem (hiperlink). O link direciona você para a página de visualização de alertas filtrada pelo tipo selecionado.
vCenters	O cartão vCenter mostra o status de integridade dos vCenters no sistema.
Backends de armazenamento	O cartão Backends de armazenamento mostra o status de integridade dos backends de armazenamento no sistema.
Cartão de nós de ferramentas ONTAP	O cartão de nós das ferramentas 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 **Exibir detalhes** para visualizar detalhes adicionais relacionados ao nó selecionado. [NOTA] Em uma configuração não HA, apenas um nó é mostrado. Na configuração do HA, três nós são mostrados.

Entenda igroups e políticas de exportação em ONTAP tools for 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 igroups e mapeá-los para LUNs para controlar quais iniciadores têm acesso aos LUNs.

Nas ONTAP tools for VMware vSphere 9.x, os igroups eram criados e gerenciados em uma estrutura simples, onde cada armazenamento de dados no vCenter era associado a um único igroup. Este modelo limitou a flexibilidade e a reutilização de igroups em vários armazenamentos de dados. As ONTAP tools for VMware vSphere 10.x introduzem igroups aninhados, onde cada armazenamento de dados no vCenter é associado a um igroup pai, enquanto cada host é vinculado a um igroup filho sob esse pai. Você pode definir igroups pai 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 do igroup é essencial para gerenciar LUNs e datastores de forma eficaz nas ONTAP tools for VMware vSphere. Diferentes fluxos de trabalho geram configurações de igroup variadas, conforme 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 por ferramentas ONTAP usam o prefixo “otv_”. Igroups personalizados podem receber qualquer nome.

Prazo	Descrição
DS<número>	Armazenamento de dados
iqn<número>	Iniciador IQN
host<número>	Anfitrião MoRef
lun<número>	ID do LUN
<DSName>Igroup<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:

- Grupo DS1I:
  - 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:

- Grupo DS1I:
  - host1Igroup → (iqn1: lun1)
  - host2Igroup → (iqn2: lun1)

Um igroup filho host2Igroup é criado e adicionado ao igroup pai existente DS1Igroup.

Exemplo 3:

Desmontar um armazenamento de dados de um host

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

Resultado:

- Grupo DS1I:
  - host2Igroup → (iqn2: lun1)

O host1Igroup 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 excluirá o igroup filho.
- Uma tarefa de limpeza agendada remove os igroups filhos pendentes sem mapeamentos de LUN. Esses cenários se aplicam somente a igroups gerenciados por ferramentas ONTAP , não aos criados de forma personalizada.

Exemplo 4:

Excluir armazenamento de dados

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

Resultado:

- Grupo DS1I:
  - host2Igroup → (iqn2: lun1)

Os igroups pai e filho serão removidos se outro armazenamento 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:

- CustomIgroup1:
  - host1Igrupo → (iqn1: lun2, lun3)
  - host2Igroup → (iqn2: lun2)
  - host3Igroup → (iqn3: lun3)

CustomIgroup1 é criado para DS2 e reutilizado para DS3. Os igroups filho 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 porque está 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 é 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 versões do 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) → ClassicIgroup1 (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) → ClassicIgroup1: otv_ClassicIgroup1 (iqn6 e iqn7: lun6, lun7)

Durante a migração:

- Um novo igroup pai (ClassicIgroup1) 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 igroups"

Políticas de exportação

As políticas de exportação controlam o acesso aos armazenamentos de dados NFS nas ONTAP tools for VMware vSphere. Eles definem quais clientes podem acessar os armazenamentos de dados e quais permissões eles têm. As políticas de exportação são criadas e gerenciadas em sistemas ONTAP e podem ser associadas a armazenamentos de dados NFS para impor o controle de acesso. Cada política de exportação consiste em regras que especificam os clientes (endereços IP ou sub-redes) que têm permissão de acesso e as permissões concedidas (somente leitura ou leitura-gravação).

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

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

Quando você exclui ou desmonta um armazenamento de dados NFS de um host ESXi, as ONTAP tools for VMware vSphere removem o endereço IP do host da política de exportação. Se nenhum outro host estiver usando essa política de exportação, ela será excluída. Quando você exclui um armazenamento de dados NFS, as ONTAP tools for VMware vSphere removem a política de exportação associada a esse armazenamento de dados se ela não for reutilizada por nenhum outro armazenamento de dados. Se a política de exportação for reutilizada, ela manterá o endereço IP do host e permanecerá inalterada. Quando você exclui os armazenamentos de dados, a política de exportação cancela a atribuição do 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"

Entenda os igroups gerenciados pelas ferramentas ONTAP

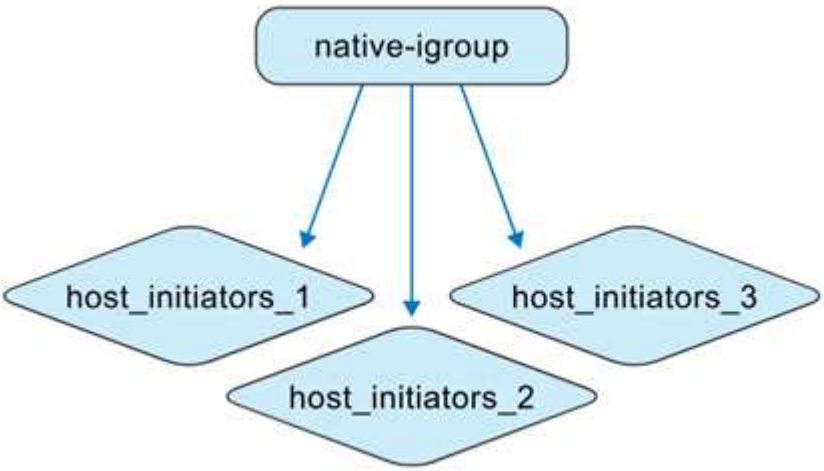
Ao gerenciar VMs de ferramentas ONTAP e sistemas de armazenamento ONTAP , entender o comportamento do igroup é essencial, especialmente ao migrar armazenamentos de dados de ambientes não ONTAP para o gerenciamento de ferramentas ONTAP . Esta seção descreve como os igroups são atualizados durante essa transição.

As ONTAP tools for VMware vSphere 10.4 simplificam o gerenciamento de armazenamento de dados automatizando a criação e a manutenção de objetos ONTAP e vCenter em ambientes de datacenter VMware.

As ONTAP tools for VMware vSphere 10.4 interpretam igroups em dois contextos diferentes:

Ferramentas não ONTAP gerenciam igroups

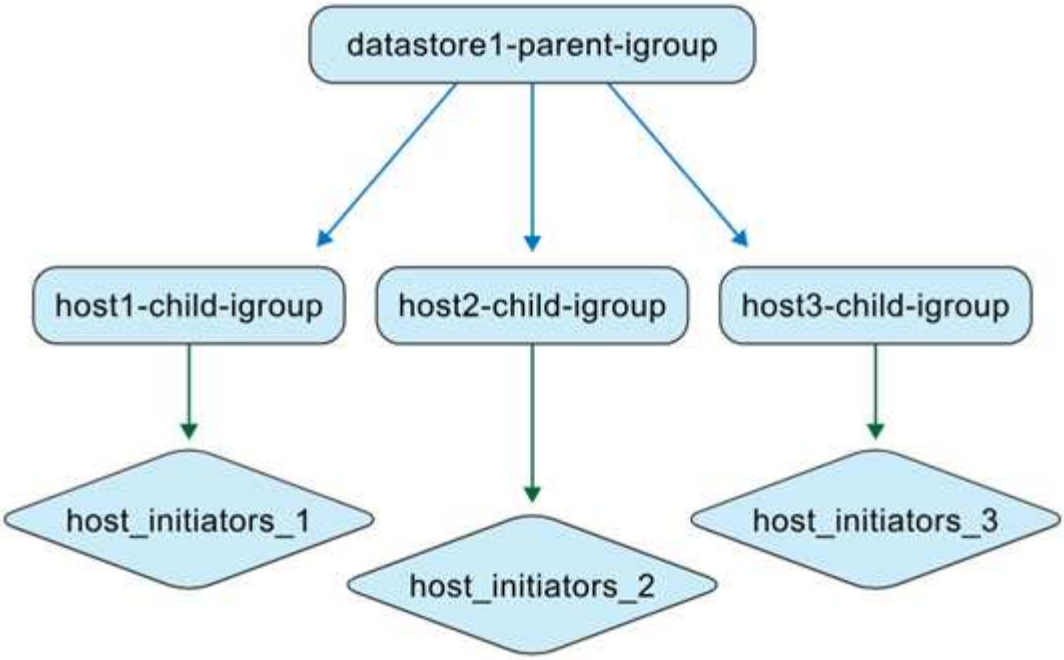
Como administrador de armazenamento, você pode criar igroups no sistema ONTAP como estruturas simples ou aninhadas. A ilustração mostra um igroup plano criado no sistema ONTAP .

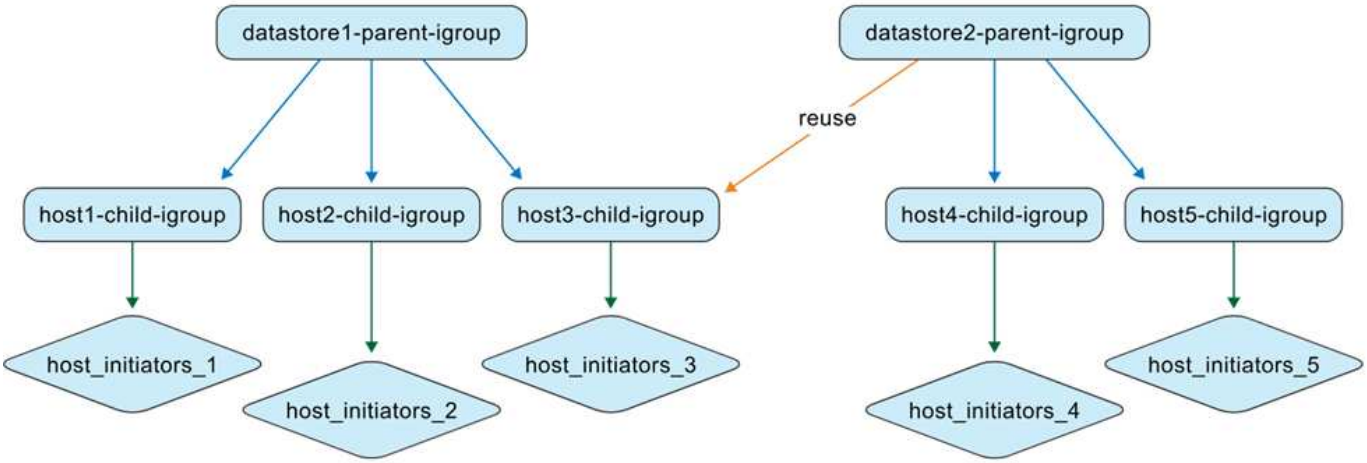


Ferramentas ONTAP gerenciam igroups

Ao criar armazenamentos de dados, as ONTAP tools for VMware vSphere 10.4 criam automaticamente igroups usando uma estrutura aninhada para facilitar o mapeamento de LUN.

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





Aqui estão alguns casos de ONTAP tools for VMware vSphere .

Quando você cria um armazenamento de dados com configurações igroup padrão

Quando você cria um armazenamento de dados e deixa o campo igroup em branco (configuração padrão), as ferramentas ONTAP geram automaticamente uma estrutura de igroup aninhada para esse armazenamento de dados. O igroup pai no nível do armazenamento de dados é nomeado usando o padrão: otv_<vcguid>_<host_parent_datacenterMoref>_<datastore_name>. Cada igroup filho no nível de host segue o padrão: otv_<hostMoref>_<vcguid>. Você pode visualizar a associação entre os igroups pai (nível de armazenamento de dados) e filho (nível de host) na seção **Grupo Iniciador Pai** da interface de armazenamento do ONTAP .

Com a abordagem de igroup aninhado, os LUNs são mapeados apenas para os igroups filhos. O inventário do vCenter Server exibe o novo armazenamento de dados.

Quando você cria um armazenamento de dados com um nome de igroup personalizado

Durante a criação do armazenamento de dados nas ferramentas ONTAP , você pode inserir um nome de

igroup personalizado em vez de selecionar no menu suspenso. As ferramentas ONTAP então criam um igroup pai no nível do armazenamento de dados usando o nome especificado. Se o mesmo host for usado para vários armazenamentos de dados, o igroup (filho) de nível de host existente será reutilizado. Como resultado, o LUN para o novo armazenamento de dados é mapeado para esse igroup filho existente, que agora pode ser associado a vários igroups pais (um para cada armazenamento de dados). A lista de armazenamento de dados da interface do usuário do vCenter Server confirma a criação bem-sucedida do novo armazenamento de dados com o nome do igroup personalizado.

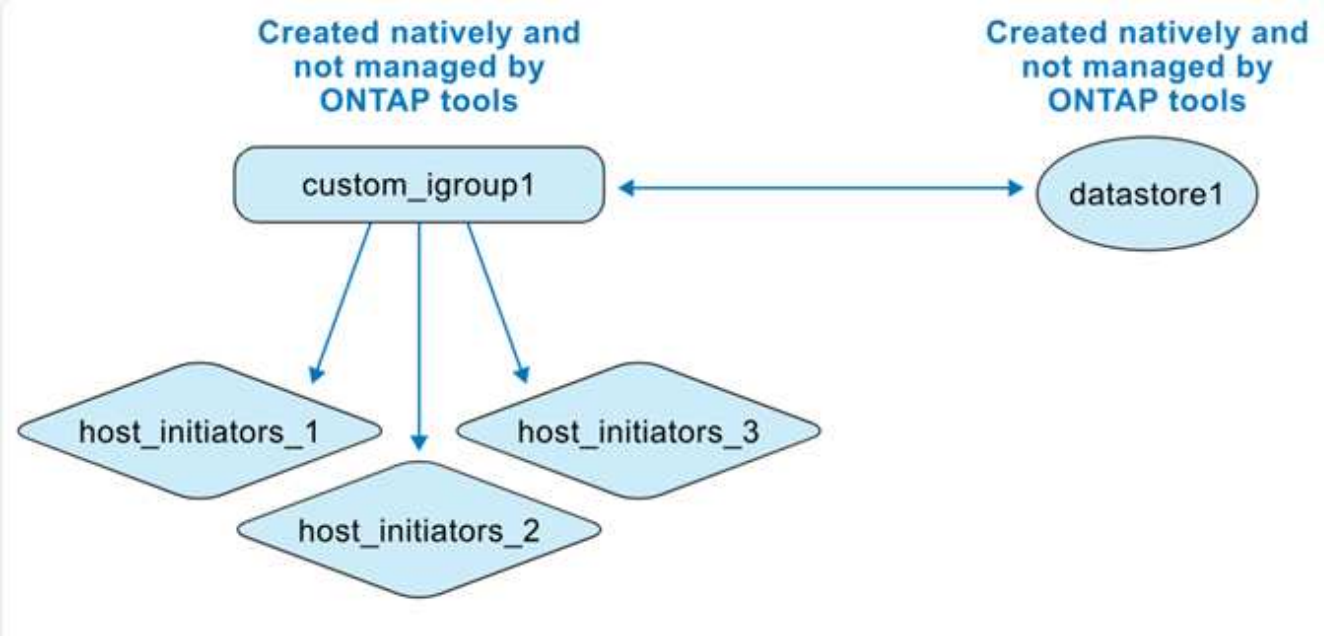
Quando você reutiliza o nome do igroup durante a criação do armazenamento de dados

Ao criar um armazenamento de dados usando a interface de usuário das ferramentas ONTAP , você pode escolher um igroup pai personalizado existente na lista suspensa. Após reutilizar o igroup pai para criar outro armazenamento de dados, a interface do usuário dos sistemas ONTAP mostra esta associação. O novo armazenamento de dados também aparece na interface do usuário do vCenter Server.

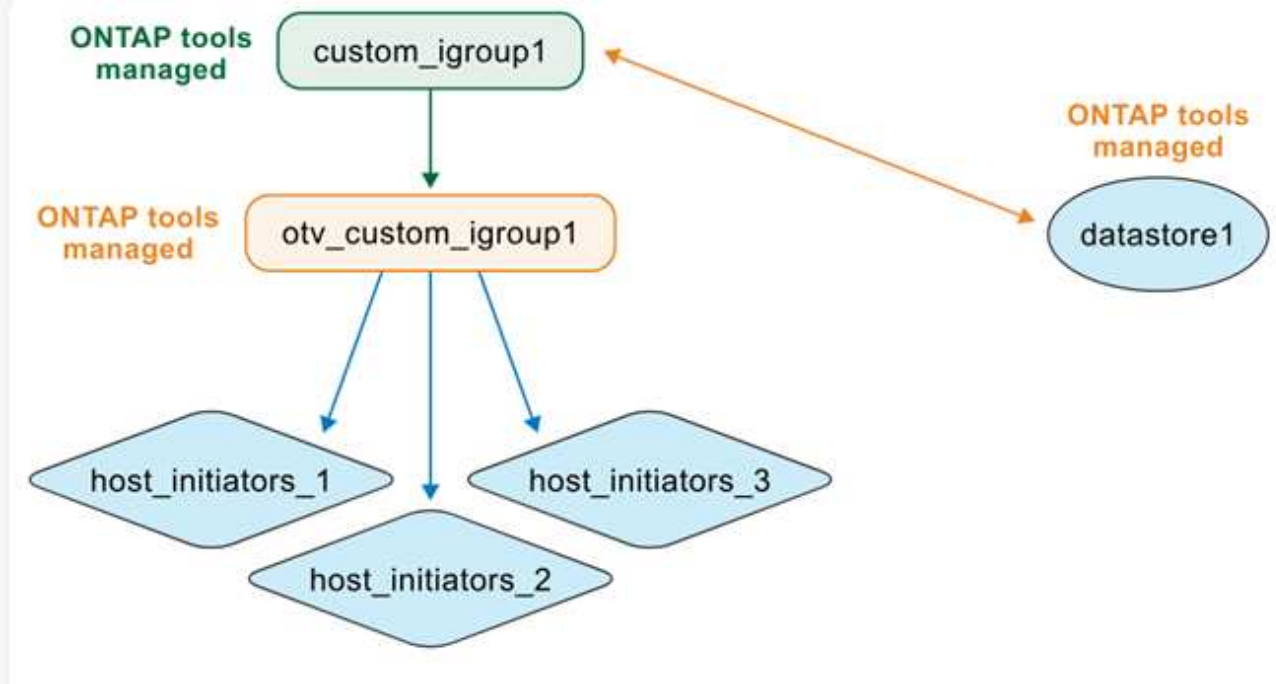
Esta operação também pode ser realizada usando a API. Para reutilizar um igroup existente durante a criação do armazenamento de dados, especifique o UUID do igroup no payload da solicitação da API.

Quando você cria um datastore e um igroup nativamente do ONTAP e do vCenter

Se você criar o igroup e o datastore diretamente em sistemas ONTAP e ambientes VMware, as ferramentas ONTAP não gerenciarão esses objetos inicialmente. Isso cria uma estrutura de igroup plana.



Para gerenciar um armazenamento de dados e um igroup existentes com ferramentas ONTAP , você deve executar uma descoberta de armazenamento de dados. As ferramentas ONTAP identificam e registram o armazenamento de dados e o igroup e os convertem em uma estrutura aninhada em seu banco de dados. Um novo igroup pai é criado usando o nome personalizado, enquanto o igroup existente é renomeado com o prefixo "otv_" e se torna o igroup filho. Os mapeamentos do iniciador permanecem inalterados. Somente igroups mapeados para armazenamentos de dados são convertidos durante a descoberta. Depois disso, a estrutura do igroup fica como na ilustração abaixo.



Você pode criar um armazenamento de dados diretamente no vCenter Server e depois colocá-lo sob o gerenciamento de ferramentas ONTAP . Primeiro, crie um igroup simples em sistemas ONTAP e mapeie um LUN para ele. Após executar a descoberta do armazenamento de dados nas ferramentas ONTAP , o igroup plano é convertido em uma estrutura aninhada. As ferramentas ONTAP então gerenciam o igroup, renomeando-o com o prefixo 'otv_'. O LUN permanece mapeado para o mesmo igroup durante todo esse processo.

Como as ferramentas ONTAP reutilizam igroups criados nativamente

Você pode provisionar um armazenamento de dados em ferramentas ONTAP usando um igroup criado originalmente em sistemas ONTAP , depois que ele for gerenciado por ferramentas ONTAP . Esses igroups aparecem na lista suspensa de nomes de grupos iniciadores personalizados. O novo LUN para o armazenamento de dados é então mapeado para o igroup filho normalizado correspondente, como "otv_NativeIgroup1".

As ONTAP tools for VMware vSphere não detectam nem usam igroups criados no sistema ONTAP que não são gerenciados pelas ferramentas ONTAP ou vinculados a um armazenamento de dados.

Habilitar ONTAP tools for VMware vSphere

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

Passos

1. Inicie o ONTAP Tools Manager em um navegador da web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Efetue login com as credenciais de administrador das ONTAP tools for VMware vSphere fornecidas durante a implantação.
3. Selecione **Editar configurações do aparelho** na seção de visão geral.

4. Na seção **Serviços**, você pode habilitar serviços opcionais como VASA Provider, importação de configuração vVols e recuperação de desastres (SRA) conforme sua necessidade.

   Ao habilitar os serviços pela primeira vez, você deve criar as credenciais do Provedor VASA e do SRA. Eles são usados para registrar ou habilitar os serviços do VASA Provider e do SRA no vCenter Server. O nome de usuário só pode conter letras, números e sublinhados. O comprimento da senha deve ter entre 8 e 256 caracteres.

   > Antes de desabilitar quaisquer serviços opcionais, certifique-se de que os servidores vCenter gerenciados pelas ferramentas ONTAP não os utilizem.

   A opção *Permitir importação de configuração vVols * é exibida somente quando o serviço VASA Provider está habilitado. Esta opção permite a migração de dados vVols do ONTAP Tools 9.xx para o ONTAP Tools 10.4.

Alterar ONTAP tools for VMware vSphere

Usando o Gerenciador de ferramentas ONTAP, dimensione as ONTAP tools for VMware vSphere para aumentar o número de nós na implantação ou altere a configuração para alta disponibilidade (HA). As ONTAP tools for VMware vSphere são implantadas inicialmente em uma configuração de nó único sem alta disponibilidade.

> Para migrar para HA quando o backup não HA estiver habilitado, desabilite o backup primeiro e habilite-o novamente após a migração.

Antes de começar

- Certifique-se de que seu modelo OVA tenha a mesma versão OVA do Nó 1. O nó 1 é o nó padrão onde as ONTAP tools for VMware vSphere OVA são implantadas inicialmente.
- Certifique-se de que o hot add da CPU e o hot plug da memória estejam habilitados.
- No vCenter Server, defina o nível de automação do Serviço de Recuperação de Desastres (DRS) como parcialmente automatizado. Após implantar o HA, reverta-o para totalmente automatizado.
- Os nomes de host dos nós na configuração de HA devem estar em letras minúsculas.

Passos

1. Inicie o ONTAP Tools Manager em um navegador da web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Efetue login com as credenciais de administrador das ONTAP tools for VMware vSphere fornecidas durante a implantação.
3. Selecione **Editar configurações do aparelho** na seção de visão geral.
4. Na seção **Configuração**, você pode aumentar o tamanho do nó e habilitar a configuração de HA conforme suas necessidades. Você precisa das credenciais do vCenter Server para fazer qualquer alteração.

   Quando as ferramentas 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 ONTAP tools for VMware vSphere, você só tem permissão para aumentar o tamanho do nó; não é possível reduzi-lo. Em uma configuração sem HA, somente uma configuração de tamanho médio é suportada. Em uma configuração de HA, configurações médias e grandes são suportadas.

5. Use o botão de alternância HA para habilitar a configuração HA. Na página **Configurações de HA**, certifique-se de que:
   - A biblioteca de conteúdo pertence ao mesmo vCenter Server onde as VMs do nó de ferramentas ONTAP são executadas. As credenciais do vCenter Server são usadas para validar e baixar o modelo OVA para alterações do dispositivo.
   - A máquina virtual que hospeda as ferramentas 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 for habilitada, não será possível reverter para uma configuração de nó único que não seja de HA.

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

   > A maioria das opções de entrada são pré-preenchidas com 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 do endereço IPv6 para os outros dois nós somente quando o endereço IPv6 estiver habilitado 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 avança para a próxima janela.

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

O que vem a seguir?

A página **Visão geral** mostra o status da implantação. Usando o ID do trabalho, você também pode rastrear o status do trabalho de edição das configurações do dispositivo na visualização de trabalhos.

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

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

Gerenciar armazenamentos de dados

Montar datastores NFS e VMFS

A montagem de um armazenamento de dados fornece acesso de armazenamento a hosts adicionais. Você pode montar o armazenamento de dados nos hosts adicionais depois de adicioná-los ao seu ambiente VMware.

Sobre esta tarefa

- Algumas ações de clique com o botão direito do mouse ficam desabilitadas ou indisponíveis dependendo da versão do cliente vSphere e do tipo de armazenamento de dados selecionado.

- Se você estiver usando o cliente vSphere 8.0 ou versões posteriores, algumas das opções de clique com o botão direito estarão ocultas.
- Das versões vSphere 7.0U3 até vSphere 8.0, mesmo que as opções apareçam, a ação será desabilitada.

- A opção de montagem de armazenamento de dados é desabilitada quando o cluster do host é protegido com configurações uniformes.

Passos

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

O que vem a seguir?

Você pode acompanhar o progresso no painel de tarefas recentes.

Desmontar datastores NFS e VMFS

A ação Desmontar armazenamento de dados desmonta um armazenamento de dados NFS ou VMFS de hosts ESXi. A ação Desmontar armazenamento de dados é habilitada para armazenamentos de dados NFS e VMFS que são descobertos ou gerenciados pelas ONTAP tools for VMware vSphere.

Passos

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

   Uma caixa de diálogo é aberta e lista os hosts ESXi nos quais o armazenamento de dados está montado. Quando a operação é realizada em um armazenamento de dados protegido, uma mensagem de aviso é exibida na tela.

3. Selecione um ou mais hosts ESXi para desmontar o armazenamento de dados.

   Não é possível desmontar o armazenamento de dados de todos os hosts. A interface do usuário sugere que você use a operação de exclusão do armazenamento de dados.

4. Selecione o botão **Desmontar**.

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

> Se o armazenamento de dados protegido for desmontado, a configuração de proteção existente poderá resultar em proteção parcial. Consulte "Modificar cluster de host protegido" para permitir proteção completa.

O que vem a seguir?

Você pode acompanhar o progresso no painel de tarefas recentes.

Montar um armazenamento de dados vVols

Você pode montar um armazenamento de dados VMware Virtual Volumes (vVols) em um ou mais hosts adicionais para fornecer acesso de armazenamento 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 e Clusters**.
2. No painel de navegação, selecione o data center que contém o armazenamento de dados.
3. Clique com o botão direito do mouse no armazenamento de dados e selecione * Ferramentas NetApp ONTAP * > **Montar armazenamento de dados**.
4. Na caixa de diálogo **Montar datastores em hosts**, selecione os hosts nos quais você deseja montar o datastore e, em seguida, selecione **Montar**.

Você pode acompanhar o progresso no painel de tarefas recentes.

Redimensionar armazenamento de dados NFS e VMFS

Redimensionar um armazenamento de dados permite aumentar o armazenamento dos arquivos da sua máquina virtual. Você pode alterar o tamanho de um armazenamento de dados conforme seus requisitos de infraestrutura mudam.

Sobre esta tarefa

Você só pode aumentar o tamanho de um armazenamento de dados NFS e VMFS. Um FlexVol volume que faz parte de um armazenamento de dados NFS e VMFS não pode ser reduzido abaixo do tamanho existente, mas pode crescer até 120% no máximo.

Passos

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

Expandir armazenamentos de dados vVols

Ao clicar com o botão direito do mouse no objeto de armazenamento de dados na exibição de objetos do vCenter, as ações suportadas ONTAP tools for VMware vSphere são mostradas na seção de plug-ins. Ações específicas são habilitadas dependendo do tipo de armazenamento de dados e dos privilégios atuais do usuário.

> A operação Expand vVols datastore não é aplicável para datastores vVols baseados no sistema ASA r2.

Passos

1. Na página inicial do vSphere Client, selecione **Hosts e Clusters**.

2. No painel de navegação, selecione o data center que contém o armazenamento de dados.
3. Clique com o botão direito do mouse no armazenamento de dados e selecione * Ferramentas NetApp ONTAP * > **Adicionar armazenamento ao armazenamento de dados**.
4. Na janela **criar ou selecionar volumes**, você pode criar novos volumes ou escolher entre os volumes existentes. A interface do usuário é autoexplicativa. Siga as instruções conforme sua escolha.
5. Na janela **Resumo**, revise as seleções e selecione **Expandir**. Você pode acompanhar o progresso no painel de tarefas recentes.

Reduzir armazenamento de dados vVols

A ação Excluir armazenamento de dados exclui o armazenamento de dados quando não há vVols no armazenamento de dados selecionado.

> A operação de armazenamento de dados vVols Shrink não é suportada para armazenamento de dados vVols baseado no sistema ASA r2.

Passos

1. Na página inicial do vSphere Client, selecione **Hosts e Clusters**.
2. No painel de navegação, selecione o data center que contém o armazenamento de dados.
3. Clique com o botão direito do mouse no armazenamento de dados vVol e selecione * Ferramentas NetApp ONTAP * > * Remover armazenamento do armazenamento de dados *.
4. Selecione volumes que não tenham vVols e selecione **Remover**.

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

5. No pop-up **Remover armazenamento**, marque a caixa de seleção **Excluir volumes do cluster ONTAP * para excluir os volumes do armazenamento de dados e do armazenamento ONTAP e selecione *Excluir**.

Excluir armazenamentos de dados

A ação Remover armazenamento do repositório de dados é suportada em todas as ONTAP tools for VMware vSphere para repositórios de dados vVols descobertos ou gerenciados pelo VMware vSphere no vCenter Server. Esta ação permite a remoção de volumes dos armazenamentos de dados vVols .

A opção de remoção é desabilitada quando há vVols residindo em um volume específico. Além de remover volumes do armazenamento de dados, você pode excluir o volume selecionado no armazenamento ONTAP .

A tarefa de exclusão do armazenamento de dados das ONTAP tools for VMware vSphere no vCenter Server faz o seguinte:

- Desmonta o contêiner vVol.
- Limpa o igroup. Se o igroup não estiver em uso, remove o iqn do igroup.
- Exclui o contêiner Vvol.
- Deixa os volumes Flex no array de armazenamento.

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

Passos

1. Efetue login no cliente vSphere.
2. Clique com o botão direito do mouse em um sistema host, em um cluster de host ou em um data center e selecione * Ferramentas NetApp ONTAP * > * Excluir armazenamento de dados *.

> Você não pode excluir os armazenamentos de dados se houver máquinas virtuais usando esse armazenamento de dados. Você precisa mover as máquinas virtuais para um armazenamento de dados diferente antes de excluí-lo. Não é possível selecionar a caixa de seleção Excluir volume se o armazenamento de dados 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 armazenamento de dados VMFS for criado em sistemas ASA r2 e fizer parte da proteção, você precisará desproteger o armazenamento de dados antes de excluí-lo.
   c. No caso de armazenamentos de dados vVols , a ação de exclusão de armazenamento de dados exclui o armazenamento de dados somente quando não há vVols associados a ele. A caixa de diálogo Excluir armazenamento de dados fornece uma opção para excluir volumes do cluster ONTAP .
   d. No caso de sistemas ASA r2 baseados em datastores vVols , a caixa de seleção para excluir os volumes de suporte não é aplicável.
3. Para excluir os volumes de suporte no armazenamento ONTAP , selecione *Excluir volumes no cluster ONTAP *.

> Não é possível excluir o volume no cluster ONTAP de um armazenamento de dados VMFS que faz parte do cluster de host protegido.

Visualizações de armazenamento ONTAP para repositórios de dados

As ONTAP tools for VMware vSphere mostram a visão lateral do armazenamento ONTAP dos datastores e seus volumes na guia de configuração.

Passos

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

Tipo de armazenamento de dados	Informações disponíveis
Armazenamento de dados NFS	A página **Detalhes de armazenamento** contém backends de armazenamento, agregados e informações de volume. A página **Detalhes do NFS** contém dados relacionados ao armazenamento de dados do NFS.

Armazenamentos de dados VMFS	A página **Detalhes do armazenamento** contém detalhes do backend de armazenamento, agregado, volume e zona de disponibilidade de armazenamento (SAZ). A página **Detalhes da unidade de armazenamento** contém detalhes da unidade de armazenamento.
Armazenamentos de dados vVols	Lista todos os volumes. Você pode expandir ou remover o armazenamento do painel de armazenamento do ONTAP . Esta visualização não é suportada pelo armazenamento de dados vVols baseado no sistema ASA r2.

Visualização de armazenamento da máquina virtual

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

> Esta visualização é aplicável para a VM que tem pelo menos um disco relacionado ao armazenamento de dados vVols gerenciado ONTAP tools for VMware vSphere montado nela.

Passos

1. No vSphere Client, navegue até a máquina virtual.
2. Selecione a aba **Monitor** no painel direito.
3. Selecione * Ferramentas NetApp ONTAP * > **Armazenamento**. Os detalhes de **Armazenamento** 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 colunas diferentes.

Gerenciar limites de armazenamento

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

Passos:

1. Efetue login no cliente vSphere.
2. Na página de atalhos, selecione * Ferramentas NetApp ONTAP * na seção de plug-ins.
3. No painel esquerdo das ferramentas ONTAP , navegue até **Configurações** > **Configurações de limite** > **Editar**.
4. Na janela **Editar Limite**, forneça os valores desejados nos campos **Quase Cheio** e **Cheio** e selecione **Salvar**. Você pode redefinir os números para os 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

Você pode executar a descoberta de um backend de armazenamento sob demanda sem esperar por uma descoberta agendada para atualizar os detalhes do armazenamento.

Siga as etapas abaixo para descobrir os backends de armazenamento.

Passos

1. Efetue login no cliente vSphere.
2. Na página de atalhos, selecione * Ferramentas NetApp ONTAP * na seção de plug-ins.
3. No painel esquerdo das ferramentas ONTAP , navegue até **Backends de armazenamento** e selecione um backend de armazenamento.
4. Selecione o menu de reticências verticais e selecione **Descobrir armazenamento**

Você pode acompanhar o progresso no painel de tarefas recentes.

Modificar backends de armazenamento

Siga as etapas nesta seção para modificar um backend de armazenamento.

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

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

1. Inicie o ONTAP Tools Manager em um navegador da web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Efetue login com as credenciais de administrador das ONTAP tools for VMware vSphere fornecidas durante a implantação.
3. Selecione backends de armazenamento na barra lateral.
4. Selecione o Storage Backend que você deseja modificar.
5. Selecione o menu de elipses verticais e selecione **Modificar**.
6. Você pode modificar as credenciais ou a porta. Digite o **Nome de usuário** e a **Senha** para modificar o backend de armazenamento.

Remover backends de armazenamento

Você precisa excluir todos os armazenamentos de dados anexados ao backend de armazenamento antes de remover o backend de armazenamento. Siga as etapas abaixo para remover um backend de armazenamento.

1. Efetue login no cliente vSphere.
2. Na página de atalhos, selecione * Ferramentas NetApp ONTAP * na seção de plug-ins.
3. No painel esquerdo das ferramentas ONTAP , navegue até **Backends de armazenamento** e selecione

um backend de armazenamento.

4. Selecione o menu de elipses verticais e selecione **Remover**. Certifique-se de que o backend de armazenamento não contenha nenhum armazenamento de dados. Você pode acompanhar o progresso no painel de tarefas recentes.

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

1. Inicie o ONTAP Tools Manager em um navegador da web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Efetue login com as credenciais de administrador das ONTAP tools for VMware vSphere fornecidas durante a implantação.
3. Selecione **Backends de armazenamento** na barra lateral.
4. Selecione o backend de armazenamento que você deseja remover
5. Selecione o menu de elipses verticais e selecione **Remover**.

Visão detalhada do backend de armazenamento

A página de backend de armazenamento lista todos os backends de armazenamento. Você pode executar operações de descoberta, modificação e remoção de armazenamento nos backends de armazenamento que você adicionou e não no SVM filho individual no cluster.

Ao selecionar o cluster pai ou o filho no backend de armazenamento, você pode ver o resumo geral do componente. Ao selecionar o cluster pai, você terá o menu suspenso de ações a partir do qual poderá executar as operações de descoberta de armazenamento, modificação e remoção.

A página de resumo fornece os seguintes detalhes:

- Status do backend de armazenamento
- Informações de capacidade
- Informações básicas sobre a VM
- Informações de rede, como endereço IP e porta da rede. Para o SVM filho, as informações serão as mesmas do backend de armazenamento pai.
- Privileges permitidos e restritos para o backend de armazenamento. Para o SVM filho, as informações serão as mesmas do backend de armazenamento pai. Os Privileges são mostrados apenas nos backends de armazenamento baseados em cluster. Se você adicionar o SVM como backend de armazenamento, as informações de privilégios não serão mostradas.
- A exibição detalhada do cluster do sistema ASA r2 não inclui a guia de camadas locais quando a propriedade desagregada é definida como "true" para o SVM ou o cluster.
- Para sistemas ASA r2 SVM, o portlet de capacidade não é mostrado. O portal de capacidade é necessário somente quando a propriedade desagregada é definida como "true" para o SVM ou o cluster.
- Para sistemas ASA r2 SVM, a seção de informações básicas mostra o tipo de plataforma.

A guia interface fornece informações detalhadas sobre a interface.

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

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.

Desassociar 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 se associar ou desassociar de um backend de armazenamento.

Passos

1. Inicie o ONTAP Tools Manager em um navegador da web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Efetue login com as credenciais de administrador das ONTAP tools for VMware vSphere fornecidas durante a implantação.
3. Selecione a instância necessária do vCenter Server na barra lateral.
4. Selecione as elipses verticais no vCenter Server que você deseja associar ou dissociar dos backends de armazenamento.
5. Selecione **Dissociar backend de armazenamento**.

Modificar uma instância do vCenter Server

Siga as etapas abaixo para modificar instâncias do vCenter Server.

1. Inicie o ONTAP Tools Manager em um navegador da web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Efetue login com as credenciais de administrador das ONTAP tools for VMware vSphere fornecidas durante a implantação.
3. Selecione a instância aplicável do vCenter Server na barra lateral
4. Selecione as elipses verticais no vCenter Server que você deseja modificar e selecione **Modificar**.
5. Modifique os detalhes da instância do vCenter Server e selecione **Modificar**.

Remover uma instância do vCenter Server

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

1. Inicie o ONTAP Tools Manager em um navegador da web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Efetue login com as credenciais de administrador das ONTAP tools for VMware vSphere fornecidas durante a implantação.
3. Selecione as instâncias aplicáveis do vCenter Server na barra lateral
4. Selecione as elipses verticais no vCenter Server que você deseja remover e selecione **Remover**.

> Após remover instâncias do vCenter Server, elas não serão mais mantidas pelo aplicativo.

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

- O plug-in não está registrado.
- Privilégios e funções de plug-in são removidos.

Gerenciar certificados

Um certificado autoassinado é gerado para ferramentas ONTAP e VASA Provider por padrão durante a implantação. Usando a interface do Gerenciador de ferramentas ONTAP , você pode renovar o certificado ou atualizá-lo para uma CA personalizada. Certificados 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 das ferramentas ONTAP .

> Um endereço IP de ferramentas ONTAP deve ser mapeado para um nome de domínio totalmente qualificado (FQDN). Os certificados devem conter o mesmo FQDN mapeado para o endereço IP das ferramentas ONTAP em nomes de assunto ou nomes alternativos de assunto.

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

Atualizar certificado de ferramentas ONTAP

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

Passos

1. Inicie o ONTAP Tools Manager em um navegador da web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Efetue login com as credenciais de administrador das ONTAP tools for VMware vSphere fornecidas durante a implantação.
3. Selecione **Certificados** > **Ferramentas ONTAP * > *Renovar** para renovar os certificados.

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

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

4. Para atualizar o certificado autoassinado para um certificado CA personalizado, selecione a opção **Certificados** > **Ferramentas ONTAP * > *Atualizar para CA**.
   a. Na janela pop-up, carregue o certificado do servidor, a chave privada do certificado do servidor, o certificado da CA raiz e os arquivos de certificado intermediário.
   b. Digite o nome de domínio para o qual você gerou este certificado e atualize o certificado.

   > O sistema ficará offline até que a atualização seja concluída e você será desconectado da interface do ONTAP Tools Manager.

Atualizar certificado de provedor VASA

As ONTAP tools for VMware vSphere são implantadas com um certificado autoassinado para o VASA Provider. Com isso, apenas uma instância do vCenter Server pode ser gerenciada para datastores vVols . Quando você gerencia várias instâncias do vCenter Server e deseja habilitar o recurso vVols nelas, é necessário alterar o certificado autoassinado para um certificado de CA personalizado.

Passos

1. Inicie o ONTAP Tools Manager em um navegador da web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Efetue login com as credenciais de administrador das ONTAP tools for VMware vSphere fornecidas durante a implantação.
3. Selecione **Certificados** > **Provedor VASA** ou **Ferramentas ONTAP * > *Renovar** para renovar os certificados.
4. Selecione **Certificados** > **Provedor VASA** ou **Ferramentas ONTAP * > *Atualizar para CA** para atualizar o certificado autoassinado para um 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 arquivos de certificado intermediário.
   b. Digite o nome de domínio para o qual você gerou este certificado e atualize o certificado.

O sistema ficará offline até que a atualização seja concluída e você será desconectado da interface do ONTAP Tools Manager.

Acesse as ONTAP tools for VMware vSphere

Visão geral das ONTAP tools for VMware vSphere

Você pode gerenciar suas configurações de aplicativo, sistema e rede usando o console de manutenção das ferramentas ONTAP . Você pode alterar sua senha de administrador e senha de manutenção. Você também pode gerar pacotes de suporte, definir diferentes níveis de log, visualizar e gerenciar configurações de TLS e iniciar diagnósticos remotos.

Você deve ter as ferramentas VMware instaladas após implantar as ONTAP tools for VMware vSphere para acessar o console de manutenção. Você deve usar `maint` como o nome de usuário e a senha que você configurou durante a implantação para efetuar login no console de manutenção das ferramentas ONTAP . Você deve usar **nano** para editar os arquivos no console de manutenção ou login root.

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

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

Menu do console	Opções
Configuração do aplicativo	1. Exibir resumo do status do servidor 2. Alterar nível de LOG para serviços de provedor VASA e serviços SRA
Configuração do sistema	1. Reinicializar máquina virtual 2. Desligar máquina virtual 3. Alterar senha do usuário 'maint' 4. Alterar fuso horário 5. Aumentar o tamanho do disco de prisão (/jail) 6. Atualizar 7. Instalar o VMware Tools

Configuração de rede	1. Exibir configurações de endereço IP 2. Exibir configurações de pesquisa de nome de domínio 3. Alterar configurações de pesquisa de nome de domínio 4. Exibir rotas estáticas 5. Alterar rotas estáticas 6. Confirmar alterações 7. Faça ping em um host 8. Restaurar configurações padrão
Suporte e Diagnóstico	1. Acessar shell de diagnóstico 2. Habilitar acesso de diagnóstico remoto 3. Forneça credenciais do vCenter para backup 4. Fazer backup

Configurar acesso de diagnóstico remoto

Você pode configurar ONTAP tools for VMware vSphere para habilitar acesso SSH para o usuário diag.

Antes de começar

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

Sobre esta tarefa

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

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

    A sessão de login permanece válida somente até a meia-noite do dia seguinte.

  - Faça login como usuário diag novamente usando SSH.

Passos

1. No vCenter Server, abra um console para o VASA Provider.
2. Efetue login como usuário de manutenção.
3. Digitar `4` para selecionar Suporte e Diagnóstico.
4. Digitar `2` para selecionar Habilitar acesso de diagnóstico remoto.
5. Digitar `y` na caixa de diálogo Confirmação para habilitar o acesso de diagnóstico remoto.
6. Digite uma senha para acesso de diagnóstico remoto.

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 ser 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 VASA Provider.
2. Efetue login como usuário de manutenção.
3. Digitar `4` para selecionar Suporte e Diagnóstico.
4. Digitar `1` para selecionar Acessar shell de diagnóstico.
5. Digitar `y` para prosseguir.
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 alterou as credenciais do vCenter Server, ONTAP ou Data LIF após a implantação, será necessário atualizar as credenciais usando este procedimento.

Passos

1. No vCenter Server, abra um console para o VASA Provider.
2. Efetue login como usuário de manutenção.
3. Digitar `2` para selecionar o Menu de Configuração do Sistema.
4. Digitar `9` para alterar as credenciais do ONTAP .
5. Digitar `10` para alterar as credenciais do vCenter.

Relatórios de ferramentas ONTAP

O plug-in de ONTAP tools for VMware vSphere fornece relatórios para máquinas virtuais e armazenamentos de dados. Quando você seleciona o ícone do plug-in NetApp ONTAP tools for VMware vSphere na seção de atalhos no cliente vCenter, a interface do usuário navega para a página Visão geral. Selecione a guia Relatórios para visualizar o relatório da máquina virtual e dos armazenamentos de dados.

O relatório de Máquinas virtuais mostra a lista de máquinas virtuais descobertas (devem ter pelo menos um disco de repositórios de dados baseados em armazenamento ONTAP) com métricas de desempenho. Quando você expande o registro da VM, todas as informações do armazenamento de dados relacionadas ao disco são exibidas.

O relatório Datastores mostra a lista de ONTAP tools for VMware vSphere que são provisionados do backend de armazenamento ONTAP de todos os tipos com métricas de desempenho.

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

Coletar os arquivos de log

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

> A geração de logs do Gerenciador de ferramentas ONTAP inclui todos os logs de todas as instâncias do vCenter Server. A geração de logs da interface de usuário do cliente vCenter tem como escopo o vCenter Server selecionado.

Passos

1. Inicie o ONTAP Tools Manager em um navegador da web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Efetue login com as credenciais de administrador das ONTAP tools for VMware vSphere fornecidas durante a implantação.
3. Selecione **Pacotes de Log** na barra lateral.

   Esta operação pode levar vários minutos.

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

   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 de usuário do cliente vCenter:

Passos

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

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

Gerenciar máquinas virtuais

Considerações para migrar ou clonar máquinas virtuais

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

Migrar máquinas virtuais protegidas

Você pode migrar as máquinas virtuais protegidas para:

- Mesmo armazenamento de dados vVols em um host ESXi diferente
- Diferentes armazenamentos de dados vVols compatíveis no mesmo host ESXi
- Diferentes armazenamentos de dados vVols compatíveis 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 com o mesmo armazenamento, o arquivo de metadados do FlexVol volume subjacente não será modificado.

Clonar máquinas virtuais protegidas

Você pode clonar máquinas virtuais protegidas para o seguinte:

- Mesmo contêiner do mesmo FlexVol volume usando grupo de replicação

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

- Mesmo contêiner de um FlexVol volume diferente usando 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.

- Diferentes contêineres ou armazenamento de dados vVols

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

Atualmente, a VMware não oferece suporte a máquinas virtuais clonadas em um modelo de VM.

Há suporte para clone de clone de uma máquina virtual protegida.

Consulte "Criando uma Máquina Virtual para Clonagem" para mais detalhes.

Snapshots de Máquina Virtual

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

Você também não pode proteger máquinas virtuais desprotegidas que tenham instantâneo de memória. Para esta versão, espera-se que você exclua o instantâneo de memória antes de habilitar a proteção para a máquina virtual.

Para VMs do Windows com tipo de armazenamento ASA r2, quando você tira um instantâneo da máquina

virtual, ele será somente leitura. Quando há energia disponível para a VM, o VASA Provider cria um LUN usando o snapshot somente leitura e então o habilita para IOPS. Durante a solicitação de desligamento, o VASA Provider exclui o LUN que foi criado e então desabilita o IOPS.

Migrar máquinas virtuais com datastores NFS e VMFS para datastores vVols

Você pode migrar máquinas virtuais de datastores NFS e VMFS para datastores de Volumes Virtuais (vVols) para aproveitar o gerenciamento de VM baseado em políticas e outros recursos do vVols . Os datastores vVols permitem que você atenda aos maiores requisitos de carga de trabalho.

Antes de começar

Certifique-se de que o VASA Provider não esteja em execução em nenhuma das máquinas virtuais que você planeja migrar. Se você migrar uma máquina virtual que esteja executando o VASA Provider para um armazenamento de dados vVols , não poderá executar nenhuma operação de gerenciamento, incluindo ligar as máquinas virtuais que estão nos armazenamentos de dados vVols .

Sobre esta tarefa

Ao migrar de um armazenamento de dados NFS e VMFS para um armazenamento de dados vVols , o vCenter Server usa APIs do vStorage para descarregamentos de integração de matriz (VAAI) ao mover dados de armazenamentos de dados VMFS, mas não de um arquivo NFS VMDK. Os descarregamentos do VAAI normalmente reduzem a carga no host.

Passos

1. Clique com o botão direito do mouse na máquina virtual que você deseja migrar e selecione **Migrar**.
2. Selecione **Alterar somente armazenamento** e depois selecione **Avançar**.
3. Selecione um formato de disco virtual, uma Política de Armazenamento de VM e um armazenamento de dados vVol que corresponda aos recursos do armazenamento de dados que você está migrando.
4. Revise as configurações e selecione **Concluir**.

Limpeza VASA

Use as etapas desta seção para executar a limpeza do VASA.

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

Passos

1. Cancele o registro do plug-in acessando \ https://OTV_IP:8143/Register.html
2. Verifique se o plug-in não está mais disponível no vCenter Server.
3. Desligue as ONTAP tools for VMware vSphere .
4. Excluir ONTAP tools for VMware vSphere .

Anexar ou desanexar um disco de dados de uma máquina virtual

Anexar um disco de dados a uma máquina virtual

Anexe um disco de dados a uma máquina virtual para expandir a capacidade de armazenamento.

Passos

1. Efetue login no cliente vSphere.
2. Clique com o botão direito do mouse em uma máquina virtual no inventário e selecione **Editar configurações**.
3. Na aba **Hardware Virtual**, selecione **Disco rígido existente**.
4. Selecione a máquina virtual onde o disco está.
5. Selecione o disco que deseja anexar e selecione **OK**

Resultado

O disco rígido aparece na lista de dispositivos de hardware virtual.

Desanexar um disco de dados da máquina virtual

Você pode desanexar um disco de dados conectado a uma máquina virtual quando ele não for mais necessário. Quando você desvincula o disco da máquina virtual, ele não é excluído automaticamente; ele permanece no sistema de armazenamento ONTAP .

Passos

1. Efetue login no cliente vSphere.
2. Clique com o botão direito do mouse em uma máquina virtual no inventário e selecione **Editar configurações**.
3. Mova o ponteiro sobre o disco e selecione **Remover**.

> O disco é removido da máquina virtual. Se outras máquinas virtuais compartilharem o disco, os arquivos do disco não serão excluídos.

Informações relacionadas

"Adicionar um novo disco rígido a uma máquina virtual"

"Adicionar um disco rígido existente a uma máquina virtual"

Descubra sistemas de armazenamento e hosts

Quando você executa as ONTAP tools for VMware vSphere pela primeira vez em um vSphere Client, as ferramentas ONTAP descobrem os hosts ESXi, seus LUNs e exportações NFS, e os sistemas de armazenamento 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 do 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 ONTAP tools for VMware vSphere usam para fazer login nos sistemas de armazenamento.

Ao descobrir os sistemas de armazenamento, as ONTAP tools for VMware vSphere coletam informações dos hosts ESXi gerenciados pela instância do vCenter Server.

Passos

1. Na página inicial do vSphere Client, selecione **Hosts e Clusters**.
2. Clique com o botão direito do mouse no data center desejado e selecione * Ferramentas NetApp ONTAP * > **Atualizar dados do host**.

   Na caixa de diálogo **Confirmar**, confirme 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.

Após a conclusão do processo de descoberta, execute as seguintes ações:

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

Modificar as configurações do host ESXi usando ferramentas ONTAP

Você pode usar o painel de ONTAP tools for 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 de sistemas do host ESXi do painel. Você pode selecionar o problema para visualizar o nome do host ou o endereço IP do host ESXi que apresenta o problema.

Passos

1. Efetue login no cliente vSphere.
2. Na página de atalhos, selecione * Ferramentas NetApp ONTAP * na seção de plug-ins.
3. Acesse o portlet **Conformidade do host ESXi** na Visão geral (painel) do plug-in ONTAP tools for VMware vSphere .
4. Selecione o link **Aplicar configurações recomendadas**.
5. Na janela **Aplicar configurações de host recomendadas**, selecione os hosts que você deseja que estejam em conformidade com as configurações de host recomendadas pela NetApp e selecione

Avançar.

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

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

Informações relacionadas

"Configurar as definições do host ESXi"

Gerenciar senhas

Alterar senha do gerenciador de ferramentas ONTAP

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

Passos

1. Inicie o ONTAP Tools Manager em um navegador da web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Efetue login com as credenciais de administrador das ONTAP tools for 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 de alteração de senha, insira a senha antiga e os detalhes da nova senha. A restrição para alterar a senha é exibida na tela da interface do usuário.
5. Selecione **Alterar** para implementar as alterações.

Redefinir a senha do gerenciador de ferramentas ONTAP

Se você esqueceu a senha do Gerenciador de ferramentas ONTAP , você pode redefinir as credenciais do administrador usando o token gerado pelo console de manutenção das ONTAP tools for VMware vSphere .

Passos

1. Inicie o ONTAP Tools Manager em um navegador da web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Na tela de login, selecione a opção **Redefinir senha**.

   Para redefinir a senha do gerente, você precisa gerar o token de redefinição usando o console de manutenção das ONTAP tools for VMware vSphere .

   a. No vCenter Server, abra o console de manutenção
   b. Digite '2' para selecionar a opção Configuração do Sistema
   c. Digite '3' para alterar a senha do usuário 'maint'.
3. Na janela pop-up de alteração de senha, insira o token de redefinição de senha, o nome de usuário e os detalhes da nova senha.

4. Selecione **Redefinir** para implementar as alterações. Após a redefinição de senha bem-sucedida, você pode usar a nova senha para efetuar login.

Redefinir a senha do usuário do aplicativo

A senha do usuário do aplicativo é usada para registro do provedor SRA e VASA no vCenter Server.

Passos

1. Inicie o ONTAP Tools Manager em um navegador da web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Efetue login com as credenciais de administrador das ONTAP tools for 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 entradas da nova senha.
6. Selecione **Redefinir** para implementar as alterações.

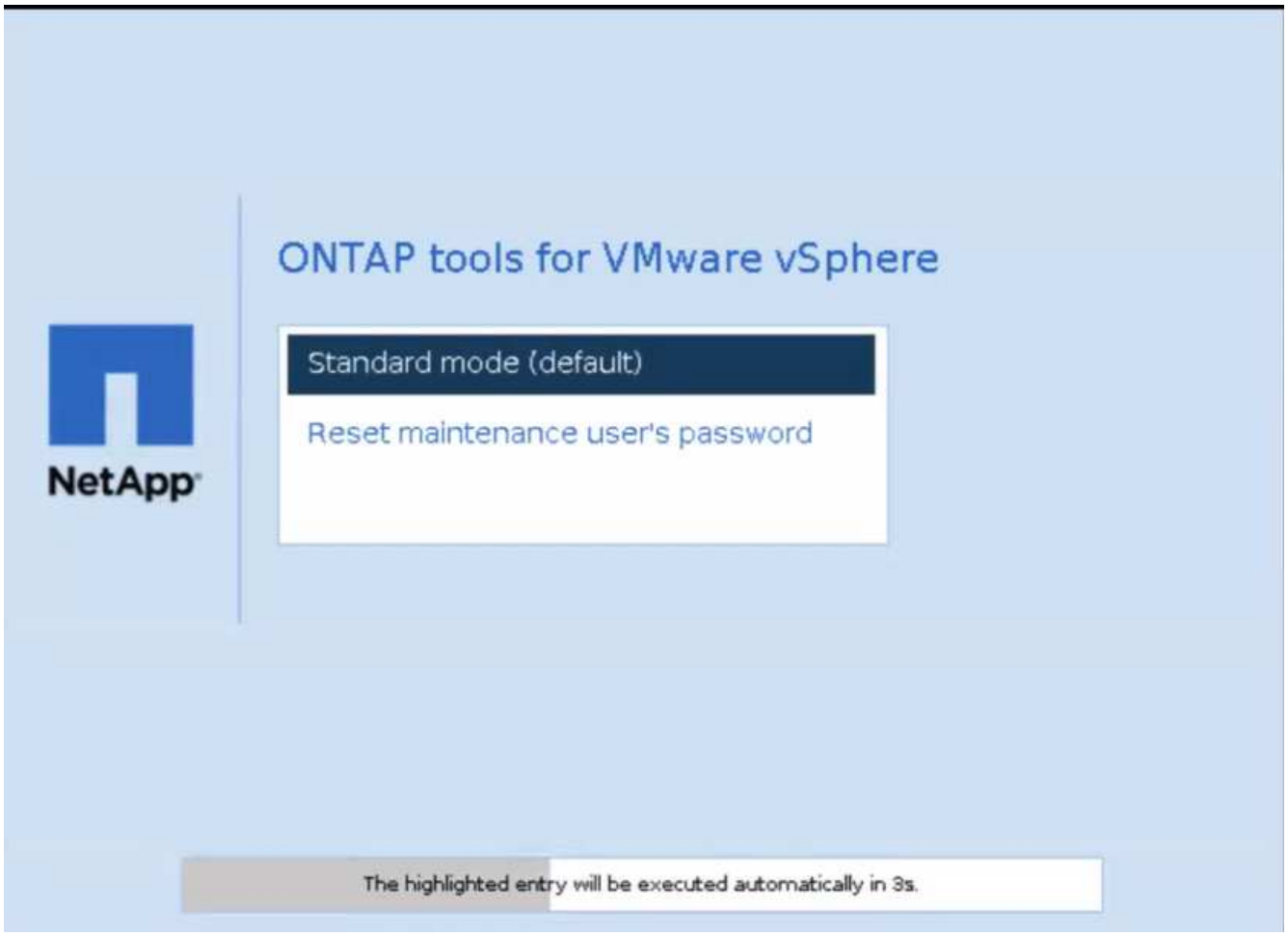
Redefinir a senha do usuário do console de manutenção

Durante a reinicialização do sistema operacional convidado, o menu do GRUB exibe uma opção para redefinir a senha do usuário do console de manutenção. Essa opção é usada para atualizar a senha do usuário do console de manutenção presente na VM correspondente. Após a redefinição da senha, a VM é reiniciada para definir a nova senha. No cenário de implantação de alta disponibilidade, após a reinicialização da VM, a senha é atualizada automaticamente nas outras duas VMs.

> Para ONTAP tools for VMware vSphere HA, você deve alterar a senha do usuário do console de manutenção no primeiro nó, que é node1.

Passos

1. Efetue login no seu vCenter Server
2. Clique com o botão direito do mouse na VM e selecione **Energia** > **Reiniciar sistema operacional convidado**. Durante a reinicialização do sistema, você verá a seguinte tela:



Você tem 5 segundos para escolher sua opção. Pressione qualquer tecla para interromper o progresso e congelar o menu do GRUB.

3. Selecione a opção **Redefinir senha do usuário de manutenção**. O console de manutenção é aberto.
4. No console, insira os detalhes da nova senha. Os detalhes da nova senha e da nova senha devem ser os mesmos para redefinir a senha com sucesso. Você tem três chances para digitar a senha correta. O sistema será reiniciado após a inserção bem-sucedida da nova senha.
5. Pressione Enter para continuar. A senha é atualizada na VM.

> O mesmo menu do GRUB também aparece durante a inicialização da VM. No entanto, você deve usar a opção de redefinição de senha somente com a opção **Reiniciar sistema operacional convidado**.

Gerenciar a proteção do cluster do host

Modificar cluster de host protegido

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

- Adicione novos armazenamentos de dados ou hosts ao cluster protegido.
- Adicione novos relacionamentos SnapMirror às configurações de proteção.

- Exclua relacionamentos SnapMirror existentes das configurações de proteção.
- Modificar um relacionamento SnapMirror existente.

Monitorar a proteção do cluster do host

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

Passos

1. Efetue login no cliente vSphere.
2. Navegue até * Ferramentas NetApp ONTAP * > * Proteção * > * Relacionamentos de cluster de host *.

   O ícone abaixo da coluna de proteção mostra o status da proteção

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

Adicionar novos datastores ou hosts

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

Passos

1. Efetue login no cliente vSphere.
2. Para editar as propriedades de um cluster protegido, você pode
   a. Navegue até * Ferramentas NetApp ONTAP * > * Proteção * > * Relacionamentos de cluster de host *, selecione o menu de reticências no cluster e selecione * Editar * ou
   b. Clique com o botão direito do mouse em um cluster de host e selecione * Ferramentas NetApp ONTAP * > **Proteger Cluster**.
3. Se você criou um armazenamento de dados na interface de usuário nativa do vCenter, esse armazenamento de dados 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 **Proteger** para habilitar a proteção completa.
4. Se você adicionou um novo host ESXi, o status de proteção será exibido como parcialmente protegido. Selecione o menu de reticências nas configurações do SnapMirror e selecione **Editar** para definir a proximidade do host ESXi recém-adicionado.

   > No caso de um relacionamento do tipo assíncrono, a ação de edição não é suportada, pois não é possível adicionar a SVM de destino para o site terciário à mesma instância das ferramentas ONTAP . No entanto, você pode usar o gerenciador de sistema ou a CLI da 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 **Proteger Cluster**.

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

Adicionar um novo relacionamento SnapMirror

Passos

1. Efetue login no cliente vSphere.
2. Para editar as propriedades de um cluster protegido, você pode
   a. Navegue até * Ferramentas NetApp ONTAP * > * Proteção * > * Relacionamentos de cluster de host *, selecione o menu de reticências no cluster e selecione * Editar * ou
   b. Clique com o botão direito do mouse em um cluster de host e selecione * Ferramentas NetApp ONTAP * > **Proteger Cluster**.
3. Selecione **Adicionar relacionamento**.
4. Adicione um novo relacionamento como tipo de política **Assíncrono** ou **AutomatedFailOverDuplex**.
5. Selecione **Proteger**.

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

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

Excluir um relacionamento SnapMirror existente

Para excluir um relacionamento SnapMirror assíncrono, o SVM ou cluster do site secundário deve ser adicionado como backend de armazenamento nas ONTAP tools for VMware vSphere. Você não pode excluir todos os relacionamentos do SnapMirror . Quando você exclui um relacionamento, o respectivo relacionamento no cluster ONTAP também é removido. Quando você exclui um relacionamento AutomatedFailOverDuplex SnapMirror , os armazenamentos de dados no destino não são mapeados e o grupo de consistência, LUNs, volumes e igroups são removidos do cluster ONTAP de destino.

A exclusão do relacionamento aciona uma nova varredura no site secundário para remover o LUN não mapeado como caminho ativo dos hosts.

Passos

1. Efetue login no cliente vSphere.
2. Para editar as propriedades de um cluster protegido, você pode
   a. Navegue até * Ferramentas NetApp ONTAP * > * Proteção * > * Relacionamentos de cluster de host *, selecione o menu de reticências no cluster e selecione * Editar * ou
   b. Clique com o botão direito do mouse em um cluster de host e selecione * Ferramentas NetApp ONTAP * > **Proteger Cluster**.
3. Selecione o menu de reticências nas configurações do SnapMirror e selecione **Excluir**.

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

Modificar um relacionamento SnapMirror existente

Para modificar um relacionamento SnapMirror assíncrono, o SVM ou cluster do site secundário deve ser adicionado como backend de armazenamento nas ONTAP tools for VMware vSphere. Se for um relacionamento AutomatedFailOverDuplex SnapMirror , você pode modificar a proximidade do host em caso de configuração uniforme e o acesso ao host em caso de configuração não uniforme. Não é possível trocar os tipos de política Asynchronous e AutomatedFailOverDuplex. Você pode definir a proximidade ou o acesso para os hosts recém-descobertos no cluster.

Não é possível editar um relacionamento SnapMirror assíncrono existente.

Passos

1. Efetue login no cliente vSphere.
2. Para editar as propriedades de um cluster protegido, você pode
   a. Navegue até * Ferramentas NetApp ONTAP * > * Proteção * > * Relacionamentos de cluster de host *, selecione o menu de reticências no cluster e selecione * Editar * ou
   b. Clique com o botão direito do mouse em um cluster de host e selecione * Ferramentas NetApp ONTAP * > **Proteger Cluster**.
3. Se o tipo de política AutomatedFailOverDuplex for selecionado, adicione detalhes de proximidade ou acesso ao host.
4. Selecione o botão **Proteger**.

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

Remover proteção do cluster do host

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

Passos

1. Para visualizar os clusters de host protegidos, navegue até * Ferramentas NetApp ONTAP * > * Proteção * > * Relacionamentos de cluster de host *.

   Nesta página, você pode monitorar os clusters de hosts protegidos juntamente com seu estado de proteção, relacionamento com o SnapMirror e seu status correspondente do SnapMirror .

2. Na janela **Proteção do cluster do host**, selecione o menu de reticências ao lado do cluster e, em seguida, selecione **Remover proteção**.

Desativar AutoSupport

Ao configurar seu sistema de armazenamento pela primeira vez, o AutoSupport é habilitado por padrão. Ele envia mensagens ao suporte técnico 24 horas após ser ativado. Ao desabilitar o AutoSupport, você não receberá mais suporte e monitoramento proativos.

É recomendável que você mantenha o AutoSupport ativado. Ajuda a acelerar a detecção e a resolução de problemas. O sistema coleta informações do AutoSupport e as armazena localmente, mesmo quando desativado. No entanto, ele não envia o relatório para nenhuma rede.

Passos

1. Inicie o ONTAP Tools Manager em um navegador da web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Efetue login com as credenciais de administrador das ONTAP tools for VMware vSphere fornecidas durante a implantação.

3. Selecione a opção **Configurações** > **Telemetria** > **Editar**.
4. Desmarque a opção * AutoSupport* e salve as alterações.

Atualizar URL do AutoSupport do AutoSupport

Atualize o URL do proxy do 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 pelo proxy apropriado, permitindo transmissão segura e conformidade.

Passos

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

   Se você desabilitar o AutoSupport, o URL do proxy também será desabilitado.

Adicionar servidores NTP

Insira os detalhes do servidor NTP para sincronizar os relógios de ponto do dispositivo ONTAP Tools.

Passos

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

   Atualize a tela para ver os valores atualizados.

Crie um backup e recupere a configuração das ferramentas ONTAP

A partir das ONTAP tools for VMware vSphere 10.3, o dispositivo usa provisionamento de armazenamento dinâmico, não sendo possível atingir RPO zero. No entanto, você pode atingir um RPO quase zero. Para atingir um RPO próximo de zero, você precisa criar um backup da configuração e restaurá-lo em uma nova máquina virtual.

Para migrar para HA quando o backup não HA estiver habilitado, desabilite o backup primeiro e habilite-o novamente após a migração.

Crie um backup e baixe o arquivo de backup

Passos

1. No vCenter Server, abra o console de manutenção.
2. Efetue login como usuário de manutenção.
3. Digitar `4` para selecionar **Suporte e Diagnóstico**.
4. Digitar `3` para selecionar a opção **Habilitar backup do sistema**.
5. Em caso de não HA, insira as credenciais do vCenter onde a máquina virtual das ferramentas ONTAP está implantada.
6. Insira o valor da frequência de backup entre 5 e 60 minutos.
7. Pressione **Enter**

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

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

   Na seção de arquivo, você pode ver o diretório. O nome do diretório será o endereço IP das ferramentas ONTAP , onde os pontos (.) serão substituídos por sublinhados, sufixados com *backup*.

10. Para obter mais informações sobre backup, baixe o arquivo backup_info.txt em **Arquivos** > **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 para a nova máquina virtual e a configuração do sistema, como serviços habilitados, tamanho do nó e modo HA, deve ser a mesma da implantação inicial.

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

1. No vCenter Server, abra o console de manutenção.
2. Efetue login como usuário de manutenção.
3. Digitar `4` para selecionar **Suporte e Diagnóstico**.
4. Digitar `2` para selecionar a opção **Habilitar acesso remoto ao diagnóstico** e criar uma nova senha para o acesso ao diagnóstico.
5. Selecione qualquer backup do diretório baixado. O nome do arquivo de backup mais recente é registrado 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. Após o arquivo de backup ser copiado, faça login no shell de diagnóstico e execute o seguinte comando:

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

   Os logs são registrados no arquivo */var/log/post-deploy-upgrade.log*.

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

Desinstalar ONTAP tools for VMware vSphere

Desinstalar as ONTAP tools for VMware vSphere exclui todos os dados nas ferramentas.

Passos

1. Remova ou mova todas as máquinas virtuais das ONTAP tools for VMware vSphere .
   - Para remover as máquinas virtuais, consulte "Remover e registrar novamente VMs e modelos de VM"
   - Para movê-los para um armazenamento de dados não gerenciado, consulte "Como migrar sua máquina virtual com o Storage vMotion"
2. "Excluir armazenamentos de dados"criado em ONTAP tools for VMware vSphere.
3. Se você habilitou o provedor VASA, selecione **Configurações** > **Configurações do provedor VASA** > **Cancelar registro** nas ferramentas 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. Consulte "Desassociar backends de armazenamento com a instância do vCenter Server" .
5. Excluir todos os backends de armazenamento. Consulte "Gerenciar backends de armazenamento" .
6. Remova o adaptador SRA do VMware Live Site Recovery:
   a. Efetue login como administrador na interface de gerenciamento do dispositivo VMware Live Site Recovery 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 que você sabe os resultados da exclusão do adaptador e selecione **Excluir**.
7. Exclua as instâncias do servidor vCenter integradas às ONTAP tools for VMware vSphere. Consulte "Gerenciar instâncias do vCenter Server" .
8. Desligue as ONTAP tools for 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 ONTAP para implantação do VMware, ele cria muitos volumes FlexVol não utilizados. Após remover as ONTAP tools for VMware vSphere, você deve remover os volumes FlexVol para evitar possíveis impactos no desempenho.

Passos

1. Determine as ONTAP tools for VMware vSphere a partir da primeira VM do nó.

   cat /opt/netapp/meta/ansible_vars.yaml | grep -i protocolo

   Se for uma implantação iSCSI, você também precisará excluir os igroups.

2. Obtenha a lista de volumes do FlexVol .

   kubectl descreve volumes persistentes | grep nomeInterno | awk -F=' '{print $2}'

3. Remova as VMs do vCenter Server. Consulte "Remover e registrar novamente VMs e modelos de VM" .
4. Excluir volumes FlexVol . Consulte "Excluir um FlexVol volume" . No comando CLI para excluir um volume, forneça o nome exato dos volumes FlexVol .
5. Exclua igroups SAN do sistema de armazenamento ONTAP em caso de implantação iSCSI. Consulte "Visualizar e gerenciar iniciadores SAN e igroups" .

Atualizar ONTAP tools for VMware vSphere

Atualização das ONTAP tools for VMware vSphere 10.x para 10.4

Você pode atualizar as ONTAP tools for VMware vSphere 10.2 ou 10.3 para 10.4. No entanto, a atualização direta das ferramentas ONTAP 10.0 ou 10.1 para 10.4 não é suportada.

OBSERVAÇÃO:

- Em sistemas ASA r2, você deve atualizar para as ONTAP tools for VMware vSphere 10.4 com ONTAP 9.16.1 antes de adicionar mais zonas de disponibilidade de armazenamento (SAZs).
- Se a atualização das ONTAP tools for VMware vSphere 10.2 ou 10.3 para a versão 10.4 falhar, a reversão não será suportada. Para recuperar a configuração, use o RPO para ONTAP tools for VMware vSphere 10.2 e o RPO quase zero ou a recuperação de instantâneo para ONTAP tools for VMware vSphere 10.3.

Antes de começar

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

Se você estiver atualizando a partir das ONTAP tools for VMware vSphere 10.2 ou 10.3, precisará concluir as seguintes etapas antes de prosseguir com a tarefa de atualização: * 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 a sua implantação. Habilite o plugin ativo para CPU e RAM.

+

Tipo de implantação	CPU(núcleo) por nó	Memória (GB) por nó	Espaço em disco (GB) por nó	CPU total (núcleo)	Memória (GB)	Espaço total em disco (GB)
Pequeno não HA	9	18	350	9	18	350
Meio sem HA	13	26	350	13	26	350
HA Pequeno	9	18	350	27	54	1050
HA Médio	13	26	350	39	78	1050
HA Grande	17	34	350	51	102	1050

- Ligue a VM após as alterações serem feitas e aguarde até que os serviços entrem em estado de execução.
- No caso de implantação de HA, faça as alterações de recursos, habilite o plugin ativo para CPU e RAM e adicione discos rígidos de 100 GB para o segundo e o terceiro nó também. Não há necessidade de reinicializar esses nós.
- Se o dispositivo foi implantado como um caminho local (implantação fácil) com as ferramentas ONTAP 10.2, você precisa fazer um snapshot de inatividade antes de atualizar.

Se você estiver atualizando das ONTAP tools for VMware vSphere 10.0 para 10.1, precisará concluir as

seguintes etapas antes de prosseguir com a tarefa de atualização: **Habilitar diagnóstico**

1. No vCenter Server, abra um console para ferramentas ONTAP .
2. Efetue login como usuário de manutenção.
3. Digite **4** para selecionar **Suporte e Diagnóstico**.
4. Digite **2** para selecionar **Ativar acesso de diagnóstico remoto**.
5. Digite **y** para definir a senha de sua escolha.
6. Efetue login no endereço IP da VM a partir do terminal/putty com o usuário 'diag' e a senha que foi 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 de kubectl -n ntv-system.
- Execute o comando *env | grep MONGODB_ROOT_PASSWORD* dentro do pod.
- Execute o comando *exit* para sair do pod.
- Execute o comando *kn exec ntv-mongodb-0 --mongodump -u root -p MONGODB_ROOT_PASSWORD --archive=/tmp/mongodb-backup.gz --gzip* 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.

Tire uma foto instantânea de todos os volumes

- Execute o comando 'kn get pvc' e salve a saída do comando.
- Faça snapshots de todos os volumes, um por 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 do usuário do ONTAP System Manager, pesquise o volume pelo nome na barra de pesquisa e abra o volume selecionando o nome. Vá para o snapshot e adicione o snapshot desse volume.

Faça o snapshot das ONTAP tools for VMware vSphere no vCenter (3 VMs no caso de implantação de alta disponibilidade, 1 VM no caso de implantação sem alta disponibilidade)

- Na interface de usuário do cliente vSphere, selecione a VM.
- Vá para a aba de instantâneos e selecione o botão **Tirar instantâneo**. Tire um instantâneo inativo da VM. Consulte "Faça um instantâneo de uma máquina virtual" para mais detalhes.

Antes de executar a atualização, exclua os pods concluídos do pacote de log com o prefixo “generate-support-bundle-job”. Se a geração do pacote de suporte estiver em andamento, aguarde sua conclusão 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 HDD, execute a seguinte tarefa.

1. Selecione a VM na configuração de nó único ou todas as três VMs na configuração HA.
2. Clique com o botão direito do mouse na(s) VM(s) e selecione **Adicionar novo dispositivo** > **Disco rígido**

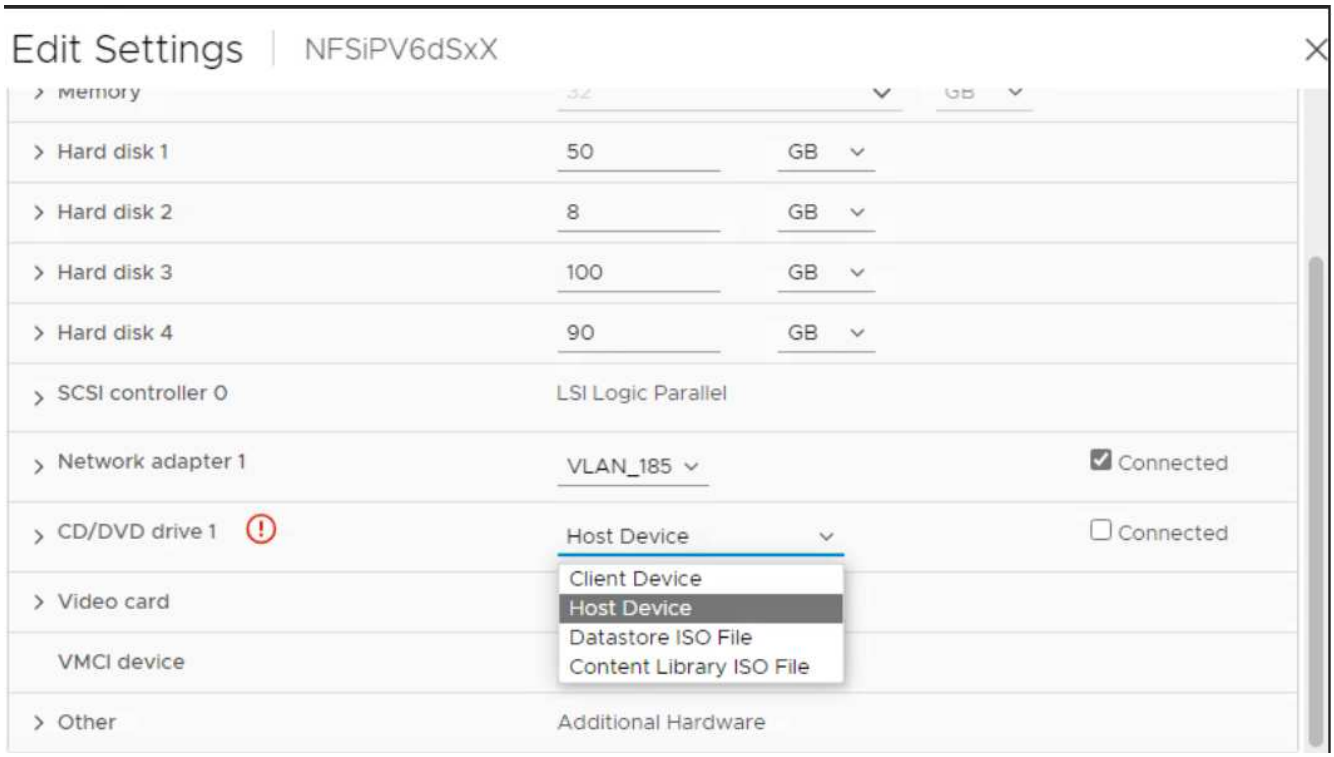
3. Adicione um HDD de 100 GB no campo **Novo disco rígido**.
4. Selecione **Aplicar**

Após adicionar o disco rígido, atualize os recursos da VM para as respectivas configurações e reinicie a VM primária.

Um novo HDD será criado. O provisionador de armazenamento dinâmico usa este HDD para gerar ou replicar os volumes.

Passos

1. Carregue ONTAP tools for VMware vSphere para biblioteca de conteúdo.
2. Na página principal da VM, selecione **Ações** > **Editar configurações**
3. Selecione o arquivo ISO da biblioteca de conteúdo na janela de edição de configurações no campo **Unidade de CD/DVD**.
4. Selecione o arquivo ISO e selecione **OK**. Selecione a caixa de seleção conectada no campo **Unidade de CD/DVD**.



5. No vCenter Server, abra um console para ferramentas ONTAP .
6. Efetue login como usuário de manutenção.
7. Digite **3** para selecionar o menu Configuração do Sistema.
8. Digite **7** para selecionar a opção de atualização.
9. Ao atualizar, as seguintes ações são executadas automaticamente:
   a. Atualização de certificado
   b. Atualização remota do plug-in

Após atualizar para as ONTAP tools for VMware vSphere 10.4, você pode:

- Desabilitar os serviços da interface do usuário do gerenciador

- Migrar de uma configuração sem HA para uma configuração com HA
- Aumente a escala de uma configuração pequena não HA para uma configuração média não HA ou para uma configuração média ou grande HA.
- No caso de uma atualização não HA, reinicie a VM das ferramentas ONTAP para refletir as alterações. No caso de uma atualização de HA, reinicie o primeiro nó para refletir as alterações no nó.

O que vem a seguir

Após atualizar as versões anteriores das ONTAP tools for VMware vSphere para 10.4, verifique novamente os adaptadores SRA para verificar se os detalhes estão atualizados na página Adaptadores de replicação de armazenamento do VMware Live Site Recovery.

Após a atualização bem-sucedida, exclua os volumes Trident do ONTAP manualmente usando o seguinte procedimento:

> Essas etapas não serão necessárias se as ONTAP tools for VMware vSphere 10.1 ou 10.2 estiverem em configurações pequenas ou médias (caminho local) não HA.

1. No vCenter Server, abra um console para ferramentas ONTAP .
2. Efetue login como usuário de manutenção.
3. Digite **4** para selecionar o menu **Suporte e Diagnóstico**.
4. Digite **1** para selecionar a opção **Access diagnostics shell**.
5. Execute o seguinte comando

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

6. Digite o nome de usuário e a senha do ONTAP

Isso exclui todos os volumes Trident no ONTAP usados nas ONTAP tools for VMware vSphere 10.1/10.2.

Informações relacionadas

"Migrar das ONTAP tools for VMware vSphere 9.xx para 10.4"

Códigos de erro de atualização

Você pode encontrar códigos de erro durante a operação de atualização das ONTAP tools for VMware vSphere . Os códigos de erro têm cinco dígitos, onde os dois primeiros dígitos representam o script que encontrou o problema e os três últimos 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. Este 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 nenhuma solução for mencionada.

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

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

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

Código de erro de atualização	Fluxo de trabalho	Resolução
052	O ISO pode ser o mesmo da versão atual ou duas versões acima da versão atual.	Use uma versão ISO compatível para atualizar a partir da sua versão atual.
068	A reversão dos pacotes Debian falhou	Use recuperação baseada em snapshot ou RPO zero e tente atualizar novamente.
069	Falha na restauração de arquivos	Use recuperação baseada em snapshot ou RPO zero e tente atualizar novamente.
070	Falha ao excluir o backup	-
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	A atualização das pré-verificações falhou	Tente atualizar novamente.
076	A atualização do registro falhou	Use recuperação baseada em snapshot ou RPO zero e tente atualizar novamente.
077	A reversão do registro falhou	Use recuperação baseada em snapshot ou RPO zero e tente atualizar novamente.
078	A atualização do operador falhou	Use recuperação baseada em snapshot ou RPO zero e tente atualizar novamente.

Código de erro de atualização	Fluxo de trabalho	Resolução
079	A reversão do operador falhou	Use recuperação baseada em snapshot ou RPO zero e tente atualizar novamente.
080	A atualização dos serviços falhou	Use recuperação baseada em snapshot ou RPO zero e tente atualizar novamente.
081	A reversão dos serviços falhou	Use recuperação baseada em snapshot ou RPO zero e tente atualizar novamente.
082	Falha ao excluir imagens antigas do contêiner	Use recuperação baseada em snapshot ou RPO zero e tente atualizar novamente.
083	A exclusão do backup falhou	Use recuperação baseada em snapshot ou RPO zero e tente atualizar novamente.
084	Falha ao alterar o JobManager de volta para Produção	Siga as etapas abaixo para recuperar/concluir a atualização. 1. Habilitar o Diagnostic Shell 2. Execute o comando: *sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade* 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. Habilitar o Diagnostic Shell 2. Execute o comando *sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade* 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	Falha na alteração da propriedade do arquivo de configuração de rotação do log de resumo	Tente atualizar novamente.
095	Falha na atualização do sistema operacional	Nenhuma recuperação para atualização do sistema operacional. Os serviços das ferramentas ONTAP serão atualizados e novos pods serão executados.

Código de erro de atualização	Fluxo de trabalho	Resolução
096	Instalar provisionador de armazenamento dinâmico	Verifique os logs de atualização e tente atualizar novamente.
097	A desinstalação dos serviços para atualização falhou	Use RPO zero ou recuperação baseada em snapshot e tente atualizar novamente.
098	a cópia do segredo dockercred do ntv-system 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 em caso de HA e a um nó em caso de implantação sem HA.
108	Falha no script de semeadura	-
109	o backup dos dados do volume persistente falhou	Verifique os logs de atualização e tente atualizar novamente.
110	a restauração dos dados do volume persistente falhou	Use recuperação baseada em snapshot ou RPO zero e tente atualizar novamente.
111	A atualização dos parâmetros de tempo limite do etcd para RKE2 falhou	Verifique os logs de atualização e tente atualizar novamente.
112	Falha na desinstalação do provisionador de armazenamento dinâmico	-
113	A atualização de recursos em nós secundários falhou	Verifique os logs de atualização e tente atualizar novamente.
104	A reinicialização do nó secundário falhou	Reinicie os nós manualmente um por um
100	a reversão do kernel falhou	-
051	a atualização do provisionador de armazenamento dinâmico falhou	Verifique os logs de atualização e tente atualizar novamente.
056	a exclusão do backup de migração falhou	N / D

A partir das ONTAP tools for VMware vSphere 10.3, o RPO zero não é mais suportado.

Saiba mais sobre "Como restaurar ONTAP tools for VMware vSphere se a atualização falhar da versão 10.0 para 10.1"

Migrar ONTAP tools for VMware vSphere 9.xx para 10.4

Migrar das ONTAP tools for VMware vSphere 9.xx para 10.4

Mover as ONTAP tools for VMware vSphere 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 ONTAP tools for VMware vSphere versões 9.12D1, 9.13D2 e 9.13P2 para as ONTAP tools for VMware vSphere 10.4.

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 armazenamentos de dados 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
Passos: 1. "Migrar o Provedor VASA" 2. "Criar políticas de armazenamento de VM"	Passos: 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 ONTAP tools for VMware vSphere 10.4" 3. "Atualizar o SRA" 4. "Criar políticas de armazenamento de VM"

Após a migração das ONTAP tools for VMware vSphere 9.xx para 10.4, os datastores vVols que usam o protocolo NVMe/FC tornam-se inoperantes porque as ferramentas ONTAP 10.4 oferecem 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 habilitar o Derby PORT 1527 nas ONTAP tools for VMware vSphere, habilite o usuário root e faça login na CLI via SSH. Em seguida, execute o seguinte comando:

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

2. Implante o OVA para ONTAP tools for VMware vSphere 10.4.
3. Adicione a instância do vCenter Server que você deseja migrar para as ONTAP tools for VMware vSphere 10.4. Consulte "Adicionar uma instância do vCenter Server" para maiores informações.
4. Integre o backend de armazenamento localmente a partir das APIs do servidor vCenter para o plug-in de ferramentas ONTAP .
5. 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/', for example: `\https://10.67.25.33:8443 .`

Método HTTP e ponto final

Esta chamada de API REST usa o seguinte método e endpoint.

Método HTTP	Caminho
PUBLICAR	/api/v1

Tipo de processamento

Assíncrono

Exemplo de ondulação

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 da solicitação para migração de outra versão:

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

Exemplo de saída JSON

Um objeto de trabalho 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": "em execução" }

6. 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`
```

Após concluir o trabalho, revise o relatório de migração. Este relatório está incluído nos dados do trabalho e pode ser acessado na resposta do trabalho.

7. Adicione as ONTAP tools for VMware vSphere ao vCenter Server e"Registre o Provedor VASA" com ONTAP tools for VMware vSphere.
8. "Habilitar provedor VASA"serviço em ONTAP tools for VMware vSphere 10.4.
9. Pare as ONTAP tools for VMware vSphere 9.10/9.11/9.12/9.13 no console de manutenção.

Não exclua o Provedor VASA.

Após a interrupção do antigo Provedor VASA, o vCenter Server faz failover para as ONTAP tools for VMware vSphere. Todos os datastores e VMs se tornam acessíveis e são atendidos pelas ONTAP tools for VMware vSphere.

10. Os datastores NFS e VMFS migrados das ONTAP tools for VMware vSphere 9.xxx ficam visíveis nas ONTAP tools for VMware vSphere 10.4 somente depois que o trabalho de descoberta do datastore é acionado, 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 do patch usando a seguinte API no Swagger ou no Postman:

Método HTTP e ponto final

Esta chamada de API REST usa o seguinte método e endpoint.

Método HTTP	Caminho
CORREÇÃO	/api/v1

Tipo de processamento

Assíncrono

Exemplo de ondulação

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 trabalho 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": "em execução" }

O corpo da solicitação está vazio para a operação de patch.

UUID é o UUID de migração retornado em resposta à API pós-migração.

Após executar a API de migração de patches, todas as VMs estarão em conformidade com a política de armazenamento.

O que vem a seguir

Após concluir a migração e registrar o ONTAP Tools 10.4 no vCenter Server, siga estas etapas:

- Aguarde a conclusão da **Descoberta**, os certificados serão atualizados automaticamente em todos os hosts.
- Aguarde tempo suficiente antes de iniciar as operações do armazenamento de dados e da máquina

virtual. O período de espera necessário varia de acordo com o número de hosts, armazenamentos de dados e máquinas virtuais na configuração. A não espera pode resultar em falhas operacionais intermitentes.

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

1. Navegue até o armazenamento de dados e selecione **Resumo** > **Políticas de armazenamento de VM**.

   O status de conformidade em **Conformidade da política de armazenamento de VM** é exibido como **Desatualizado**.

2. Selecione a política de VM de armazenamento e a VM correspondente
3. Selecione **Aplicar**

   O status de conformidade em **Conformidade da política de armazenamento de VM** agora é mostrado como compatível.

Informações relacionadas

- "Saiba mais sobre as ONTAP tools for VMware vSphere 10 RBAC"
- "Atualização das ONTAP tools for VMware vSphere 10.x para 10.4"

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 **CleanupP** e **Reprotect** estão desabilitados, enquanto os botões TEST e RUN 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 nova proteção estiver pendente. Certifique-se de que o processo de reproteção seja concluído antes de prosseguir com a migração. Se um failover de teste estiver em andamento, limpe-o e inicie a migração.

1. Siga estas etapas para excluir o adaptador SRA das ferramentas ONTAP para VMware vSphere 9.xx no VMware Site Recovery:
   a. Acesse a página de gerenciamento de configuração do VMware Live Site Recovery
   b. Vá para a seção **Adaptador de Replicação de Armazenamento**.
   c. No menu de reticências, selecione **Redefinir configuração**.
   d. No menu de reticências, selecione **Excluir**.
2. Execute essas etapas nos sites de proteção e recuperação.
   a. "Habilitar ONTAP tools for VMware vSphere"
   b. Instale as ONTAP tools for VMware vSphere 10.4 SRA seguindo as etapas em"Configurar SRA no dispositivo VMware Live Site Recovery" .
   c. Na página de interface do usuário do VMware Live Site Recovery, execute as operações **Descobrir matrizes** e **Descobrir dispositivos** e confirme se os dispositivos são exibidos como antes da migração.

Automatize usando a API REST

Saiba mais sobre as ONTAP tools for VMware vSphere 10 REST API

ONTAP tools for VMware vSphere 10 são um conjunto de ferramentas para gerenciamento do ciclo de vida de máquinas virtuais. Inclui uma API REST robusta que você pode usar como parte dos seus processos de automação.

Fundação de serviços web REST

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

Recursos e representação estatal

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

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

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

Mensagens HTTP

O Protocolo de Transferência de Hipertexto (HTTP) é o protocolo usado pelo cliente e servidor de serviços web para trocar mensagens sobre os recursos. Ele segue o modelo CRUD baseado nas operações genéricas de criação, leitura, atualização e exclusão. 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 o JavaScript Object Notation (JSON). JSON é um padrão do setor para representar estruturas de dados simples em texto simples e é usado para transferir informações de estado que descrevem os recursos e as ações desejadas.

Segurança

A segurança é um aspecto importante de uma API REST. Além do protocolo Transport Layer Security (TLS) usado para proteger o tráfego HTTP na rede, as ONTAP tools for VMware vSphere 10 REST API 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 ONTAP tools for VMware vSphere 10 executam a maioria das solicitações de forma síncrona, retornando um código de status quando a operação é concluída. Ele também oferece suporte ao processamento assíncrono para tarefas que exigem mais tempo para serem concluídas.

Ambiente do gerenciador de ferramentas ONTAP

Há vários aspectos do ambiente do Gerenciador de ferramentas ONTAP que você deve considerar.

Máquina virtual

As ONTAP tools for VMware vSphere 10 são implantadas usando a arquitetura de plug-in remoto do vSphere. O software, incluindo suporte para a API REST, é executado em uma máquina virtual separada.

Endereço IP das ferramentas ONTAP

As ONTAP tools for 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 será atribuído a um componente interno do balanceador de carga. O endereço é usado pela interface de usuário do Gerenciador de ferramentas ONTAP , bem como para acessar a página de documentação do Swagger e a API REST diretamente.

Duas APIs REST

Além das ONTAP tools for VMware vSphere 10 REST API, o cluster ONTAP tem sua própria REST API. O Gerenciador de ferramentas ONTAP usa a API REST do ONTAP como cliente para executar tarefas relacionadas ao armazenamento. É importante ter em mente que essas duas APIs são separadas e distintas. Para obter mais informações, consulte "Automação ONTAP" .

Detalhes de implementação das ONTAP tools for VMware vSphere 10 REST API

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 o design das ONTAP tools for VMware vSphere 10 REST API antes de usá-las.

A API REST inclui diversas categorias de recursos, como vCenters e Agregados. Revise o"Referência de API" para mais informações.

Como acessar a API REST

Você pode acessar as ONTAP tools for VMware vSphere 10 por meio do endereço IP das ferramentas ONTAP junto com a porta. Há várias partes no URL completo, incluindo:

- Ferramentas ONTAP endereço IP e porta
- Versão API
- Categoria de recurso
- Recurso específico

Você deve configurar o endereço IP durante a configuração inicial, enquanto a porta permanece fixa em 8443. A primeira parte da URL é consistente para cada instância do ONTAP tools for VMware vSphere 10; somente a categoria do recurso e o recurso específico mudam entre os endpoints.

> Os valores de endereço IP e porta nos exemplos abaixo são apenas para fins ilustrativos. Você precisa alterar esses valores para seu ambiente.

Exemplo para acessar serviços de autenticação

```
https://10.61.25.34:8443/virtualization/api/v1/auth/login
```

Esta URL pode ser usada para solicitar um token de acesso usando o método POST.

Exemplo para listar os servidores vCenter

`https://10.61.25.34:8443/virtualization/api/v1/vcenters`

Esta URL pode ser usada para solicitar uma lista das instâncias definidas do servidor vCenter usando o método GET.

Detalhes HTTP

As ONTAP tools for VMware vSphere 10 usam HTTP e parâmetros relacionados para atuar nas instâncias e coleções de recursos. Detalhes da implementação do HTTP são apresentados abaixo.

Métodos HTTP

Os métodos ou verbos HTTP suportados pela API REST são apresentados na tabela abaixo.

Método	CRUD	Descrição
PEGAR	Ler	Recupera propriedades de objeto para uma instância ou coleção de recursos. Isso é considerado uma operação de lista quando usado com uma coleção.
PUBLICAR	Criar	Cria uma nova instância de recurso com base nos parâmetros de entrada.
COLOCAR	Atualizar	Atualiza uma instância de recurso inteira com o corpo da solicitação JSON fornecido. Os valores-chave que não podem ser modificados pelo usuário são preservados.
CORREÇÃO	Atualizar	Solicita que um conjunto de alterações selecionadas na solicitação seja aplicado à instância do recurso.
EXCLUIR	Excluir	Exclui uma instância de recurso existente.

Cabeçalhos de solicitação e resposta

A tabela a seguir resume os cabeçalhos HTTP mais importantes usados com a API REST.

Cabeçalho	Tipo	Notas de uso
Aceitar	Solicitar	Este é o tipo de conteúdo que o aplicativo cliente pode aceitar. Os valores válidos incluem '*/*` ou `application/json`.
x-auth	Solicitar	Contém um token de acesso que identifica o usuário que emite a solicitação por meio do aplicativo cliente.
Tipo de conteúdo	Resposta	Retornado pelo servidor com base no `Accept` cabeçalho da solicitação.

Códigos de status HTTP

Os códigos de status HTTP usados pela API REST são descritos abaixo.

Código	Significado	Descrição
200	OK	Indica sucesso para chamadas que não criam uma nova instância de recurso.

Código	Significado	Descrição
201	Criado	Um objeto foi criado com sucesso com um identificador exclusivo para a instância do recurso.
202	Aceito	A solicitação foi aceita e um trabalho em segundo plano foi criado para executá-la.
204	Nenhum conteúdo	A solicitação foi bem-sucedida, embora nenhum conteúdo tenha sido retornado.
400	Pedido ruim	A entrada solicitada não é reconhecida ou é inadequada.
401	Não autorizado	O usuário não está autorizado e deve se autenticar.
403	Proibido	Acesso negado devido a um erro de autorização.
404	Não encontrado	O recurso mencionado 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 na 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 ONTAP Tools Manager (nome de usuário e senha).
- Os tokens são formatados como JSON Web Token (JWT).
- Cada token expira após 60 minutos.
- As solicitações de API de um cliente devem incluir o token no `x-auth` cabeçalho da solicitação.

Consulte"Sua primeira chamada de API REST" para um exemplo de solicitação e uso de um token de acesso.

Solicitações síncronas e assíncronas

A maioria das chamadas da API REST são concluídas rapidamente e, portanto, executadas de forma síncrona. Ou seja, eles retornam um código de status (como 200) após uma solicitação ser concluída. Solicitações que demoram mais para serem concluídas são executadas de forma assíncrona usando um trabalho em segundo plano.

Após emitir uma chamada de API executada de forma assíncrona, o servidor retorna um código de status HTTP 202. Isso indica que a solicitação foi aceita, mas ainda não foi concluída. Você pode consultar 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 armazenamento de dados e vVol. Consulte a categoria do gerenciador de tarefas da API REST na página do Swagger para obter mais informações.

Suas primeiras ONTAP tools for VMware vSphere 10

Você pode emitir uma chamada de API usando curl para começar a usar as ONTAP tools for VMware vSphere 10.

Antes de começar

Você deve revisar as informações e os parâmetros necessários nos exemplos de curl.

Informações necessárias

Você precisa do seguinte:

- ONTAP tools for VMware vSphere 10 endereço IP ou FQDN, bem como a porta
- Credenciais para o administrador do ONTAP Tools Manager (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 que ele seja executado. As variáveis estão descritas na tabela abaixo.

Variável	Descrição
$FQDN_IP_PORT	O nome de domínio totalmente qualificado ou endereço IP do Gerenciador de ferramentas ONTAP , juntamente com o número da porta.
$MEUUSUÁRIO	Nome de usuário para a conta do Gerenciador de ferramentas ONTAP .
$MINHASENHA	Senha associada ao nome de usuário do Gerenciador de ferramentas ONTAP .
$ACCESS_TOKEN	O token de acesso emitido pelo Gerenciador de ferramentas ONTAP .

Os seguintes comandos e saídas 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
```

Etapa 1: Adquira 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 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: emitir a chamada da API REST

Depois de obter um token de acesso, você pode usar curl para emitir uma chamada de API REST. Inclua o token de acesso adquirido na primeira etapa.

Exemplo de ondulação

```
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 ONTAP .

Referência de API para as ONTAP tools for VMware vSphere 10 REST API

A referência da API REST das ONTAP tools for VMware vSphere 10 contém detalhes sobre todas as chamadas de API. Esta referência é útil ao desenvolver aplicativos de automação.

Você pode acessar a documentação da API REST das ONTAP tools for VMware vSphere 10 on-line por meio da interface de usuário do Swagger. Você precisa do endereço IP ou FQDN das ONTAP tools for VMware vSphere 10, bem como da porta.

Passos

1. Digite a seguinte URL no seu navegador, substituindo o endereço IP apropriado e a combinação de porta pela variável e pressione **Enter**.

   `https://$FQDN_IP_PORT/`

   Exemplo

   `https://10.61.25.33:8443/`

2. Como exemplo de uma chamada de API individual, role para baixo até a categoria **vCenters** e selecione **GET** ao lado do ponto de extremidade `/virtualization/api/v1/vcenters`

Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

Direitos autorais

"https://www.netapp.com/company/legal/copyright/"

Marcas Registradas

NETAPP, o logotipo da NETAPP e as marcas listadas na página de Marcas Registradas da NetApp são marcas registradas da NetApp, Inc. Outros nomes de empresas e produtos podem ser marcas registradas de seus respectivos proprietários.

"https://www.netapp.com/company/legal/trademarks/"

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/"

Código aberto

Os arquivos de aviso fornecem informações sobre direitos autorais e licenças de terceiros usados no software NetApp .

"Aviso para ONTAP tools for VMware vSphere 10.4"

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 DESTE DOCUMENTO. 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 SOBRESSALENTES; 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 DESTE SOFTWARE, 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.