VMware

Enterprise applications

NetApp
February 11, 2026

Índice

VMware

VMware vSphere com ONTAP

VMware vSphere com ONTAP

A ONTAP serviu como uma solução de armazenamento de dados de primeira linha para o VMware vSphere e, mais recentemente, para ambientes Cloud Foundation desde sua introdução no data center moderno em 2002. Ele continua a introduzir recursos inovadores que simplificam o gerenciamento e reduzem custos.

Este documento apresenta a solução ONTAP para vSphere, destacando as informações mais recentes do produto e as práticas recomendadas para simplificar a implantação, mitigar riscos e simplificar o gerenciamento.

> Esta documentação substitui os relatórios técnicos publicados anteriormente *TR-4597: VMware vSphere for ONTAP*

As práticas recomendadas complementam outros documentos, como guias e listas de compatibilidade. Eles são desenvolvidos com base em testes de laboratório e extensa experiência de campo por engenheiros e clientes da NetApp. Elas podem não ser as únicas práticas suportadas que funcionam em todos os ambientes, mas são geralmente as soluções mais simples que atendem às necessidades da maioria dos clientes.

Este documento se concentra em recursos nas versões recentes do ONTAP (9.x) executadas no vSphere 7,0 ou posterior. Consulte "Ferramenta de Matriz de interoperabilidade (IMT)" e "Guia de compatibilidade da VMware" para obter detalhes relacionados a lançamentos específicos.

Por que o ONTAP para VMware vSphere?

Os clientes selecionam com confiança o ONTAP para vSphere para soluções de armazenamento SAN e NAS. A nova arquitetura simplificada de armazenamento desagregado, presente nos mais recentes All SAN Arrays, proporciona uma experiência simplificada e familiar aos administradores de armazenamento SAN, mantendo a maioria das integrações e o conjunto de recursos dos sistemas ONTAP tradicionais. Os sistemas ONTAP fornecem proteção excepcional de instantâneos e ferramentas de gerenciamento robustas. Ao transferir funções para armazenamento dedicado, o ONTAP maximiza os recursos do host, reduz custos e mantém o desempenho ideal. Além disso, as cargas de trabalho podem ser facilmente migradas usando o Storage vMotion entre VMFS, NFS ou vVols.

As vantagens de usar o ONTAP para vSphere

Há muitos motivos pelos quais dezenas de milhares de clientes escolheram o ONTAP como sua solução de storage para o vSphere, como um sistema de storage unificado compatível com protocolos SAN e nas, recursos robustos de proteção de dados usando snapshots com uso eficiente de espaço e diversas ferramentas para ajudar você a gerenciar dados de aplicações. O uso de um sistema de storage separado do hipervisor permite descarregar várias funções e maximizar seu investimento nos sistemas de host vSphere. Essa abordagem não só garante que os recursos de host estejam focados nas cargas de trabalho dos aplicativos, mas também evita efeitos aleatórios de desempenho nos aplicativos das operações de storage.

Usar o ONTAP junto com o vSphere é uma ótima combinação que permite reduzir despesas com hardware de host e software VMware. Você também pode proteger seus dados a um custo menor com alto desempenho consistente. Como as cargas de trabalho virtualizadas são móveis, você pode explorar diferentes abordagens usando o Storage vMotion para mover VMs entre datastores VMFS, NFS ou vVols , tudo no mesmo sistema de armazenamento.

Aqui estão os principais fatores que os clientes valorizam hoje:

- **Armazenamento unificado.** Os sistemas que executam o ONTAP são unificados de várias maneiras significativas. Originalmente, essa abordagem se referia aos protocolos NAS e SAN, e o ONTAP continua sendo uma plataforma líder para SAN, juntamente com sua força original no NAS. No mundo do vSphere, essa abordagem também pode significar um sistema unificado para infraestrutura de desktop virtual (VDI) junto com infraestrutura de servidor virtual (VSI). Os sistemas que executam ONTAP geralmente são mais baratos para VSI do que os arrays empresariais tradicionais e ainda têm recursos avançados de eficiência de armazenamento para lidar com VDI no mesmo sistema. O ONTAP também unifica uma variedade de mídias de armazenamento, de SSDs a SATA, e pode estendê-las facilmente para a nuvem. Não há necessidade de comprar um sistema operacional de armazenamento para desempenho, outro para arquivos e ainda outro para a nuvem. ONTAP une todos eles.
- **All SAN Array (ASA).** Os sistemas ONTAP ASA mais recentes (começando com A1K, A90, A70, A50, A30 e A20) foram criados com base em uma nova arquitetura de storage que elimina o paradigma tradicional de storage da ONTAP de gerenciamento de agregados e volumes. Como não há compartilhamentos de sistema de arquivos, não há necessidade de volumes! Todo o storage anexado a um par de HA é Tratado como uma zona de disponibilidade de storage (SAZ) comum na qual LUNs e namespaces NVMe são provisionados como "unidades de storage" (SUS). Os sistemas ASA mais recentes foram projetados para serem simples de gerenciar, com uma experiência familiar para administradores de storage de SAN. Essa nova arquitetura é ideal para ambientes vSphere, pois permite o gerenciamento fácil de recursos de storage e oferece uma experiência simplificada para administradores de storage SAN. A arquitetura do ASA também é compatível com a mais recente tecnologia NVMe over Fabrics (NVMe-of), que oferece ainda mais performance e escalabilidade para workloads vSphere.
- **Tecnologia Snapshot.** A ONTAP foi a primeira a fornecer tecnologia snapshot para proteção de dados, e continua sendo a mais avançada do setor. Essa abordagem com uso eficiente de espaço para proteção de dados foi estendida para oferecer suporte às APIs do VMware vSphere para Array Integration (VAAI). Essa integração permite que você aproveite os recursos de snapshot do ONTAP para operações de backup e restauração, reduzindo o impacto no seu ambiente de produção. Essa abordagem também permite que você use snapshots para recuperação rápida de VMs, reduzindo o tempo e o esforço necessários para restaurar os dados. Além disso, a tecnologia de snapshot da ONTAP é integrada às soluções de recuperação de site em tempo real (VLSR, anteriormente Gerenciador de recuperação de site [SRM]) da VMware, fornecendo uma estratégia abrangente de proteção de dados para o seu ambiente virtualizado.
- **Gerenciamento baseado em políticas de armazenamento e volumes virtuais.** A NetApp foi uma das primeiras parceiras de design da VMware no desenvolvimento do vSphere Virtual Volumes (vVols), fornecendo informações arquitetônicas e suporte inicial para vVols e VMware vSphere APIs for Storage Awareness (VASA). Essa abordagem não apenas trouxe gerenciamento granular de armazenamento de VM para o VMFS, como também ofereceu suporte à automação do provisionamento de armazenamento por meio do gerenciamento baseado em políticas de armazenamento. Essa abordagem permite que arquitetos de armazenamento projetem pools de armazenamento com diferentes recursos que podem ser facilmente consumidos por administradores de VM. ONTAP lidera o setor de armazenamento em escala de vVol, dando suporte a centenas de milhares de vVols em um único cluster, enquanto fornecedores de matrizes corporativas e matrizes flash menores dão suporte a apenas alguns milhares de vVols por matriz. A NetApp também está impulsionando a evolução do gerenciamento granular de VMs com recursos futuros.
- **Eficiência de armazenamento.** Embora a NetApp tenha sido a primeira a oferecer desduplicação para cargas de trabalho de produção, essa inovação não foi a primeira nem a última nessa área. Tudo

começou com snapshots, um mecanismo de proteção de dados com eficiência de espaço e sem impacto no desempenho, juntamente com a tecnologia FlexClone para fazer instantaneamente cópias de leitura/gravação de VMs para uso em produção e backup. A NetApp passou a fornecer recursos em linha, incluindo desduplicação, compactação e desduplicação de bloco zero, para extrair o máximo de armazenamento de SSDs caros. O ONTAP também adicionou a capacidade de compactar operações de E/S e arquivos menores em um bloco de disco usando compactação. A combinação desses recursos fez com que os clientes geralmente observassem economias de até 5:1 para VSI e até 30:1 para VDI. A mais nova geração de sistemas ONTAP também inclui compactação e desduplicação aceleradas por hardware, o que pode melhorar ainda mais a eficiência do armazenamento e reduzir custos. Essa abordagem permite que você armazene mais dados em menos espaço, reduzindo o custo geral de armazenamento e melhorando o desempenho. A NetApp está tão confiante em seus recursos de eficiência de armazenamento que oferece um Garantia de Eficiência.

- **Multilocação.** O ONTAP é líder em multilocação há muito tempo, permitindo que você crie várias máquinas virtuais de armazenamento (SVMs) em um único cluster. Essa abordagem permite isolar cargas de trabalho e fornecer diferentes níveis de serviço para diferentes locatários, tornando-a ideal para provedores de serviços e grandes empresas. A última geração de sistemas ONTAP também inclui suporte para gerenciamento de capacidade de locatários. Esse recurso permite que você defina limites de capacidade para cada locatário, garantindo que nenhum locatário possa consumir todos os recursos disponíveis. Essa abordagem ajuda a garantir que todos os inquilinos recebam o nível de serviço esperado, ao mesmo tempo em que proporciona um alto nível de segurança e isolamento entre eles. Além disso, os recursos de multilocação do ONTAP são integrados à plataforma vSphere da VMware, permitindo que você gerencie e monitore facilmente seu ambiente virtualizado por meio de "Ferramentas do ONTAP para VMware vSphere" e "Insights da infraestrutura de dados" .
- **Nuvem híbrida.** Seja usado para nuvem privada local, infraestrutura de nuvem pública ou uma nuvem híbrida que combina o melhor de ambas, as soluções ONTAP ajudam você a construir sua estrutura de dados para simplificar e otimizar o gerenciamento de dados. Comece com sistemas all-flash de alto desempenho e, em seguida, combine-os com sistemas de armazenamento em disco ou em nuvem para proteção de dados e computação em nuvem. Escolha entre Azure, AWS, IBM ou Google Cloud para otimizar custos e evitar aprisionamento. Aproveite o suporte avançado para OpenStack e tecnologias de contêiner conforme necessário. A NetApp também oferece backup baseado em nuvem (SnapMirror Cloud, Cloud Backup Service e Cloud Sync) e ferramentas de arquivamento e níveis de armazenamento (FabricPool) para ONTAP para ajudar a reduzir despesas operacionais e aproveitar o amplo alcance da nuvem.
- **E muito mais.** Aproveite a performance extrema dos arrays NetApp AFF A-Series para acelerar sua infraestrutura virtualizada e gerenciar custos. Aproveite operações totalmente ininterruptas, desde a manutenção até os upgrades até a substituição completa do seu sistema de storage, usando clusters ONTAP com escalabilidade horizontal. Proteger dados em repouso com os recursos de criptografia do NetApp sem custo adicional. Certifique-se de que o desempenho atenda aos níveis de serviço de negócios por meio de recursos de qualidade de serviço refinados. Todos eles fazem parte da ampla variedade de recursos fornecidos com o ONTAP, o software de gerenciamento de dados empresariais líder do setor.

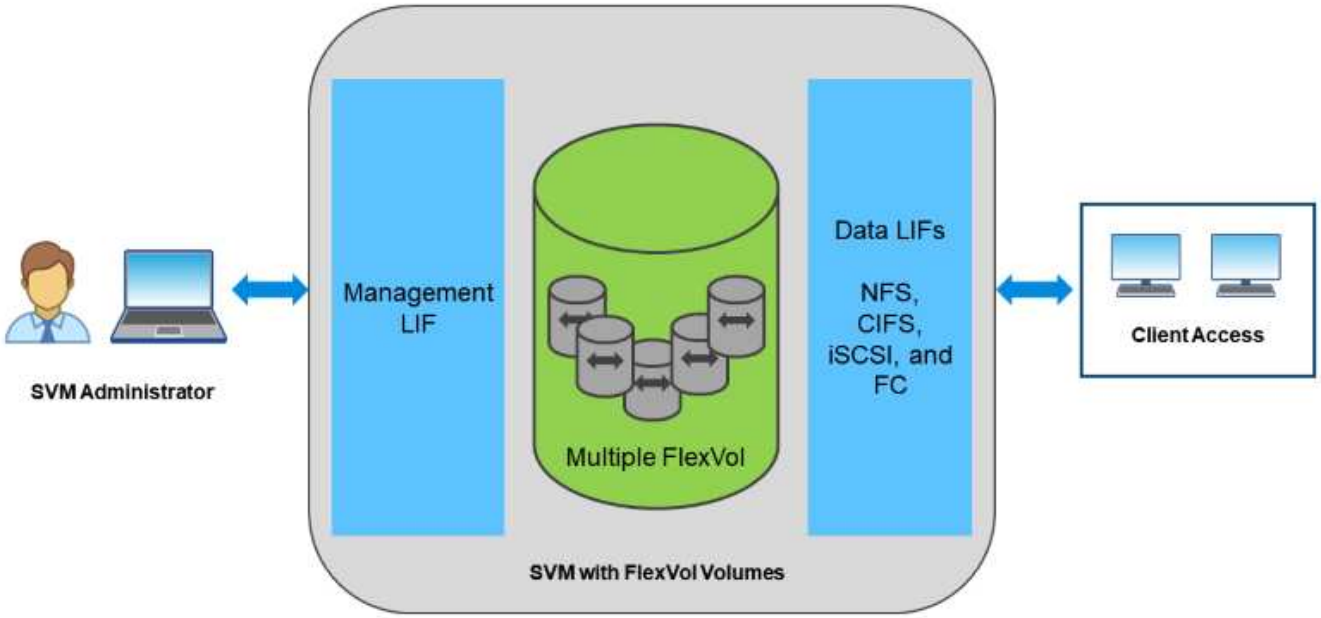
Storage unificado

O ONTAP unifica o storage por meio de uma abordagem simplificada definida por software para gerenciamento seguro e eficiente, performance aprimorada e escalabilidade otimizada. Essa abordagem aprimora a proteção de dados e permite o uso eficaz de recursos de nuvem.

Originalmente, essa abordagem unificada se referia ao suporte aos protocolos nas e SAN em um sistema de storage, e a ONTAP continua sendo uma plataforma líder de SAN, juntamente com sua força original em nas. O ONTAP agora também fornece suporte ao protocolo de objetos S3. Embora o S3 não seja usado para

datastores, você pode usá-lo para aplicações in-Guest. Pode obter mais informações sobre o suporte ao protocolo S3 no ONTAP no "Visão geral da configuração do S3". O termo storage unificado evoluiu para significar uma abordagem unificada para o gerenciamento de storage, incluindo a capacidade de gerenciar todos os seus recursos de storage a partir de uma única interface. Isso inclui a capacidade de gerenciar recursos de storage de nuvem e no local, os sistemas All SAN Array (ASA) mais recentes e a capacidade de gerenciar vários sistemas de storage em uma única interface.

Uma máquina virtual de storage (SVM) é a unidade de alocação segura a vários clientes no ONTAP. É uma construção lógica que permite o acesso do cliente a sistemas que executam o ONTAP. Os SVMs podem servir dados simultaneamente por meio de vários protocolos de acesso a dados por meio de interfaces lógicas (LIFs). As SVMs fornecem acesso a dados no nível do arquivo por meio de protocolos nas, como CIFS e NFS, e acesso a dados em nível de bloco por meio de protocolos SAN, como iSCSI, FC/FCoE e NVMe. Os SVMs podem fornecer dados a clientes SAN e nas de forma independente ao mesmo tempo, bem como ao S3.



No mundo vSphere, essa abordagem também pode significar um sistema unificado para infraestrutura de desktop virtual (VDI), juntamente com a infraestrutura de servidor virtual (VSI). Os sistemas que executam o ONTAP geralmente são mais baratos para VSI do que os arrays empresariais tradicionais e ainda têm recursos avançados de eficiência de storage para lidar com a VDI no mesmo sistema. O ONTAP também unifica uma variedade de Mídia de armazenamento, de SSDs a SATA, e pode estender isso facilmente para a nuvem. Não é necessário comprar um array flash para obter desempenho, um array SATA para arquivos e sistemas separados para a nuvem. ONTAP une todos eles.

OBSERVAÇÃO: para obter mais informações sobre SVMs, armazenamento unificado e acesso ao cliente, consulte "Virtualização de storage" no Centro de Documentação do ONTAP 9.

Ferramentas de virtualização para ONTAP

O NetApp fornece várias ferramentas de software independentes compatíveis com os sistemas ONTAP e ASA tradicionais, integrando o vSphere para gerenciar efetivamente seu ambiente virtualizado.

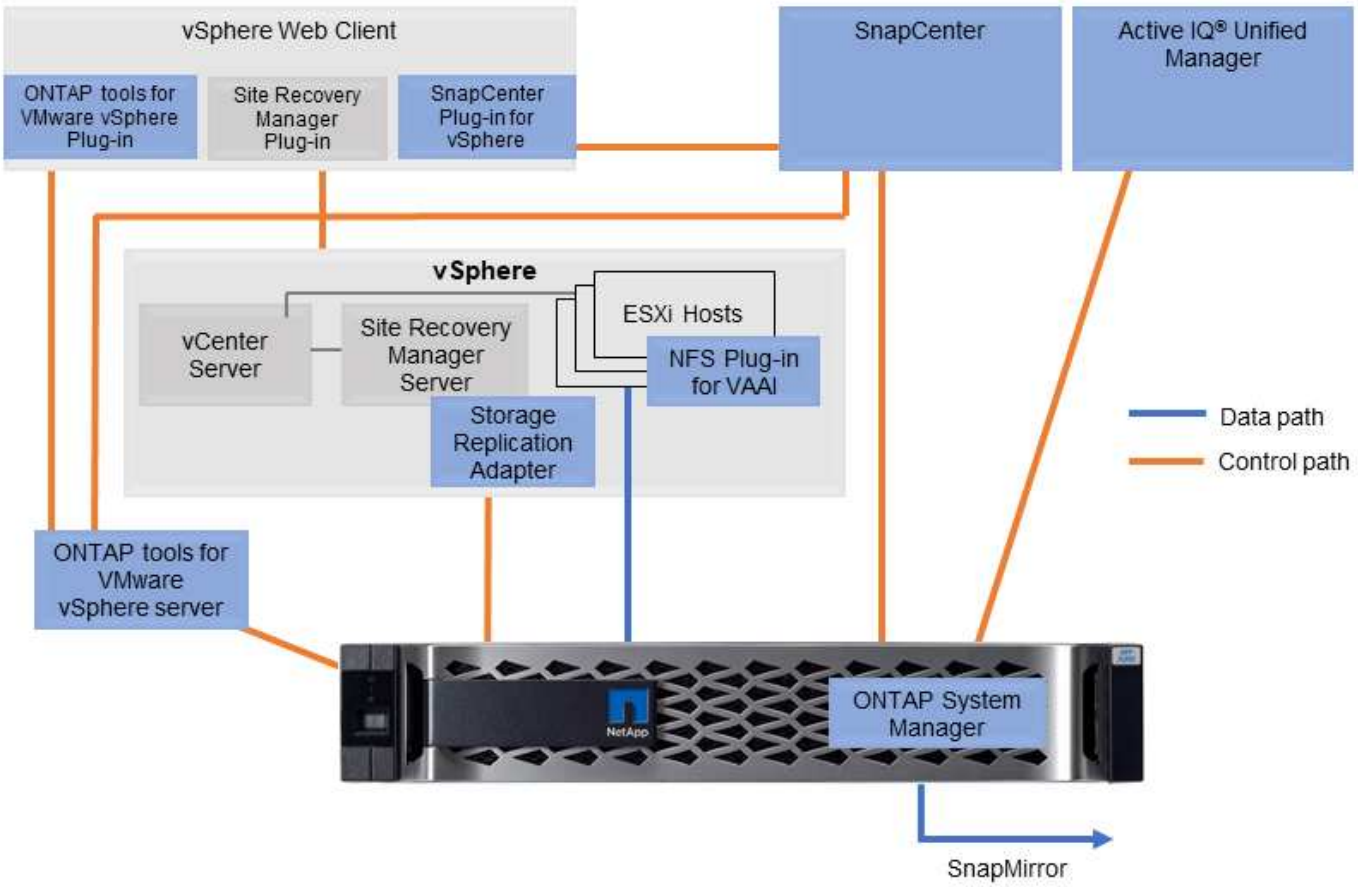
As ferramentas a seguir estão incluídas com a licença ONTAP One sem custo adicional. Consulte a Figura 1 para ver uma descrição de como essas ferramentas funcionam juntas no seu ambiente vSphere.

Ferramentas do ONTAP para VMware vSphere

"Ferramentas do ONTAP para VMware vSphere" O é um conjunto de ferramentas para usar o armazenamento do ONTAP junto com o vSphere. O plug-in do vCenter, anteriormente conhecido como Virtual Storage Console (VSC), simplifica o gerenciamento de storage e os recursos de eficiência, aprimora a disponibilidade e reduz os custos de storage e a sobrecarga operacional, independentemente de você estar usando SAN ou nas. Ele usa as práticas recomendadas para provisionar armazenamentos de dados e otimiza as configurações de host ESXi para ambientes de storage de bloco e NFS. Para todos esses benefícios, a NetApp recomenda o uso dessas ferramentas do ONTAP como uma prática recomendada ao usar o vSphere com sistemas que executam o ONTAP. Ele inclui um dispositivo de servidor, extensões de IU para vCenter, provedor VASA e adaptador de replicação de armazenamento. Quase tudo nas ferramentas do ONTAP pode ser automatizado com o uso de APIs REST simples, consumíveis pela maioria das ferramentas de automação modernas.

- * Extensões de IU do vCenter.* As extensões de IU das ferramentas do ONTAP simplificam o trabalho das equipes de operações e administradores do vCenter, incorporando menus sensíveis ao contexto fáceis de usar para gerenciar hosts e armazenamento, portlets informativos e recursos de alerta nativos diretamente na IU do vCenter para fluxos de trabalho simplificados.
- **Fornecedor VASA para ONTAP.** O provedor VASA para ONTAP oferece suporte à estrutura VMware vStorage APIs for Storage Awareness (VASA). Ele é fornecido como parte das ferramentas do ONTAP para o VMware vSphere como um único dispositivo virtual para facilitar a implantação. O provedor VASA coneta o vCenter Server com o ONTAP para auxiliar no provisionamento e monitoramento do armazenamento de VM. Ele permite o suporte do VMware Virtual volumes (vVols), o gerenciamento de perfis de funcionalidades de storage e o desempenho individual de vVols de VM, além de alarmes para monitorar a capacidade e a conformidade com os perfis.
- **Adaptador de replicação de armazenamento.** O SRA é usado junto com o VMware Live Site Recovery (VLSR)/Site Recovery Manager (SRM) para gerenciar a replicação de dados entre sites de produção e recuperação de desastres usando o SnapMirror para replicação baseada em array. Ele pode automatizar a tarefa de failover em caso de desastre e pode ajudar a testar as réplicas de DR sem interrupções para garantir a confiança na sua solução de DR.

A figura a seguir mostra as ferramentas do ONTAP para vSphere.



Plug-in do SnapCenter para VMware vSphere

O "Plug-in do SnapCenter para VMware vSphere" é um plug-in para o vCenter Server que permite gerenciar backups e restaurações de máquinas virtuais (VMs) e armazenamentos de dados. Ele fornece uma interface única para gerenciar backups, restaurações e clones de VMs e armazenamentos de dados em vários sistemas ONTAP . O SnapCenter oferece suporte à replicação e recuperação de sites secundários usando o SnapMirror. As versões mais recentes também oferecem suporte ao SnapMirror para nuvem (S3), instantâneos à prova de violação, SnapLock e sincronização ativa do SnapMirror . O SnapCenter Plug-In para VMware vSphere pode ser integrado com plugins de aplicativos SnapCenter para fornecer backups consistentes com aplicativos.

Plug-in NFS para VMware VAAI

O "Plug-in NFS do NetApp para VMware VAAI" é um plug-in para hosts ESXi que permite que eles usem recursos do VAAI com datastores NFS no ONTAP. Ele dá suporte a descarga de cópia para operações de clone, reserva de espaço para arquivos de disco virtual com espessura e descarga de snapshot. Descarregar operações de cópia para armazenamento não é necessariamente mais rápido de ser concluído, mas reduz os requisitos de largura de banda da rede e descarrega recursos do host, como ciclos de CPU, buffers e filas. Você pode usar as ferramentas do ONTAP para o VMware vSphere para instalar o plug-in em hosts ESXi ou, onde for compatível, o vLCM (vSphere Lifecycle Manager).

Opções de software premium

Os seguintes produtos de software premium estão disponíveis na NetApp. Eles não estão incluídos na licença do ONTAP One e devem ser adquiridos separadamente.

- "NetApp Disaster Recovery"para VMware vSphere. Este é um serviço baseado em nuvem que fornece

recuperação de desastres e backup para ambientes VMware. Ele pode ser usado com ou sem SnapCenter e oferece suporte a DR local para local usando SAN ou NAS, e local para/da nuvem usando NFS, onde houver suporte.

- "Insights de infraestrutura de dados (DII)". Este é um serviço baseado em nuvem que fornece monitoramento e análise para ambientes VMware. Ele oferece suporte a outros fornecedores de armazenamento em ambientes de armazenamento heterogêneos, bem como a vários fornecedores de switches e outros hipervisores. O DII fornece insights completos de ponta a ponta sobre o desempenho, a capacidade e a integridade do seu ambiente VMware.

Volumes virtuais (vVols) e gerenciamento baseado em políticas de storage (SPBM)

Anunciado pela primeira vez em 2012, a NetApp foi um dos primeiros parceiros de design da VMware no desenvolvimento das APIs do VMware vSphere para conscientização de armazenamento (VASA), a base do gerenciamento baseado em políticas de armazenamento (SPBM) com storage arrays empresariais. Essa abordagem trouxe gerenciamento limitado de storage granular de VM para o storage VMFS e NFS.

Como parceiro de design de tecnologia, a NetApp forneceu informações sobre arquitetura e, em 2015, anunciou suporte para vVols. Essa nova tecnologia agora permitiu a automação do provisionamento de storage granular e verdadeiramente nativo em array por meio do SPBM.

Volumes virtuais (vVols)

O vVols é uma arquitetura revolucionária de armazenamento que permite o gerenciamento granular do armazenamento de VM, permitindo que o armazenamento seja gerenciado não apenas por VM (incluindo metadados de VM), mas mesmo por VMDK. O vVols é um componente essencial da estratégia de Software Defined Data Center (SDDC) que forma a base do VMware Cloud Foundation (VCF), fornecendo uma arquitetura de armazenamento mais eficiente e escalável para ambientes virtualizados.

Os vVols permitem que as VMs consumam o storage por VM, porque cada objeto de storage de VM é uma entidade exclusiva no NetApp ONTAP. Com os sistemas ASA R2 que não precisam mais de gerenciamento de volume, isso significa que cada objeto de armazenamento de VM é uma unidade de armazenamento exclusiva (SU) no storage e pode ser controlado de forma independente. Isso permite a criação de políticas de storage que podem ser aplicadas a VMs individuais ou VMDKs (e, portanto, SUS indivudual), fornecendo controle granular sobre serviços de storage, como performance, disponibilidade e proteção de dados.

Gerenciamento baseado em políticas de storage (SPBM)

O SPBM fornece uma estrutura que serve como uma camada de abstração entre os serviços de armazenamento disponíveis para o seu ambiente de virtualização e os elementos de armazenamento provisionados por meio de políticas. Essa abordagem permite que os arquitetos de storage projetem pools de storage com recursos diferentes. Esses pools podem ser facilmente consumidos pelos administradores de VM. Os administradores podem, então, corresponder aos requisitos de carga de trabalho da máquina virtual aos pools de armazenamento provisionados. Essa abordagem simplifica o gerenciamento de storage e permite o uso mais eficiente dos recursos de storage.

O SPBM é um componente chave do vVols, fornecendo uma estrutura baseada em políticas para gerenciar serviços de storage. As políticas são criadas pelos administradores do vSphere usando regras e recursos expostos pelo provedor VASA (VP) do fornecedor. É possível criar políticas para diferentes serviços de storage, como performance, disponibilidade e proteção de dados. As políticas podem ser atribuídas a VMs ou VMDKs individuais, fornecendo controle granular sobre os serviços de storage.

NetApp ONTAP e vVols

A NetApp ONTAP lidera o setor de storage em escala de vVols, dando suporte a centenas de milhares de vVols em um único cluster*. Em contraste, os fornecedores de array empresarial e flash arrays menores dão suporte a apenas milhares de vVols por array. O ONTAP fornece uma solução de storage dimensionável e eficiente para ambientes VMware vSphere, com suporte ao vVols com um conjunto avançado de serviços de storage, incluindo deduplicação de dados, compactação, thin Provisioning e proteção de dados. O SPBM permite uma integração perfeita com ambientes VMware vSphere.

Mencionamos anteriormente que os administradores de VM podem consumir capacidade como pools de storage. Isso é feito por meio do uso de contêineres de storage que são representados no vSphere como armazenamentos de dados lógicos.

Os contêineres de storage são criados por administradores de storage e são usados para agrupar recursos de storage que podem ser consumidos por administradores de VM. Os contêineres de armazenamento podem ser criados de forma diferente dependendo do tipo de sistema ONTAP que você está usando. Com clusters tradicionais do ONTAP 9, os contêineres recebem um ou mais volumes do FlexVol de backup que juntos formam o pool de storage. Com os sistemas ASA R2, todo o cluster é o pool de storage.

Para obter mais informações sobre o VMware vSphere Virtual volumes, SPBM e ONTAP, "TR-4400: VMware vSphere Virtual volumes com ONTAP"consulte .

*Dependendo da plataforma e do protocolo

Armazenamentos de dados e protocolos

Visão geral dos recursos do vSphere datastore e do protocolo

Seis protocolos são usados para conetar o VMware vSphere a datastores em um sistema que executa o ONTAP:

- FCP
- NVMe/FC
- NVMe/TCP
- ISCSI
- NFS v3
- NFS v4.1

FCP, NVMe/FC, NVMe/TCP e iSCSI são protocolos de bloco que usam o vSphere Virtual Machine File System (VMFS) para armazenar VMs dentro de LUNs ONTAP ou namespaces NVMe contidos em um ONTAP FlexVol volume. O NFS é um protocolo de arquivos que coloca as VMs em armazenamentos de dados (que são simplesmente volumes ONTAP) sem a necessidade de VMFS. SMB (CIFS), iSCSI, NVMe/TCP ou NFS também podem ser usados diretamente de um sistema operacional convidado para o ONTAP.

As tabelas a seguir apresentam os recursos de datastore tradicionais compatíveis com vSphere e ONTAP. Essas informações não se aplicam a datastores vVols, mas geralmente se aplicam ao vSphere 6.x e versões posteriores usando versões compatíveis do ONTAP. Você também pode consultar a "Ferramenta VMware Configuration Maximums" para versões específicas do vSphere e confirmar limites específicos.

Capacidade/funcionalidade	FC	ISCSI	NVMe-of	NFS
Formato	VMFS ou mapeamento de dispositivo bruto (RDM)	VMFS ou RDM	VMFS	n/a.
Número máximo de armazenamentos de dados ou LUNs	1024 LUNs por host ESXi, até 32 caminhos por LUN, até 4096 caminhos totais por host, até 128 hosts por datastore	1024 LUNs por host ESXi, até 32 caminhos por LUN, até 4096 caminhos totais por host, até 128 hosts por datastore	256 namespaces por host ESXi, até 32 caminhos por namespace por host, 2048 caminhos totais por host, até 16 hosts por datastore	256 conexões NFS por host (impactadas pelo nconnect e pelo entroncamento de sessão) NFS padrão. MaxVolumes é 8. Use as ferramentas do ONTAP para o VMware vSphere para aumentar para 256.
Tamanho máximo do datastore	64 TB	64 TB	64 TB	300TB FlexVol volume ou superior com volume FlexGroup
Tamanho máximo do arquivo do datastore	62 TB	62 TB	62 TB	62TB com ONTAP 9.12.1P2 e posterior
Profundidade de fila ideal por LUN ou sistema de ficheiros	64-256	64-256	Negociação automática	Consulte NFS.MaxQueueDepth em "Host ESXi recomendado e outras configurações do ONTAP".

A tabela a seguir lista as funcionalidades relacionadas ao armazenamento VMware suportadas.

Capacidade/recurso	FC	ISCSI	NVMe-of	NFS
VMotion	Sim	Sim	Sim	Sim
Storage vMotion	Sim	Sim	Sim	Sim
VMware HA	Sim	Sim	Sim	Sim
Storage Distributed Resource Scheduler (SDRS)	Sim	Sim	Sim	Sim
Software de backup habilitado para VMware vStorage APIs for Data Protection (VADP)	Sim	Sim	Sim	Sim

Capacidade/recurso	FC	ISCSI	NVMe-of	NFS
Microsoft Cluster Service (MSCS) ou cluster de failover em uma VM	Sim	Sim 1	Sim 1	Não suportado
Tolerância de falhas	Sim	Sim	Sim	Sim
Live Site Recovery/Site Recovery Manager	Sim	Sim	2	V3 apenas 2
VMs com thin Provisioning (discos virtuais)	Sim	Sim	Sim	Sim esta configuração é o padrão para todas as VMs no NFS quando não estiver usando o VAAI.
Multipathing nativo da VMware	Sim	Sim	Sim	O entroncamento de sessão NFS v4,1 requer ONTAP 9.14,1 e posterior

A tabela a seguir lista os recursos de gerenciamento de armazenamento ONTAP compatíveis.

Capacidade/funcionalidade	FC	ISCSI	NVMe-of	NFS
Deduplicação de dados	Economia no array	Economia no array	Economia no array	Economia no datastore
Thin Provisioning	Datastore ou RDM	Datastore ou RDM	Armazenamento de dados	Armazenamento de dados
Redimensione o datastore	Cresça apenas	Cresça apenas	Cresça apenas	Crescer, crescer com crescimento automático e diminuir
Plug-ins do SnapCenter para Windows, aplicações Linux (no convidado)	Sim	Sim	Sim	Sim
Monitoramento e configuração de host usando as ferramentas do ONTAP para VMware vSphere	Sim	Sim	Sim	Sim

Capacidade/funcionalidade	FC	ISCSI	NVMe-of	NFS
Provisionamento usando as ferramentas do ONTAP para VMware vSphere	Sim	Sim	Sim	Sim

A tabela a seguir lista os recursos de backup suportados.

Capacidade/funcionalidade	FC	ISCSI	NVMe-of	NFS
Instantâneos do ONTAP	Sim	Sim	Sim	Sim
SRM suportado por backups replicados	Sim	Sim	2	V3 apenas 2
Volume SnapMirror	Sim	Sim	Sim	Sim
Acesso à imagem VMDK	Software de backup habilitado para SnapCenter e VADP	Software de backup habilitado para SnapCenter e VADP	Software de backup habilitado para SnapCenter e VADP	Software de backup habilitado para SnapCenter e VADP, vSphere Client e vSphere Web Client datastore browser
Acesso ao nível do arquivo VMDK	Software de backup habilitado para SnapCenter e VADP, somente Windows	Software de backup habilitado para SnapCenter e VADP, somente Windows	Software de backup habilitado para SnapCenter e VADP, somente Windows	Software de backup habilitado para SnapCenter e VADP e aplicativos de terceiros
Granularidade NDMP	Armazenamento de dados	Armazenamento de dados	Armazenamento de dados	Datastore ou VM

[1] **NetApp recomenda** usar iSCSI in-guest para clusters Microsoft em vez de VMDKs com multiwriter habilitado em um datastore VMFS. Essa abordagem é totalmente suportada pela Microsoft e VMware, oferece grande flexibilidade com ONTAP (SnapMirror para sistemas ONTAP locais ou na nuvem), é fácil de configurar e automatizar, e pode ser protegida com SnapCenter. vSphere 7 adiciona uma nova opção de VMDK em cluster. Isso é diferente dos VMDKs com multiwriter habilitado, que exigem um datastore VMFS 6 com suporte a VMDK em cluster habilitado. Outras restrições se aplicam. Consulte a documentação da VMware "Configuração para Cluster de failover do Windows Server" para diretrizes de configuração.

2 os armazenamentos de dados usando NVMe-of e NFS v4,1 exigem replicação do vSphere. A replicação baseada em array para NFS v4,1 não é atualmente suportada pelo SRM. Atualmente, a replicação baseada em array com NVMe-of não é compatível com as ferramentas do ONTAP para o adaptador de replicação de armazenamento (SRA) do VMware vSphere.

Selecionar um protocolo de armazenamento

Os sistemas que executam ONTAP suportam todos os principais protocolos de storage, para que os clientes possam escolher o que é melhor para seu ambiente, dependendo da infraestrutura de rede existente e planejada e das habilidades da equipe. Historicamente, os testes da NetApp geralmente mostraram pouca

diferença entre protocolos executados em velocidades de linha e números de conexões semelhantes. No entanto, o NVMe-oF (NVMe/TCP e NVMe/FC) apresenta ganhos notáveis em IOPS, redução na latência e até 50% ou mais de redução no consumo de CPU do host pela IO de storage. Na outra extremidade do espectro, NFS oferece a maior flexibilidade e facilidade de gerenciamento, especialmente para grandes quantidades de VMs. Todos esses protocolos podem ser usados e gerenciados com ONTAP tools for VMware vSphere, que fornece uma interface simples para criar e gerenciar datastores.

Os seguintes fatores podem ser úteis para considerar uma escolha de protocolo:

- * Ambiente operacional atual.* Embora as equipes DE TI geralmente sejam qualificadas para gerenciar a infraestrutura Ethernet IP, nem todas elas são qualificadas para gerenciar uma malha FC SAN. No entanto, usar uma rede IP de uso geral que não foi projetada para o tráfego de armazenamento pode não funcionar bem. Considere a infraestrutura de rede que você tem em vigor, quaisquer melhorias planejadas e as habilidades e disponibilidade da equipe para gerenciá-los.
- * Facilidade de configuração.* Além da configuração inicial da malha FC (switches e cabeamento adicionais, zoneamento e verificação de interoperabilidade de HBA e firmware), os protocolos de bloco também exigem criação e mapeamento de LUNs e descoberta e formatação pelo SO convidado. Depois que os volumes NFS são criados e exportados, eles são montados pelo host ESXi e prontos para uso. O NFS não tem nenhuma qualificação especial de hardware ou firmware para gerenciar.
- **Facilidade de gerenciamento.** Com protocolos SAN, se for necessário mais espaço, várias etapas são necessárias, incluindo expandir um LUN, realizar uma nova varredura para descobrir o novo tamanho e, em seguida, expandir o sistema de arquivos. Embora seja possível expandir um LUN, não é possível reduzir o tamanho de um LUN. NFS permite redimensionar facilmente para cima ou para baixo, e esse redimensionamento pode ser automatizado pelo sistema de storage. SAN oferece exigência de espaço por meio dos comandos DEALLOCATE/TRIM/UNMAP do sistema operacional convidado, permitindo que o espaço de arquivos excluídos seja devolvido ao array. Esse tipo de exigência de espaço não é possível com datastores NFS.
- **Transparência do espaço de armazenamento.** A utilização do storage geralmente é mais fácil de ver em ambientes NFS porque o thin Provisioning devolve economia imediatamente. Da mesma forma, a economia de deduplicação e clonagem ficam imediatamente disponíveis para outras VMs no mesmo armazenamento de dados ou para outros volumes do sistema de storage. Normalmente, a densidade da VM também é maior em um armazenamento de dados NFS, o que pode melhorar a economia de deduplicação e reduzir os custos de gerenciamento com menos armazenamentos de dados para gerenciar.

Layout do datastore

Os sistemas de storage ONTAP oferecem grande flexibilidade na criação de datastores para VMs e discos virtuais. Embora muitas práticas recomendadas do ONTAP sejam aplicadas ao usar as ferramentas do ONTAP para provisionar armazenamentos de dados para o vSphere (listadas na "Host ESXi recomendado e outras configurações do ONTAP"seção), veja algumas diretrizes adicionais a serem consideradas:

- A implementação de vSphere com datastores NFS do ONTAP resulta em uma solução de alto desempenho e fácil de gerenciar, que oferece proporções de VM por datastore que não podem ser obtidas com protocolos de storage baseado em blocos. Essa arquitetura pode resultar em um aumento de dez vezes na densidade de datastores, com uma redução correspondente no número de datastores. Embora um datastore maior possa beneficiar a eficiência de storage e proporcionar vantagens operacionais, considere usar pelo menos quatro datastores (FlexVol volumes) por nó para armazenar suas VMs em um único controlador ONTAP, a fim de obter o máximo desempenho dos recursos de hardware. Essa abordagem também permite estabelecer datastores com diferentes políticas de recuperação. Alguns podem ser copiados ou replicados com mais frequência do que outros, com base nas necessidades do negócio. Vários datastores não são necessários com FlexGroup volumes para desempenho, pois eles são escaláveis por design.

- **NetApp recomenda** o uso de volumes FlexVol para a maioria dos datastores NFS. A partir do ONTAP 9.8, volumes FlexGroup também são suportados para uso como datastores e geralmente são recomendados para determinados casos de uso. Outros containers de storage ONTAP, como qtrees, geralmente não são recomendados porque atualmente não são suportados nem pelas ONTAP tools for VMware vSphere nem pelo plug-in NetApp SnapCenter para VMware vSphere.
- Um bom tamanho para um datastore FlexVol volume é de cerca de 4TB a 8TB. Esse tamanho é um bom ponto de equilíbrio para performance, facilidade de gerenciamento e proteção de dados. Comece pequeno (digamos, 4TB) e cresça o datastore conforme necessário (até o máximo de 300TB). Armazenamentos de dados menores são mais rápidos para se recuperar do backup ou após um desastre e podem ser movidos rapidamente pelo cluster. Considere o uso do dimensionamento automático do ONTAP para aumentar e diminuir automaticamente o volume conforme o espaço usado muda. As ferramentas do ONTAP para o Assistente de provisionamento de datastore do VMware vSphere usam o dimensionamento automático por padrão para novos datastores. A personalização adicional dos limites de crescimento e redução e o tamanho máximo e mínimo podem ser feitos com o System Manager ou com a linha de comando.
- Como alternativa, armazenamentos de dados VMFS podem ser configurados com LUNs ou namespaces NVMe (chamados de unidades de storage em novos sistemas ASA) acessados por FC, iSCSI, NVMe/FC ou NVMe/TCP. O VMFS permite que armazenamentos de dados sejam acessados simultaneamente por cada servidor ESX em um cluster. Os armazenamentos de dados VMFS podem ter até 64TB TB de tamanho e consistem em até 32 2TB LUNs (VMFS 3) ou um único LUN 64TB (VMFS 5). O tamanho máximo de LUN do ONTAP é de 128TB GB em sistemas AFF, ASA e FAS. O NetApp sempre recomenda o uso de um único LUN grande para cada datastore, em vez de tentar usar extensões. Assim como o NFS, considere o uso de vários armazenamentos de dados (volumes ou unidades de storage) para maximizar a performance em uma única controladora ONTAP.
- Os sistemas operacionais Guest (SO) mais antigos precisavam de alinhamento com o sistema de storage para obter o melhor desempenho e eficiência de storage. No entanto, os sistemas operacionais modernos suportados por fornecedores de distribuidores Microsoft e Linux, como a Red Hat, não precisam mais de ajustes para alinhar a partição do sistema de arquivos com os blocos do sistema de armazenamento subjacente em um ambiente virtual. Se você estiver usando um sistema operacional antigo que pode exigir alinhamento, procure na base de conhecimento de suporte da NetApp artigos usando "alinhamento de VM" ou solicite uma cópia do TR-3747 de um Contato de vendas ou parceiro da NetApp.
- Evite o uso de utilitários de desfragmentação no sistema operacional convidado, pois isso não oferece nenhum benefício de desempenho e afeta a eficiência de armazenamento e o uso de espaço instantâneo. Considere também desativar a indexação de pesquisa no SO convidado para desktops virtuais.
- A ONTAP liderou o setor com recursos de eficiência de storage inovadores, permitindo que você aproveite ao máximo seu espaço em disco utilizável. Os sistemas AFF levam essa eficiência ainda mais longe com a deduplicação e a compactação in-line padrão. Os dados são deduplicados em todos os volumes de um agregado. Portanto, você não precisa mais agrupar sistemas operacionais semelhantes e aplicativos semelhantes em um único datastore para maximizar a economia.
- Em alguns casos, talvez você nem precise de um datastore. Considere sistemas de arquivos de propriedade de hóspedes, como sistemas de arquivos NFS, SMB, NVMe/TCP ou iSCSI gerenciados pelo convidado. Para obter orientações específicas sobre aplicações, consulte relatórios técnicos da NetApp para a sua aplicação. Por exemplo, "Bancos de dados Oracle no ONTAP" tem uma seção sobre virtualização com detalhes úteis.
- Os discos de primeira classe (ou discos virtuais aprimorados) permitem discos gerenciados pelo vCenter, independentemente de uma VM com o vSphere 6,5 e posterior. Embora gerenciados principalmente pela API, eles podem ser úteis com o vVols, especialmente quando gerenciados por ferramentas OpenStack ou Kubernetes. Eles são suportados pelo ONTAP, bem como pelas ferramentas do ONTAP para VMware vSphere.

Migração de datastore e VM

Ao migrar VMs de um datastore existente em outro sistema de storage para o ONTAP, veja algumas práticas a serem lembradas:

- Use o Storage vMotion para mover o volume de suas máquinas virtuais para o ONTAP. Essa abordagem não só não causa interrupções às VMs em execução, como também permite que recursos de eficiência de storage da ONTAP, como deduplicação e compactação, processem os dados à medida que migram. Considere usar os recursos do vCenter para selecionar várias VMs da lista de inventário e, em seguida, agendar a migração (use a tecla Ctrl enquanto clica em ações) em um momento apropriado.
- Embora seja possível planejar cuidadosamente uma migração para datastores de destino apropriados, geralmente é mais simples migrar em massa e organizar posteriormente conforme necessário. Você pode querer usar essa abordagem para orientar sua migração para diferentes datastores se tiver necessidades específicas de proteção de dados, como diferentes agendamentos de Snapshot. Além disso, uma vez que as VMs estejam no cluster NetApp, o storage vMotion pode usar offloads VAAI para mover VMs entre datastores no cluster sem exigir uma cópia baseada no host. Observe que o NFS não realiza o offload do storage vMotion de VMs ligadas; no entanto, o VMFS realiza.
- As máquinas virtuais que precisam de uma migração mais cuidadosa incluem bancos de dados e aplicativos que usam armazenamento anexado. Em geral, considere o uso das ferramentas do aplicativo para gerenciar a migração. Para Oracle, considere usar ferramentas Oracle como RMAN ou ASM para migrar os arquivos do banco de dados. Consulte "Migração de bancos de dados Oracle para sistemas de storage ONTAP" para obter mais informações. Da mesma forma, para o SQL Server, considere usar ferramentas do SQL Server Management Studio ou do NetApp, como o SnapManager para SQL Server ou SnapCenter.

Ferramentas do ONTAP para VMware vSphere

A prática recomendada mais importante ao usar vSphere com sistemas executando ONTAP é instalar e usar o ONTAP tools for VMware vSphere plug-in (anteriormente conhecido como Virtual Storage Console). Este vCenter plug-in simplifica o gerenciamento de storage, aumenta a disponibilidade e reduz os custos de storage e a sobrecarga operacional, seja usando SAN ou NAS, em ASA, AFF, FAS ou até mesmo ONTAP Select (uma versão definida por software do ONTAP executada em uma VM VMware ou KVM). Ele utiliza as melhores práticas para o provisionamento de datastores e otimiza as configurações do host ESXi para multipath e timeouts de HBA (estes são descritos no Apêndice B). Por ser um vCenter plug-in, está disponível para todos os clientes web vSphere que se conectam ao servidor vCenter.

O plug-in também ajuda a usar outras ferramentas do ONTAP em ambientes vSphere. Ele permite instalar o plug-in NFS para VMware VAAI, que permite descarga de cópia para o ONTAP para operações de clonagem de VM, reserva de espaço para arquivos de disco virtual espessos e descarga de snapshot ONTAP.

> Em clusters baseados em imagem vSphere, você ainda vai querer adicionar o NFS plug-in à sua imagem para que eles não fiquem fora de conformidade quando você o instalar com ONTAP tools.

As ferramentas do ONTAP também são a interface de gerenciamento para muitas funções do provedor VASA para ONTAP, oferecendo suporte ao gerenciamento baseado em políticas de storage com vVols.

Em geral, **a NetApp recomenda** o uso das ferramentas do ONTAP para a interface do VMware vSphere no vCenter para provisionar armazenamentos de dados tradicionais e vVols para garantir que as práticas recomendadas sejam seguidas.

Rede geral

Configurar as definições de rede ao utilizar vSphere com sistemas que executam ONTAP é simples e semelhante a outras configurações de rede. Aqui estão alguns pontos a considerar:

- Separe o tráfego de rede de armazenamento de outras redes. Uma rede separada pode ser obtida usando uma VLAN dedicada ou switches separados para armazenamento. Se a rede de armazenamento partilhar caminhos físicos, como uplinks, poderá necessitar de portas de QoS ou uplink adicionais para garantir uma largura de banda suficiente. Não conete os hosts diretamente ao storage; use os switches para ter caminhos redundantes e permitir que o VMware HA funcione sem intervenção. "Ligação direta em rede"Consulte para obter informações adicionais.
- Os frames grandes podem ser usados se desejado e suportados pela sua rede, especialmente ao usar iSCSI. Se forem usados, certifique-se de que estejam configurados de forma idêntica em todos os dispositivos de rede, VLANs e assim por diante no caminho entre o armazenamento e o host ESXi. Caso contrário, você pode ver problemas de desempenho ou conexão. A MTU também deve ser definida de forma idêntica no switch virtual ESXi, na porta VMkernel e também nas portas físicas ou grupos de interface de cada nó ONTAP.
- O NetApp recomenda apenas desativar o controle de fluxo de rede nas portas de interconexão de cluster dentro de um cluster ONTAP. O NetApp não faz outras recomendações sobre as práticas recomendadas para as portas de rede restantes usadas para tráfego de dados. Você deve ativar ou desativar conforme necessário. "TR-4182"Consulte para obter mais informações sobre o controlo de fluxo.
- Quando os storages ESXi e ONTAP estão conetados a redes de armazenamento Ethernet, **a NetApp recomenda** configurar as portas Ethernet às quais esses sistemas se conetam como portas de borda de protocolo de árvore de expansão rápida (RSTP) ou usando o recurso Cisco PortFast. **A NetApp recomenda** ativar o recurso de tronco de porta de árvore de expansão rápida em ambientes que usam o recurso Cisco PortFast e que têm entroncamento de VLAN 802,1Q habilitado para o servidor ESXi ou os storages ONTAP.
- **A NetApp recomenda** as seguintes práticas recomendadas para agregação de links:
  - Utilize switches que suportam agregação de links de portas em dois chassis de switch separados usando uma abordagem de grupo de agregação de links multi-chassi, como o Virtual PortChannel (vPC) da Cisco.
  - Desative o LACP para portas de switch conetadas ao ESXi a menos que você esteja usando dvSwitches 5,1 ou posterior com o LACP configurado.
  - Use o LACP para criar agregados de link para sistemas de storage ONTAP com grupos de interface multimodo dinâmico com hash de porta ou IP. "Gerenciamento de rede"Consulte para obter mais orientações.
  - Use uma política de agrupamento de hash IP no ESXi ao usar agregação de link estático (por exemplo, EtherChannel) e vSwitches padrão ou agregação de link baseada em LACP com switches distribuídos vSphere. Se a agregação de links não for usada, use "Rota baseada no ID de porta virtual de origem".

SAN (FC, FCoE, NVMe/FC, iSCSI), RDM

No vSphere, há quatro maneiras de usar dispositivos de armazenamento em bloco:

- Com datastores VMFS
- Com mapeamento de dispositivo bruto (RDM)
- Como um LUN conetado iSCSI ou namespace NVMe/TCP acessado e controlado por um iniciador de software de um sistema operacional convidado VM

- Como um datastore vVols

O VMFS é um sistema de arquivos em cluster de alto desempenho que fornece datastores que são pools de armazenamento compartilhado. Armazenamentos de dados VMFS podem ser configurados com LUNs acessados usando FC, iSCSI, FCoE ou namespaces NVMe acessados usando os protocolos NVMe/FC ou NVMe/TCP. O VMFS permite que o armazenamento seja acessado simultaneamente por cada servidor ESX em um cluster. O tamanho máximo de LUN é geralmente 128TB, começando com ONTAP 9.12.1P2 (e anterior com sistemas ASA); portanto, um datastore VMFS 5 ou 6 de tamanho máximo de 64TB pode ser criado usando um único LUN.

As extensões são um conceito de armazenamento do vSphere pelo qual você pode "unir" vários LUNs para criar um único armazenamento de dados maior. Você nunca deve usar extensões para alcançar o tamanho desejado do datastore. Um único LUN é a melhor prática para um datastore VMFS.

O vSphere inclui suporte integrado para vários caminhos para dispositivos de armazenamento. O vSphere pode detetar o tipo de dispositivo de armazenamento para sistemas de armazenamento suportados e configurar automaticamente a pilha de multipathing para suportar os recursos do sistema de armazenamento em uso, regarldess do protocolo usado ou se estiver usando ASA, AFF, FAS ou ONTAP definido por software.

Tanto o vSphere quanto o ONTAP dão suporte ao Asymmetric Logical Unit Access (ALUA) para estabelecer caminhos ativos/otimizados e ativos/não otimizados para Fibre Channel e iSCSI, além de acesso a namespace assimétrico (ANA) para namespaces NVMe usando NVMe/FC e NVMe/TCP. No ONTAP, um caminho otimizado para ALUA ou ANA segue um caminho de dados direto, usando uma porta de destino no nó que hospeda o LUN ou namespace que está sendo acessado. O ALUA/ANA é ativado por padrão no vSphere e no ONTAP. O software multipathing no vSphere reconhece o cluster ONTAP como ALUA ou ANA e usa o plug-in nativo apropriado com a política de balanceamento de carga round robin.

Com os sistemas ASA do NetApp, os LUNs e namespaces são apresentados aos hosts ESXi com pathing simétrico. O que significa que todos os caminhos estão ativos e otimizados. O software multipathing no vSphere reconhece o sistema ASA como simétrico e usa o plug-in nativo apropriado com a política de balanceamento de carga round robin.

"Host ESXi recomendado e outras configurações do ONTAP"Consulte para obter as definições de multipathing otimizadas.

O ESXi não vê LUNs, namespaces ou caminhos além de seus limites. Em um cluster ONTAP maior, é possível alcançar o limite de caminho antes do limite de LUN. Para lidar com essa limitação, o ONTAP oferece suporte ao mapa de LUN seletivo (SLM) na versão 8,3 e posterior.

Consulte a "Ferramenta VMware Configuration Maximums"para obter os limites suportados mais atualizados no ESXi.

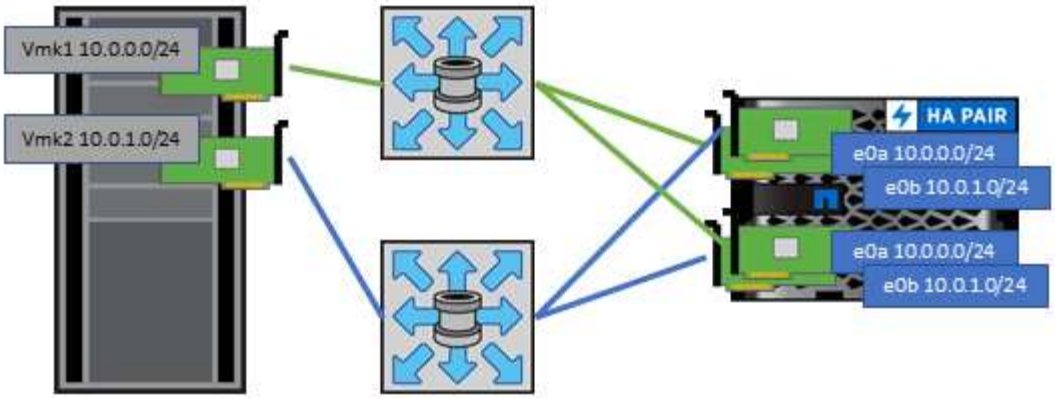
O SLM limita os nós que anunciam caminhos para um determinado LUN. É uma prática recomendada do NetApp ter pelo menos dois LIFs por nó e por SVM e usar o SLM para limitar os caminhos anunciados para o nó que hospeda o LUN e seu parceiro de HA. Embora existam outros caminhos, eles não são anunciados por padrão. É possível modificar os caminhos anunciados com os argumentos adicionar e remover nó de relatório dentro do SLM. Observe que os LUNs criados em versões anteriores ao 8,3 anunciam todos os caminhos e precisam ser modificados para anunciar apenas os caminhos para o par de HA de hospedagem. Para obter mais informações sobre o SLM, consulte a seção 5,9 do "TR-4080". O método anterior de portsets também pode ser usado para reduzir ainda mais os caminhos disponíveis para um LUN. Os Portsets ajudam reduzindo o número de caminhos visíveis através dos quais os iniciadores em um iggroup podem ver LUNs.

- O SLM está ativado por predefinição. A menos que você esteja usando portsets, nenhuma configuração adicional é necessária.
- Para LUNs criadas antes do Data ONTAP 8.3, aplique manualmente o SLM executando o `lun mapping remove-reporting-nodes` comando para remover os nós de relatórios de LUN e restringir o acesso LUN ao nó proprietário de LUN e ao seu parceiro de HA.

Os protocolos de bloco baseados em SCSI (iSCSI, FC e FCoE) acessam LUNs usando IDs de LUN e números de série, juntamente com nomes exclusivos. FC e FCoE usam nomes mundiais (WWNNs e WWPNs) e iSCSI usa nomes qualificados iSCSI (IQNs) para estabelecer caminhos com base em mapeamentos de LUN para agrupar filtrados por portsets e SLM. Os protocolos de bloco baseados em NVMe são gerenciados atribuindo o namespace com um ID de namespace gerado automaticamente a um subsistema NVMe e mapeando esse subsistema para o nome qualificado do NVMe (NQN) do(s) host(s). Independentemente do FC ou TCP, os namespaces NVMe são mapeados usando o NQN e não o WWPN ou WWNN. O host então cria um controlador definido por software para que o subsistema mapeado acesse seus namespaces. O caminho para LUNs e namespaces dentro do ONTAP não tem sentido para os protocolos de bloco e não é apresentado em nenhum lugar do protocolo. Portanto, um volume que contém apenas LUNs não precisa ser montado internamente, e um caminho de junção não é necessário para volumes que contêm LUNs usados em datastores.

Outras práticas recomendadas a considerar:

- Verifique "Host ESXi recomendado e outras configurações do ONTAP"as configurações recomendadas pelo NetApp em colaboração com a VMware.
- Certifique-se de que é criada uma interface lógica (LIF) para cada SVM em cada nó no cluster do ONTAP para obter disponibilidade e mobilidade máximas. A prática recomendada de SAN ONTAP é usar duas portas físicas e LIFs por nó, uma para cada malha. O ALUA é usado para analisar caminhos e identificar caminhos otimizados ativos (diretos) versus caminhos não otimizados ativos. O ALUA é usado para FC, FCoE e iSCSI.
- Para redes iSCSI, use várias interfaces de rede VMkernel em sub-redes de rede diferentes com agrupamento NIC quando vários switches virtuais estiverem presentes. Você também pode usar várias NICs físicas conetadas a vários switches físicos para fornecer HA e maior taxa de transferência. A figura a seguir fornece um exemplo de conectividade multipath. No ONTAP, configure um grupo de interface de modo único para failover com dois ou mais links conetados a dois ou mais switches ou use LACP ou outra tecnologia de agregação de links com grupos de interface multimodo para fornecer HA e os benefícios da agregação de links.
- Se o CHAP (Challenge-Handshake Authentication Protocol) for usado no ESXi para autenticação de destino, ele também deve ser configurado no ONTAP usando a CLI (`vserver iscsi security create`) ou com o Gerenciador de sistema (edite a segurança do iniciador em armazenamento > SVMs > Configurações da SVM > Protocolos > iSCSI).
- Use as ferramentas do ONTAP para o VMware vSphere para criar e gerenciar LUNs e grupos de pessoas. O plug-in determina automaticamente as WWPNs de servidores e cria grupos apropriados. Ele também configura LUNs de acordo com as melhores práticas e os mapeia para os grupos corretos.
- Use RDMs com cuidado porque eles podem ser mais difíceis de gerenciar e também usam caminhos, que são limitados como descrito anteriormente. Os LUNs ONTAP suportam ambos "modo de compatibilidade física e virtual" os RDMs.
- Para saber mais sobre como usar o NVMe/FC com o vSphere 7,0, consulte este "Guia de configuração de host ONTAP NVMe/FC" e "TR-4684".a figura a seguir mostra a conectividade multipath de um host vSphere para um LUN ONTAP.



NFS

O ONTAP é, entre muitas outras coisas, um array nas com escalabilidade horizontal de classe empresarial. O ONTAP capacita o VMware vSphere com acesso simultâneo a datastores conectados a NFS de muitos hosts ESXi, excedendo muito os limites impostos aos sistemas de arquivos VMFS. O uso do NFS com o vSphere oferece alguns benefícios de visibilidade da eficiência de storage e facilidade de uso, como mencionado na "armazenamentos de dados"seção.

As práticas recomendadas a seguir são recomendadas ao usar o ONTAP NFS com vSphere:

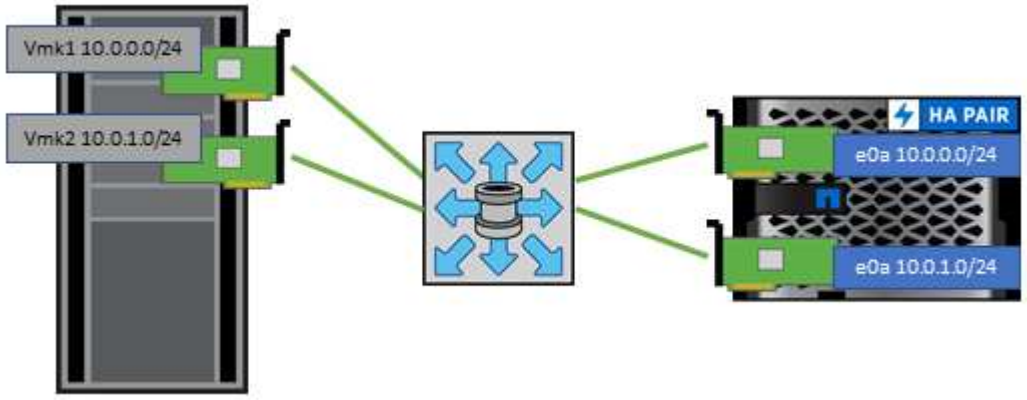
- Use as ferramentas do ONTAP para VMware vSphere (a prática recomendada mais importante):
  - Use as ferramentas do ONTAP para o VMware vSphere para provisionar armazenamentos de dados porque ele simplifica o gerenciamento de políticas de exportação automaticamente.
  - Ao criar datastores para clusters VMware com o plug-in, selecione o cluster em vez de um único servidor ESX. Essa opção o aciona para montar automaticamente o datastore em todos os hosts do cluster.
  - Use a função de montagem de plug-in para aplicar datastores existentes a novos servidores.
  - Quando não estiver usando as ferramentas do ONTAP para VMware vSphere, use uma única política de exportação para todos os servidores ou para cada cluster de servidores onde é necessário controle de acesso adicional.
- Use uma única interface lógica (LIF) para cada SVM em cada nó no cluster do ONTAP. As recomendações anteriores de um LIF por datastore não são mais necessárias. Embora o acesso direto (LIF e datastore no mesmo nó) seja o melhor, não se preocupe com o acesso indireto porque o efeito de desempenho geralmente é mínimo (microssegundos).
- Se você usar o fpolicy, certifique-se de excluir arquivos .lck, pois eles são usados pelo vSphere para bloquear sempre que uma VM é ligada.
- Todas as versões do VMware vSphere com suporte no momento podem usar o NFS v3 e o v4,1. O suporte oficial para nconnect foi adicionado ao vSphere 8,0 update 2 for NFS v3 e à atualização 3 for NFS v4,1. Para o NFS v4,1, o vSphere continua a oferecer suporte ao entroncamento de sessão, autenticação Kerberos e autenticação Kerberos com integridade. É importante notar que o entroncamento de sessão requer o ONTAP 9.14,1 ou uma versão posterior. Você pode saber mais sobre o recurso nconnect e como ele melhora o desempenho em "NFSv3 nconnect recurso com NetApp e VMware".

- O valor máximo para nconnect no vSphere 8 é 4 e o valor padrão é 1. O limite máximo de valor no vSphere pode ser aumentado em uma base por host por meio de configurações avançadas, no entanto, geralmente não é necessário.
- Um valor de 4 é recomendado para ambientes que exigem mais desempenho do que uma única conexão TCP pode fornecer.
- Esteja ciente de que o ESXi tem um limite de 256 conexões NFS e cada conexão nconnect conta para esse total. Por exemplo, dois datastores com nconnect 4 contariam como oito conexões totais.
- É importante testar o impacto no desempenho do nconnect no seu ambiente antes de implementar mudanças em grande escala em ambientes de produção.

- Vale a pena notar que NFSv3 e NFSv4,1 usam diferentes mecanismos de bloqueio. O NFSv3 usa o bloqueio do lado do cliente, enquanto o NFSv4,1 usa o bloqueio do lado do servidor. Embora um volume ONTAP possa ser exportado através de ambos os protocolos, o ESXi pode montar apenas um datastore através de um protocolo. No entanto, isso não significa que outros hosts ESXi não possam montar o mesmo datastore através de uma versão diferente. Para evitar quaisquer problemas, é essencial especificar a versão do protocolo a ser usada durante a montagem, garantindo que todos os hosts usem a mesma versão e, portanto, o mesmo estilo de bloqueio. É essencial evitar misturar versões NFS entre hosts. Se possível, use perfis de host para verificar a conformidade.
  - Como não há conversão automática de datastore entre NFSv3 e NFSv4,1, crie um novo datastore NFSv4,1 e use o Storage vMotion para migrar VMs para o novo datastore.
  - Consulte as notas da tabela de interoperabilidade NFS v4,1 no "Ferramenta de Matriz de interoperabilidade do NetApp" para obter os níveis de patch ESXi específicos necessários para suporte.
- Como mencionado no "definições", se você não estiver usando o vSphere CSI for Kubernetes, você deve definir o newSyncInterval per "VMware KB 386364"
- As regras de política de exportação de NFS são usadas para controlar o acesso pelos hosts vSphere. Você pode usar uma diretiva com vários volumes (datastores). Com o NFS, o ESXi usa o estilo de segurança sys (UNIX) e requer a opção de montagem raiz para executar VMs. No ONTAP, essa opção é chamada de superusuário e, quando a opção superusuário é usada, não é necessário especificar o ID de usuário anônimo. Observe que regras de política de exportação com valores diferentes `-anon` e `-allow -suid` podem causar problemas de descoberta de SVM com ferramentas do ONTAP. Os endereços IP devem ser uma lista separada por vírgulas sem espaços dos endereços de porta vmkernel que montam os datastores. Aqui está uma regra de política de exemplo:
  - Protocolo de acesso: nfs (que inclui nfs3 e nfs4)
  - Lista de nomes de host de correspondência de cliente, endereços IP, Netgroups ou domínios: 192.168.42.21,192.168.42.22
  - Regra de Acesso RO: Qualquer
  - Regra de Acesso RW: Qualquer
  - ID de usuário para o qual usuários anônimos são mapeados: 65534
  - Tipos de segurança do superusuário: Qualquer
  - Honra setuid bits em SETATTR: True
  - Permitir a criação de dispositivos: Verdadeiro
- Se o plug-in NFS NetApp for usado, o protocolo deve ser definido como `nfs` quando a regra de política de exportação for criada ou modificada. O protocolo NFSv4 é necessário para que a descarga de cópia VAAI funcione, e especificar o protocolo como `nfs` inclui automaticamente as versões NFSv3 e NFSv4. Isso é

necessário mesmo que o tipo de armazenamento de dados seja criado como NFS v3.

- Os volumes do armazenamento de dados NFS são juntados do volume raiz do SVM. Portanto, o ESXi também precisa ter acesso ao volume raiz para navegar e montar volumes do armazenamento de dados. A política de exportação para o volume raiz e para quaisquer outros volumes em que a junção do volume do datastore esteja aninhada, deve incluir uma regra ou regras para os servidores ESXi concedendo acesso somente leitura. Aqui está uma política de exemplo para o volume raiz, também usando o plug-in VAAI:
  - Protocolo de acesso: nfs
  - Especificação correspondência Cliente: 192.168.42.21,192.168.42.22
  - Regra de Acesso RO: Sys
  - Regra de acesso RW: Nunca (melhor segurança para o volume raiz)
  - UID anónimo
  - Superusuário: Sys (também necessário para o volume raiz com VAAI)
- Embora o ONTAP ofereça uma estrutura de namespace de volume flexível para organizar volumes em uma árvore usando junções, essa abordagem não tem valor para o vSphere. Ele cria um diretório para cada VM na raiz do datastore, independentemente da hierarquia do namespace do storage. Assim, a prática recomendada é simplesmente montar o caminho de junção para volumes para vSphere no volume raiz do SVM, que é como as ferramentas do ONTAP para VMware vSphere provisionam datastores. Não ter caminhos de junção aninhados também significa que nenhum volume é dependente de qualquer volume que não seja o volume raiz e que tirar um volume off-line ou destruí-lo, mesmo intencionalmente, não afeta o caminho para outros volumes.
- Um tamanho de bloco de 4K é bom para partições NTFS em datastores NFS. A figura a seguir mostra a conectividade de um host vSphere para um datastore ONTAP NFS.



A tabela a seguir lista as versões de NFS e os recursos compatíveis.

Recursos do vSphere	NFSv3	NFSv4.1
VMotion e Storage vMotion	Sim	Sim
Alta disponibilidade	Sim	Sim
Tolerância de falhas	Sim	Sim
DRS	Sim	Sim
Perfis de host	Sim	Sim
Armazenamento DRS	Sim	Não

Recursos do vSphere	NFSv3	NFSv4.1
Controle de e/S de storage	Sim	Não
SRM	Sim	Não
Volumes virtuais	Sim	Não
Aceleração de hardware (VAAI)	Sim	Sim
Autenticação Kerberos	Não	Sim (aprimorado com o vSphere 6,5 e posterior para oferecer suporte a AES, krb5i)
Suporte multipathing	Não	Sim (ONTAP 9.14,1)

Volumes FlexGroup

Use o ONTAP e o FlexGroup volumes com o VMware vSphere para armazenamentos de dados simples e dimensionáveis que aproveitam todo o poder de um cluster ONTAP inteiro.

O ONTAP 9,8, juntamente com as ferramentas do ONTAP para VMware vSphere 9,8-9,13 e o plug-in SnapCenter para VMware 4,4 e versões mais recentes, adicionou suporte para datastores com suporte de volume FlexGroup no vSphere. O FlexGroup volumes simplifica a criação de grandes armazenamentos de dados e cria automaticamente os volumes constituintes distribuídos necessários no cluster do ONTAP para obter o máximo de desempenho a partir de um sistema ONTAP.

Use o FlexGroup volumes com vSphere se você precisar de um único armazenamento de dados dimensionável vSphere com o poder de um cluster ONTAP completo ou se você tiver workloads de clonagem muito grandes que podem se beneficiar do mecanismo de clonagem do FlexGroup mantendo o cache clone aquecido constantemente.

Descarga de cópia

Além de testes extensivos do sistema com cargas de trabalho do vSphere, o ONTAP 9.8 adicionou um novo mecanismo de descarga de cópia para datastores FlexGroup. Este novo sistema usa um mecanismo de cópia melhorado para replicar arquivos entre constituintes em segundo plano, permitindo o acesso à origem e ao destino. Esse cache constituinte-local é então usado para instanciar rapidamente clones da VM sob demanda.

Para ativar a descarga de cópia otimizada do FlexGroup, consulte "Como configurar volumes ONTAP FlexGroup para permitir descarga de cópia VAAI"

É possível que, se você usar a clonagem do VAAI, mas não clonar o suficiente para manter o cache aquecido, seus clones podem não ser mais rápidos do que uma cópia baseada em host. Se for esse o caso, você pode ajustar o tempo limite do cache para melhor atender às suas necessidades.

Considere o seguinte cenário:

- Você criou um novo FlexGroup com 8 constituintes
- O tempo limite do cache para o novo FlexGroup é definido para 160 minutos

Nesse cenário, os primeiros 8 clones a serem concluídos serão cópias completas, não clones de arquivos locais. Qualquer clonagem adicional dessa VM antes que o tempo limite de 160 segundos expire usará o mecanismo de clone de arquivo dentro de cada constituinte de uma forma round-robin para criar cópias quase imediatas distribuídas uniformemente pelos volumes constituintes.

Cada novo trabalho clone que um volume recebe repõe o tempo limite. Se um volume constituinte no exemplo FlexGroup não receber uma solicitação de clone antes do tempo limite, o cache para essa VM específica será limpo e o volume precisará ser preenchido novamente. Além disso, se a origem do clone original mudar (por exemplo, você atualizou o modelo), então o cache local em cada componente será invalidado para evitar qualquer conflito. Como dito anteriormente, o cache é ajustável e pode ser configurado para corresponder às necessidades do seu ambiente.

Para obter mais informações sobre como usar o FlexGroup volumes com VAAI, consulte este artigo da KB: "VAAI: Como o armazenamento em cache funciona com o FlexGroup volumes?"

Em ambientes onde você não consegue aproveitar ao máximo o cache FlexGroup, mas ainda exige clonagem rápida entre volumes, considere o uso de vVols. A clonagem entre volumes com vVols é muito mais rápida do que usar datastores tradicionais e não depende de um cache.

Definições de QoS

A configuração do QoS no nível FlexGroup usando o Gerenciador de sistema do ONTAP ou o shell do cluster é suportada, no entanto, não fornece reconhecimento de VM ou integração do vCenter.

O QoS (IOPS máx/min) pode ser definido em VMs individuais ou em todas as VMs em um datastore na IU do vCenter ou por meio de APIs REST usando ferramentas do ONTAP. A configuração de QoS em todas as VMs substitui todas as configurações separadas por VM. As configurações não se estendem a VMs novas ou migradas no futuro; defina a QoS nas novas VMs ou reaplique QoS a todas as VMs no datastore.

Observe que o VMware vSphere trata todas as IO para um datastore NFS como uma única fila por host, e a regulagem da QoS em uma VM pode afetar a performance de outras VMs no mesmo datastore para esse host. Isso está em contraste com o vVols, que pode manter suas configurações de política de QoS se eles migrarem para outro datastore e não afetarem o IO de outras VMs quando forem controlados.

Métricas

O ONTAP 9.8 também adicionou novas métricas de performance baseadas em arquivos (IOPS, taxa de transferência e latência) para o FlexGroup Files, e essas métricas podem ser visualizadas nas ferramentas do ONTAP para os relatórios de VM e painel do VMware vSphere. O plug-in das ferramentas do ONTAP para VMware vSphere também permite que você defina regras de qualidade do serviço (QoS) usando uma combinação de IOPS máximo e/ou mínimo. Eles podem ser configurados em todas as VMs em um datastore ou individualmente para VMs específicas.

Práticas recomendadas

- Use as ferramentas do ONTAP para criar datastores do FlexGroup para garantir que o FlexGroup seja criado de forma otimizada e que as políticas de exportação sejam configuradas para corresponder ao seu ambiente vSphere. No entanto, depois de criar o volume FlexGroup com as ferramentas do ONTAP, você descobrirá que todos os nós do cluster do vSphere estão usando um único endereço IP para montar o datastore. Isso pode resultar em um gargalo na porta de rede. Para evitar esse problema, desmonte o datastore e remonte-o usando o assistente padrão do vSphere datastore usando um nome DNS de round-robin que carrega o balanceamento entre LIFs no SVM. Depois de remontar, as ferramentas do ONTAP poderão gerenciar o datastore novamente. Se as ferramentas do ONTAP não estiverem disponíveis, use os padrões do FlexGroup e crie sua política de exportação seguindo as diretrizes do "Datastores e protocolos - NFS".
- Ao dimensionar um armazenamento de dados do FlexGroup, lembre-se de que o FlexGroup consiste em vários volumes FlexVol menores que criam um namespace maior. Como tal, dimensione o datastore para ter pelo menos 8x (assumindo os componentes 8 padrão) o tamanho do seu maior arquivo VMDK mais 10-20% de espaço livre não utilizado para permitir flexibilidade no rebalanceamento. Por exemplo, se você

tiver um VMDK de 6TB TB no seu ambiente, dimensione o datastore do FlexGroup não menor que 52,8TB TB (6x8 a 10%).

- VMware e NetApp suportam entroncamento de sessão NFSv4,1 começando com ONTAP 9.14,1. Consulte as notas da ferramenta de Matriz de interoperabilidade (IMT) do NetApp NFS 4,1 para obter detalhes específicos da versão. O NFSv3 não oferece suporte a vários caminhos físicos para um volume, mas oferece suporte ao nconnect a partir do vSphere 8.0U2. Mais informações sobre o nconnect podem ser encontradas no "NFSv3 nLigue o recurso ao NetApp e VMware".
- Use o plug-in NFS para VMware VAAI para descarga de cópia. Observe que, embora a clonagem seja aprimorada em um datastore FlexGroup, como mencionado anteriormente, o ONTAP não oferece vantagens significativas de desempenho em comparação com a cópia do host ESXi ao copiar VMs entre volumes FlexVol e/ou FlexGroup. Portanto, considere seus workloads de clonagem ao decidir usar volumes VAAI ou FlexGroup. Modificar o número de volumes constituintes é uma forma de otimizar a clonagem baseada em FlexGroup. Como está ajustando o tempo limite do cache mencionado anteriormente.
- Use as ferramentas do ONTAP para o VMware vSphere 9,8-9,13 para monitorar a performance das VMs FlexGroup usando métricas do ONTAP (painel e relatórios de VM) e gerenciar a QoS em VMs individuais. Essas métricas não estão disponíveis atualmente por meio de comandos ou APIs do ONTAP.
- O plug-in do SnapCenter para VMware vSphere versão 4,4 e posterior oferece suporte ao backup e à recuperação de VMs em um datastore FlexGroup no sistema de storage primário. A VCS 4,6 adiciona suporte ao SnapMirror para datastores baseados em FlexGroup. Usar snapshots e replicação baseados em array é a maneira mais eficiente de proteger seus dados.

Configuração de rede

A configuração das configurações de rede ao usar o vSphere com sistemas executando o ONTAP é simples e semelhante a outras configurações de rede.

Aqui estão algumas coisas a considerar:

- Separe o tráfego de rede de armazenamento de outras redes. Uma rede separada pode ser obtida usando uma VLAN dedicada ou switches separados para armazenamento. Se a rede de armazenamento partilhar caminhos físicos, como uplinks, poderá necessitar de portas de QoS ou uplink adicionais para garantir uma largura de banda suficiente. Não conete os hosts diretamente ao storage a menos que o guia de solução o chame especificamente; use switches para ter caminhos redundantes e permitir que o VMware HA funcione sem intervenção.
- Jumbo Frames devem ser usados se suportado pela sua rede. Se forem usados, certifique-se de que estejam configurados de forma idêntica em todos os dispositivos de rede, VLANs e assim por diante no caminho entre o armazenamento e o host ESXi. Caso contrário, você pode ver problemas de desempenho ou conexão. A MTU também deve ser definida de forma idêntica no switch virtual ESXi, na porta VMkernel e também nas portas físicas ou grupos de interface de cada nó ONTAP.
- O NetApp recomenda apenas desativar o controle de fluxo de rede nas portas de interconexão de cluster dentro de um cluster ONTAP. A NetApp não faz outras recomendações sobre práticas recomendadas em relação ao controle de fluxo para as portas de rede restantes usadas para tráfego de dados. Você deve ativá-lo ou desativá-lo conforme necessário. "TR-4182"Consulte para obter mais informações sobre o controlo de fluxo.
- Quando os storages ESXi e ONTAP estão conetados a redes de armazenamento Ethernet, a NetApp recomenda configurar as portas Ethernet às quais esses sistemas se conetam como portas de borda de protocolo de árvore de expansão rápida (RSTP) ou usando o recurso Cisco PortFast. A NetApp recomenda ativar o recurso de tronco de porta de árvore de expansão rápida em ambientes que usam o recurso Cisco PortFast e que têm entroncamento de VLAN 802,1Q habilitado para o servidor ESXi ou para os storages ONTAP.

- A NetApp recomenda as seguintes práticas recomendadas para agregação de links:
  - Use switches que suportam agregação de links de portas em dois chassis de switch separados usando uma abordagem de grupo de agregação de links de vários gabinetes, como o Virtual PortChannel (VPC) da Cisco.
  - Desative o LACP para portas de switch conetadas ao ESXi a menos que você esteja usando dvSwitches 5,1 ou posterior com o LACP configurado.
  - Use o LACP para criar agregados de link para sistemas de storage ONTAP com grupos de interface multimodo dinâmico com hash IP.
  - Use uma política de agrupamento de hash IP no ESXi.

A tabela a seguir fornece um resumo dos itens de configuração de rede e indica onde as configurações são aplicadas.

Item	ESXi	Interrutor	Nó	SVM
Endereço IP	VMkernel	Não**	Não**	Sim
Agregação de links	Switch virtual	Sim	Sim	Não*
VLAN	Grupos de portas VMkernel e VM	Sim	Sim	Não*
Controle de fluxo	NIC	Sim	Sim	Não*
Spanning tree	Não	Sim	Não	Não
MTU (para quadros jumbo)	Switch virtual e porta VMkernel (9000)	Sim (definido para máx.)	Sim (9000)	Não*
Grupos de failover	Não	Não	Sim (criar)	Sim (selecione)

*Os LIFs SVM se conetam a portas, grupos de interfaces ou interfaces VLAN que têm VLAN, MTU e outras configurações. No entanto, as configurações não são gerenciadas no nível da SVM.

**Esses dispositivos têm endereços IP próprios para gerenciamento, mas esses endereços não são usados no contexto da rede de armazenamento ESXi.

SAN (FC, NVMe/FC, iSCSI, NVMe/TCP), RDM

O ONTAP oferece storage de bloco de classe empresarial para VMware vSphere usando iSCSI tradicional e Fibre Channel Protocol (FCP), bem como o protocolo de bloco de última geração, altamente eficiente e de alta performance, o NVMe over Fabrics (NVMe-of), com suporte a NVMe/FC e NVMe/TCP.

Para obter as práticas recomendadas detalhadas para a implementação de protocolos de bloco para armazenamento de VM com o vSphere e o ONTAP, consulte "Datastores e Protocolos - SAN"

NFS

O vSphere permite que os clientes usem arrays NFS de classe empresarial para fornecer acesso simultâneo a datastores para todos os nós em um cluster ESXi. Como mencionado na "armazenamentos de dados" seção, há alguns benefícios de visibilidade de eficiência de storage e facilidade de uso ao usar o NFS com vSphere.

Para obter as melhores práticas recomendadas, consulte "Datastores e Protocolos - NFS"

Ligação direta em rede

Às vezes, os administradores de storage preferem simplificar suas infraestruturas removendo switches de rede da configuração. Isso pode ser suportado em alguns cenários. No entanto, existem algumas limitações e ressalvas a serem observadas.

ISCSI e NVMe/TCP

Um host usando iSCSI ou NVMe/TCP pode ser conetado diretamente a um sistema de storage e operar normalmente. A razão é pathing. Conexões diretas a dois controladores de storage diferentes resultam em dois caminhos independentes para o fluxo de dados. A perda de caminho, porta ou controlador não impede que o outro caminho seja usado.

NFS

O armazenamento NFS com conexão direta pode ser usado, mas com uma limitação significativa - o failover não funcionará sem um esforço significativo de script, o que seria da responsabilidade do cliente.

O motivo pelo qual o failover sem interrupções é complicado com o storage NFS com conexão direta é o roteamento que ocorre no sistema operacional local. Por exemplo, suponha que um host tenha um endereço IP de 192.168.1.1/24 e esteja conetado diretamente a um controlador ONTAP com um endereço IP de 192.168.1.50/24. Durante o failover, esse endereço 192.168.1.50 pode fazer failover para a outra controladora e estará disponível para o host, mas como o host deteta sua presença? O endereço 192.168.1.1 original ainda existe na NIC host que não se coneta mais a um sistema operacional. O tráfego destinado a 192.168.1.50 continuaria a ser enviado para uma porta de rede inoperável.

A segunda NIC do SO poderia ser configurada como 19 2.168.1.2 e seria capaz de se comunicar com o endereço 192.168.1.50 com falha, mas as tabelas de roteamento local teriam um padrão de usar um endereço **e apenas um** para se comunicar com a sub-rede 192.168.1.0/24. Um sysadmin poderia criar uma estrutura de script que detetaria uma conexão de rede com falha e alteraria as tabelas de roteamento local ou colocaria interfaces para cima e para baixo. O procedimento exato dependeria do SO em uso.

Na prática, os clientes da NetApp têm NFS com conexão direta, mas normalmente apenas para workloads em que as pausas de e/S durante failovers são aceitáveis. Quando os suportes rígidos são usados, não deve haver nenhum erro de e/S durante essas pausas. O IO deve congelar até que os serviços sejam restaurados, seja por uma intervenção de failback ou manual para mover endereços IP entre NICs no host.

FC Direct Connect

Não é possível conectar diretamente um host a um sistema de storage ONTAP usando o protocolo FC. A razão é o uso de NPIV. A WWN que identifica uma porta ONTAP FC para a rede FC usa um tipo de virtualização chamado NPIV. Qualquer dispositivo conetado a um sistema ONTAP deve ser capaz de reconhecer um NPIV WWN. Não há fornecedores atuais de HBA que ofereçam um HBA que possa ser instalado em um host que possa suportar um destino NPIV.

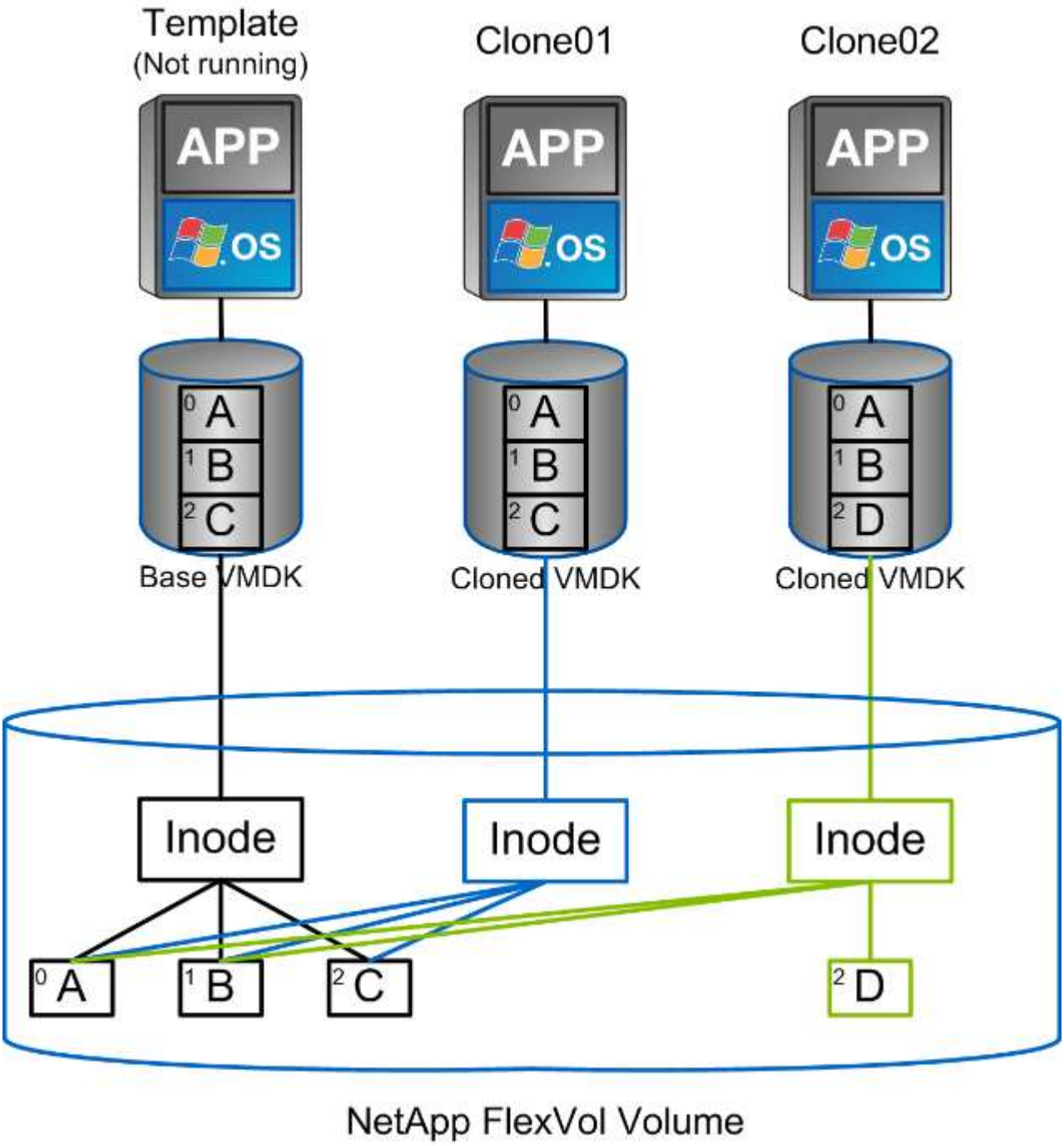
Clonagem de VM e datastore

Clonar um objeto de storage permite criar rapidamente cópias para uso adicional, como provisionamento de VMs adicionais, operações de backup/recuperação etc.

No vSphere, você pode clonar uma VM, um disco virtual, um vVol ou um datastore. Depois de clonado, o objeto pode ser ainda mais personalizado, muitas vezes por meio de um processo automatizado. O vSphere é compatível com clones de cópia completa, bem como clones vinculados, onde ele controla as alterações separadamente do objeto original.

Os clones vinculados são ótimos para economizar espaço, mas aumentam a quantidade de e/S que o vSphere lida com a VM, afetando a performance dessa VM e, talvez, o host geral. É por isso que os clientes da NetApp costumam usar clones baseados em sistema de storage para obter o melhor dos dois mundos: Uso eficiente do storage e maior performance.

A figura a seguir mostra a clonagem de ONTAP.



A clonagem pode ser descarregada para sistemas que executam o ONTAP por meio de vários mecanismos, normalmente no nível de VM, vVol ou datastore. Estes incluem o seguinte:

- VVols usando o fornecedor de APIs do NetApp vSphere para reconhecimento de armazenamento (VASA). Os clones do ONTAP são usados para dar suporte aos snapshots do VVol gerenciados pelo vCenter que são eficientes em termos de espaço com efeito de e/S mínimo para criá-los e excluí-los. As VMs também

podem ser clonadas usando o vCenter, e elas também são descarregadas para o ONTAP, seja em um único datastore/volume ou entre datastores/volumes.

- Clonagem e migração do vSphere usando as APIs do vSphere – Array Integration (VAAI). As operações de clonagem de VM podem ser descarregadas para o ONTAP em ambientes SAN e nas (a NetApp fornece um plug-in ESXi para habilitar o VAAI para NFS). O vSphere apenas descarrega as operações em VMs frias (desativadas) em um datastore nas, enquanto as operações em VMs quentes (clonagem e armazenamento vMotion) também são descarregadas para SAN. O ONTAP usa a abordagem mais eficiente com base na origem e no destino. Essa capacidade também é usada "Omnissa Horizon View" pelo .
- SRA (usado com o VMware Live Site Recovery/Site Recovery Manager). Aqui, os clones são usados para testar a recuperação da réplica de DR sem interrupções.
- Backup e recuperação usando ferramentas do NetApp, como o SnapCenter. Os clones de VM são usados para verificar as operações de backup, bem como para montar um backup de VM para que arquivos individuais possam ser restaurados.

A clonagem descarregada do ONTAP pode ser invocada por ferramentas VMware, NetApp e de terceiros. Clones que são descarregados para o ONTAP têm várias vantagens. Na maioria dos casos, elas usam espaço eficiente, precisando de storage somente para alterações no objeto. Não há efeito de desempenho adicional para lê-las e gravá-las e, em alguns casos, o desempenho é aprimorado ao compartilhar blocos em caches de alta velocidade. Eles também descarregam ciclos de CPU e e/S de rede do servidor ESXi. A descarga de cópia em um datastore tradicional usando um FlexVol volume pode ser rápida e eficiente com a licença FlexClone licenciada (incluída na licença ONTAP One), mas as cópias entre volumes FlexVol podem ser mais lentas. Se você mantiver os modelos de VM como uma fonte de clones, considere colocá-los no volume do datastore (use pastas ou bibliotecas de conteúdo para organizá-los) para clones rápidos e com uso eficiente de espaço.

Você também pode clonar um volume ou LUN diretamente no ONTAP para clonar um armazenamento de dados. Com os datastores NFS, a tecnologia FlexClone pode clonar um volume inteiro, e o clone pode ser exportado do ONTAP e montado pelo ESXi como outro datastore. Para armazenamentos de dados VMFS, o ONTAP pode clonar um LUN em um volume ou volume inteiro, incluindo um ou mais LUNs nele. Um LUN que contém um VMFS deve ser mapeado para um grupo de iniciadores ESXi (igroup) e, em seguida, demarcado pelo ESXi para ser montado e usado como um datastore regular. Para alguns casos de uso temporário, um VMFS clonado pode ser montado sem uma nova assinatura. Depois que um datastore é clonado, as VMs dentro dele podem ser registradas, reconfiguradas e personalizadas como se fossem VMs clonadas individualmente.

Em alguns casos, recursos licenciados adicionais podem ser usados para aprimorar a clonagem, como o SnapRestore para backup ou o FlexClone. Essas licenças são frequentemente incluídas em pacotes de licenças sem nenhum custo adicional. É necessária uma licença FlexClone para as operações de clonagem da Vevolve, bem como para dar suporte a snapshots gerenciados de uma VVol (que são descarregados do hipervisor para a ONTAP). Uma licença do FlexClone também pode melhorar certos clones baseados em VAAI quando usados em um datastore/volume (cria cópias instantâneas com uso eficiente de espaço em vez de cópias em bloco). Ele também é usado pelo SRA ao testar a recuperação de uma réplica de DR e SnapCenter para operações de clone, além de pesquisar cópias de backup para restaurar arquivos individuais.

Proteção de dados

Fazer backup e recuperar rapidamente suas máquinas virtuais (VMs) são as principais vantagens do uso do ONTAP para vSphere. Essa funcionalidade pode ser gerenciada facilmente no vCenter por meio do plug-in do SnapCenter para VMware vSphere. Muitos clientes aprimoram suas soluções de backup de terceiros com o SnapCenter para

aproveitar a tecnologia de snapshot da ONTAP, pois oferece a maneira mais rápida e simples de recuperar uma VM com o ONTAP. O SnapCenter está disponível gratuitamente para clientes que têm a licença ONTAP One e outros pacotes de licença também podem estar disponíveis.

Além disso, o SnapCenter Plug-In para VMware pode ser integrado com "NetApp Backup and Recovery para máquinas virtuais", permitindo soluções eficazes de backup 3-2-1 para a maioria dos sistemas ONTAP . Observe que algumas taxas podem ser aplicadas ao usar o Backup e Recuperação para máquinas virtuais com serviços premium, como armazenamentos de objetos para armazenamento de backup adicional. Esta seção descreve as várias opções disponíveis para proteger suas VMs e armazenamentos de dados.

Instantâneos de volume do NetApp ONTAP

Use snapshots para fazer cópias rápidas da VM ou do armazenamento de dados sem afetar a performance e enviá-las para um sistema secundário usando o SnapMirror para proteção de dados externa a mais longo prazo. Essa abordagem minimiza o espaço de armazenamento e a largura de banda da rede, armazenando apenas informações alteradas.

Os snapshots são um recurso importante do ONTAP, permitindo que você crie cópias pontuais de seus dados. Eles são eficientes em espaço e podem ser criados rapidamente, o que os torna ideais para proteger VMs e datastores. Os snapshots podem ser usados para vários fins, incluindo backup, recuperação e teste. Esses snapshots são diferentes dos snapshots VMware (consistência) e são adequados para proteção de longo prazo. Os snapshots gerenciados pelo vCenter da VMware só são recomendados para uso a curto prazo devido ao desempenho e outros efeitos. "Limitações do Snapshot"Consulte para obter mais detalhes.

Os snapshots são criados no nível do volume e podem ser usados para proteger todas as VMs e armazenamentos de dados dentro desse volume. Isso significa que você pode criar um snapshot de um datastore inteiro, que inclui todas as VMs dentro desse datastore.

Para armazenamentos de dados NFS, você pode visualizar facilmente arquivos de VM em snapshots navegando no diretório .snapshots. Isso permite que você acesse e restaure rapidamente arquivos de um snapshot sem a necessidade de usar uma solução de backup específica.

Para datastores VMFS, você pode criar um FlexClone do datastore com base no snapshot desejado. Isso permite que você crie um novo datastore baseado no snapshot, que pode ser usado para fins de teste ou desenvolvimento. O FlexClone só consumirá espaço para as alterações feitas após o snapshot ser obtido, tornando-o uma maneira eficiente de espaço para criar uma cópia do datastore. Uma vez que o FlexClone é criado, você pode mapear o LUN ou namespace para um host ESXi como um datastore comum. Isso permite que você restaure arquivos de VM específicos, além de permitir a criação rápida de ambientes de teste ou desenvolvimento com base em dados de produção sem impactar a performance do ambiente de produção.

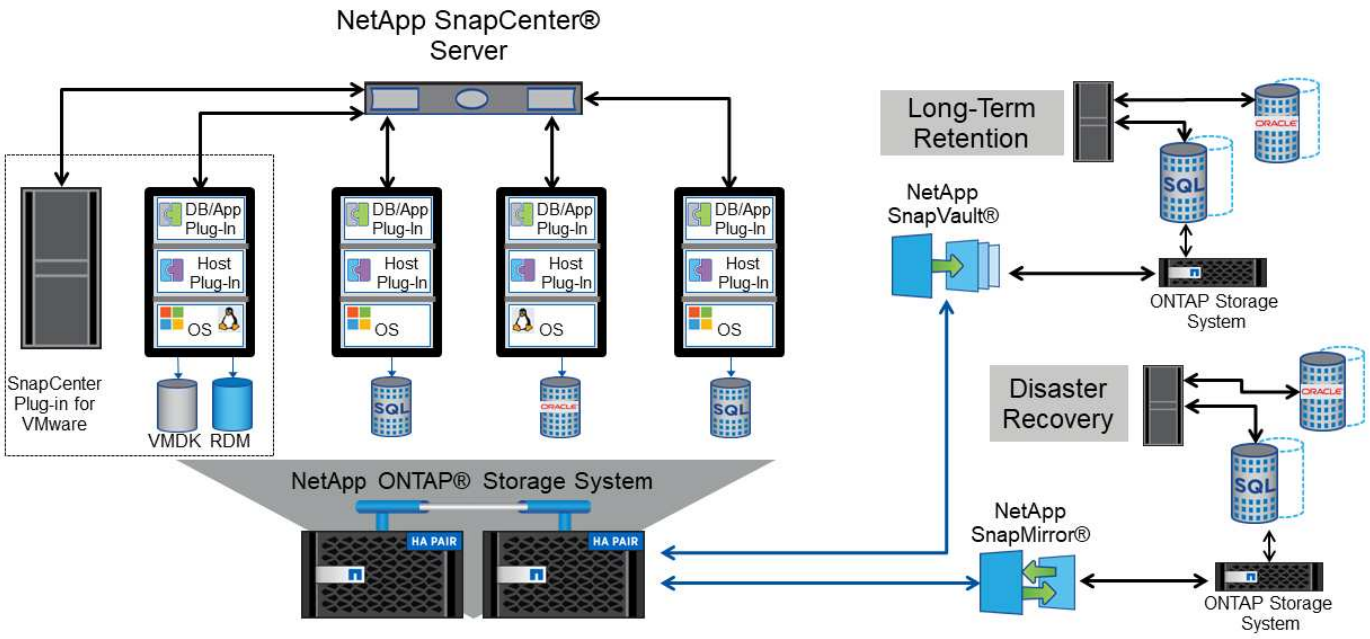
Para obter mais informações sobre snapshots, consulte a documentação do ONTAP . Os links a seguir fornecem detalhes adicionais: "Cópias Snapshot locais do ONTAP" "Fluxo de trabalho de replicação do ONTAP SnapMirror"

Plug-in do SnapCenter para VMware vSphere

O SnapCenter permite criar políticas de backup que podem ser aplicadas a vários trabalhos. Essas políticas podem definir agendamento, retenção, replicação e outros recursos. Elas continuam permitindo uma seleção opcional de snapshots consistentes com VM, o que aproveita a capacidade do hipervisor de silenciar a I/o antes de tirar um snapshot da VMware. No entanto, devido ao efeito de desempenho dos snapshots VMware, eles geralmente não são recomendados, a menos que você precise que o sistema de arquivos Guest seja encerrado. Em vez disso, use snapshots para proteção geral e use ferramentas de aplicativos, como plug-ins de aplicativos SnapCenter, para proteger dados transacionais, como SQL Server ou Oracle.

Esses plug-ins oferecem recursos estendidos para proteger os bancos de dados em ambientes físicos e virtuais. Com o vSphere, você pode usá-los para proteger bancos de dados SQL Server ou Oracle em que os dados são armazenados em LUNs RDM, vVols ou namespaces NVMe/TCP e LUNs iSCSI diretamente conetados ao sistema operacional convidado ou arquivos VMDK em armazenamentos de dados VMFS ou NFS. Os plug-ins permitem a especificação de diferentes tipos de backups de banco de dados, suporte a backup on-line ou off-line e proteção de arquivos de banco de dados juntamente com arquivos de log. Além de backup e recuperação, os plug-ins também dão suporte à clonagem de bancos de dados para fins de desenvolvimento ou teste.

A figura a seguir mostra um exemplo de implantação do SnapCenter.



Para obter informações sobre o dimensionamento, consulte a. "Guia de dimensionamento do plug-in SnapCenter para VMware vSphere"

Ferramentas do ONTAP para VMware vSphere com recuperação de site ao vivo da VMware

As ferramentas do ONTAP para VMware vSphere (OT4VS) são um plug-in gratuito que oferece uma integração perfeita entre o VMware vSphere e o NetApp ONTAP. Ele permite que você gerencie seu armazenamento do ONTAP diretamente do cliente da Web vSphere, facilitando a execução de tarefas como provisionamento de armazenamento, gerenciamento de replicação e monitoramento de desempenho.

Para melhorar os recursos de recuperação de desastres, considere a utilização do NetApp SRA for ONTAP, que faz parte das ferramentas do ONTAP para VMware vSphere, juntamente com o VMware Live Site Recovery (anteriormente conhecido como Site Recovery Manager). Essa ferramenta não só dá suporte à replicação de armazenamentos de dados em um local de recuperação de desastres usando o SnapMirror, como também permite testes sem interrupções no ambiente de recuperação de desastres clonando os armazenamentos de dados replicados. Além disso, a recuperação de um desastre e a reproteção da produção após a resolução de uma interrupção são simplificadas graças aos recursos de automação incorporados.

NetApp Disaster Recovery

Recuperação de desastres (DR) é um serviço baseado em nuvem que fornece uma solução abrangente para proteger seus dados e aplicativos em caso de desastre. Ele oferece uma variedade de recursos, incluindo failover e failback automatizados, vários pontos de recuperação pontuais, recuperação de desastres

consistente com o aplicativo e suporte para sistemas ONTAP locais e baseados na nuvem. O NetApp Disaster Recovery foi projetado para funcionar perfeitamente com o ONTAP e seu ambiente VMware vSphere, fornecendo uma solução unificada para recuperação de desastres.

Cluster de armazenamento Metro do vSphere (vMSC) com sincronização ativa do NetApp MetroCluster e do SnapMirror

Por fim, para obter o mais alto nível de proteção de dados, considere uma configuração vMSC (VMware vSphere Metro Storage Cluster) usando o NetApp MetroCluster. O vMSC é uma solução compatível com NetApp certificada pela VMware que usa replicação síncrona, oferecendo os mesmos benefícios de um cluster de alta disponibilidade, mas distribuída em locais separados para proteger contra desastres no local. A sincronização ativa do NetApp SnapMirror, com ASA e AFF, e o MetroCluster com AFF, oferece configurações econômicas para replicação síncrona com recuperação transparente de qualquer falha de componente de storage, bem como recuperação transparente no caso da sincronização ativa do SnapMirror ou recuperação de comando único no caso de um desastre no local com MetroCluster. O vMSC é descrito em mais detalhes em "TR-4128".

Qualidade do serviço (QoS)

Os limites de taxa de transferência são úteis no controle de níveis de serviço, no gerenciamento de cargas de trabalho desconhecidas ou para testar aplicativos antes da implantação para garantir que eles não afetem outras cargas de trabalho em produção. Eles também podem ser usados para restringir uma carga de trabalho bully depois que ela é identificada.

Suporte à política de QoS ONTAP

Os sistemas que executam o ONTAP podem usar o recurso de QoS de storage para limitar a taxa de transferência em Mbps e/ou e/os por segundo (IOPS) para diferentes objetos de storage, como arquivos, LUNs, volumes ou SVMs inteiras.

Níveis mínimos de serviço baseados em IOPS também são compatíveis para fornecer desempenho consistente para objetos SAN no ONTAP 9.2 e para objetos nas no ONTAP 9.3.

O limite máximo de taxa de transferência de QoS em um objeto pode ser definido em Mbps e/ou IOPS. Se ambos forem usados, o primeiro limite atingido é imposto pelo ONTAP. Um workload pode conter vários objetos e uma política de QoS pode ser aplicada a um ou mais workloads. Quando uma política é aplicada a vários workloads, os workloads compartilham o limite total da política. Objetos aninhados não são suportados (por exemplo, arquivos dentro de um volume não podem ter sua própria política). Os mínimos de QoS só podem ser definidos em IOPS.

As ferramentas a seguir estão disponíveis no momento para gerenciar políticas de QoS do ONTAP e aplicá-las a objetos:

- CLI do ONTAP
- Gerente do sistema da ONTAP
- OnCommand Workflow Automation
- Active IQ Unified Manager
- Kit de ferramentas do NetApp PowerShell para ONTAP
- Ferramentas do ONTAP para o provedor VMware vSphere VASA

Para atribuir uma política de QoS a um LUN, incluindo VMFS e RDM, o ONTAP SVM (exibido como SVM), caminho de LUN e número de série podem ser obtidos no menu sistemas de armazenamento na página inicial de ferramentas do ONTAP para VMware vSphere. Selecione o sistema de storage (SVM) e, em seguida, objetos relacionados > SAN. Use essa abordagem ao especificar QoS usando uma das ferramentas do ONTAP.

"Visão geral do gerenciamento e monitoramento de desempenho"Consulte para obter mais informações.

Armazenamentos de dados NFS que não são vVols

Uma política de QoS do ONTAP pode ser aplicada a todo o datastore ou arquivos VMDK individuais dentro dele. No entanto, é importante entender que todas as VMs em um datastore NFS tradicional (não vVols) compartilham uma fila de e/S comum de um determinado host. Se qualquer VM for estrangulada por uma política de QoS do ONTAP, isso resultará na prática em que toda e/S desse datastore parecerá ser estrangulada para esse host.

Exemplo: * você configura um limite de QoS no VM1.vmdk para um volume que é montado como um armazenamento de dados NFS tradicional pelo host esxi-01. * O mesmo host (esxi-01) está usando vm2.vmdk e está no mesmo volume. * Se VM1.vmdk for estrangulado, então vm2.vmdk também parecerá ser estrangulado, pois compartilha a mesma fila de e/S com VM1.vmdk.

Isso não se aplica ao vVols.

A partir do vSphere 6,5, você pode gerenciar limites granulares de arquivos em datastores não vVols utilizando o Storage Policy-Based Management (SPBM) com Storage I/o Control (SIOC) v2.

Consulte os links a seguir para obter mais informações sobre como gerenciar o desempenho com as políticas SIOC e SPBM.

"Regras baseadas no host do SPBM: SIOC v2" "Gerencie os recursos de e/S de storage com o vSphere"

Para atribuir uma política de QoS a um VMDK no NFS, observe as seguintes diretrizes:

- A política deve ser aplicada ao `vmname-flat.vmdk` que contém a imagem de disco virtual real, não ao `vmname.vmdk` (arquivo de descritor de disco virtual) ou `vmname.vmx` (arquivo de descritor de VM).
- Não aplique políticas a outros arquivos VM, como arquivos de swap virtuais (`vmname.vswp`).
- Ao usar o cliente da Web vSphere para encontrar caminhos de arquivo (datastore > Files), esteja ciente de que ele combina as informações do `- flat.vmdk` e e `. vmdk` simplesmente mostra um arquivo com o nome do `. vmdk` , mas o tamanho do `- flat.vmdk`. Adicione `-flat` ao nome do arquivo para obter o caminho correto.

Os armazenamentos de dados do FlexGroup oferecem recursos aprimorados de QoS ao usar as ferramentas do ONTAP para VMware vSphere 9,8 e posterior. Você pode facilmente definir QoS em todas as VMs em um datastore ou em VMs específicas. Consulte a seção FlexGroup deste relatório para obter mais informações. Esteja ciente de que as limitações de QoS mencionadas anteriormente com armazenamentos de dados NFS tradicionais ainda se aplicam.

Armazenamentos de dados VMFS

Usando LUNs ONTAP, as políticas de QoS podem ser aplicadas ao FlexVol volume que contém LUNs ou LUNs individuais, mas não arquivos VMDK individuais, porque o ONTAP não tem conhecimento do sistema de arquivos VMFS.

Armazenamentos de dados vVols

A QoS mínima e/ou máxima pode ser facilmente definida em VMs individuais ou VMDKs sem afetar qualquer outra VM ou VMDK usando o gerenciamento baseado em políticas de storage e vVols.

Ao criar o perfil de capacidade de storage para o contêiner da VVol, especifique um valor máximo e/ou mínimo de IOPS sob a capacidade de desempenho e, em seguida, faça referência a esse SCP com a política de armazenamento da VM. Use essa política ao criar a VM ou aplicar a diretiva a uma VM existente.

> O vVols requer o uso de ferramentas do ONTAP para VMware vSphere, que funciona como o provedor VASA para ONTAP. "VMware vSphere Virtual volumes (vVols) com o ONTAP"Consulte para obter as práticas recomendadas do vVols.

QoS ONTAP e VMware SIOC

O ONTAP QoS e o VMware vSphere Storage I/o Control (SIOC) são tecnologias complementares que o vSphere e os administradores de storage podem usar em conjunto para gerenciar a performance de VMs vSphere hospedadas em sistemas executando o ONTAP. Cada ferramenta tem suas próprias forças, como mostrado na tabela a seguir. Devido aos diferentes escopos do VMware vCenter e do ONTAP, alguns objetos podem ser vistos e gerenciados por um sistema e não pelo outro.

Propriedade	QoS ONTAP	VMware SIOC
Quando ativo	A política está sempre ativa	Ativo quando existe contenção (latência do datastore sobre o limite)
Tipo de unidades	IOPS, Mbps	IOPS, compartilhamentos
Escopo do vCenter ou do aplicativo	Vários ambientes do vCenter, outros hipervisores e aplicações	Servidor vCenter único
Definir QoS na VM?	VMDK somente em NFS	VMDK em NFS ou VMFS
Definir QoS no LUN (RDM)?	Sim	Não
Definir QoS no LUN (VMFS)?	Sim	Sim (o datastore pode ser estrangulado)
Definir QoS no volume (armazenamento de dados NFS)?	Sim	Sim (o datastore pode ser estrangulado)
Definir QoS no SVM (locatário)?	Sim	Não
Abordagem baseada em políticas?	Sim. Pode ser compartilhado por todas as cargas de trabalho na política ou aplicado na íntegra a cada workload na política.	Sim, com o vSphere 6,5 e posterior.
Licença necessária	Incluído com ONTAP	Enterprise Plus

Programador de recursos distribuídos do VMware Storage

O VMware Storage Distributed Resource Scheduler (SDRS) é um recurso do vSphere que coloca as VMs no armazenamento com base na latência de e/S atual e no uso do espaço. Em seguida, ele move a VM ou VMDKs sem interrupções entre os armazenamentos de dados em um cluster de datastore (também chamado de pod), selecionando o melhor datastore no qual colocar a VM ou VMDKs no cluster do datastore. Um cluster de datastore é um conjunto de datastores semelhantes que são agregados em uma única unidade de

consumo da perspetiva do administrador do vSphere.

Ao usar SDRS com ferramentas do ONTAP para VMware vSphere, primeiro você deve criar um datastore com o plug-in, usar o vCenter para criar o cluster do datastore e, em seguida, adicionar o datastore a ele. Após a criação do cluster do datastore, armazenamentos de dados adicionais podem ser adicionados ao cluster do datastore diretamente do assistente de provisionamento na página Detalhes.

Outras práticas recomendadas da ONTAP para SDRS incluem o seguinte:

- Todos os armazenamentos de dados no cluster devem usar o mesmo tipo de armazenamento (como SAS, SATA ou SSD), ser todos os armazenamentos de dados VMFS ou NFS e ter as mesmas configurações de replicação e proteção.
- Considere usar SDRS no modo padrão (manual). Essa abordagem permite que você analise as recomendações e decida se as aplicará ou não. Esteja ciente desses efeitos das migrações VMDK:
  - Quando OS SDRS migram VMDKs entre armazenamentos de dados, qualquer economia de espaço da clonagem ou deduplicação do ONTAP é perdida. Você pode executar novamente a deduplicação para recuperar essas economias.
  - Depois que OS SDRS movem VMDKs, o NetApp recomenda recriar os snapshots no datastore de origem porque o espaço é bloqueado pela VM que foi movida.
  - Mover VMDKs entre armazenamentos de dados no mesmo agregado tem poucos benefícios, e OS SDRS não têm visibilidade de outras cargas de trabalho que possam compartilhar o agregado.

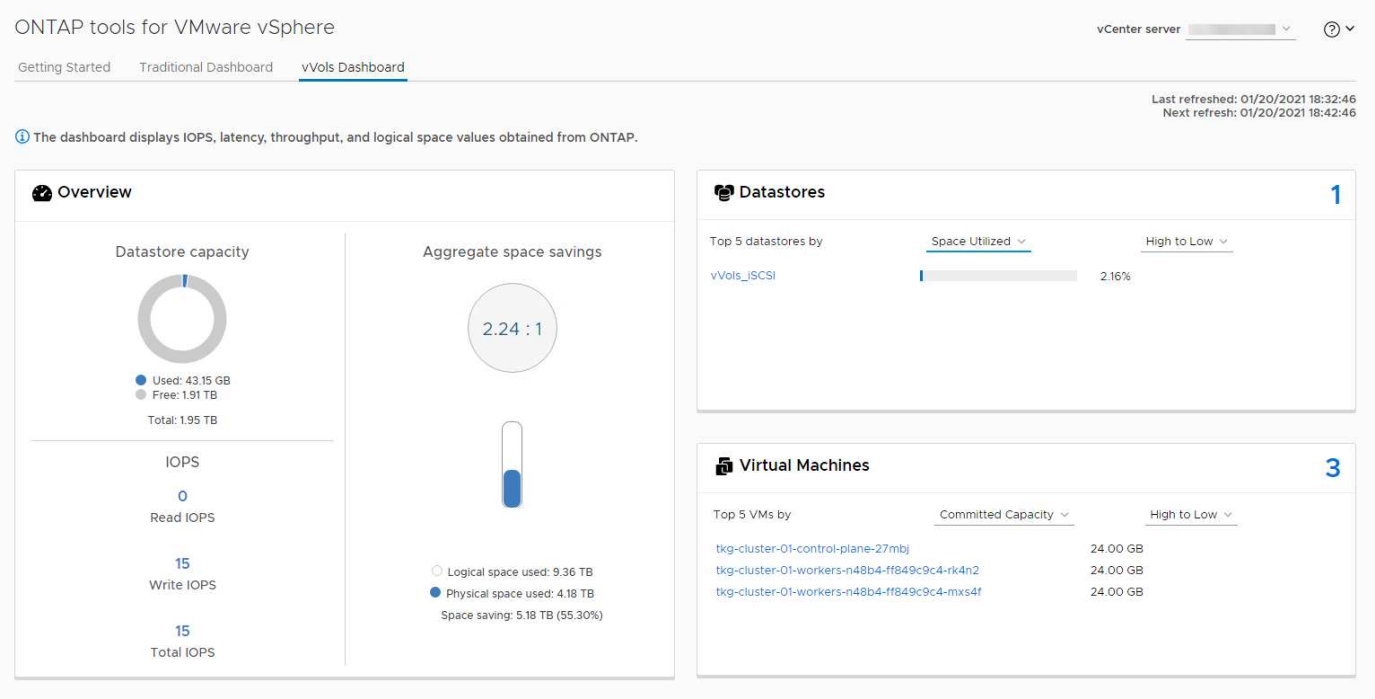
VVols e gerenciamento baseado em políticas de storage

As VMware vSphere APIs for Storage Awareness (VASA) facilitam para um administrador de storage configurar datastores com recursos bem definidos e permitir que o administrador da VM use-os sempre que necessário para provisionar VMs sem ter que interagir uns com os outros. Vale a pena dar uma olhada nessa abordagem para ver como ela pode otimizar suas operações de storage de virtualização e evitar muito trabalho trivial.

Antes do VASA, os administradores de VM podiam definir políticas de armazenamento de VM, mas precisavam trabalhar com o administrador de armazenamento para identificar armazenamentos de dados apropriados, geralmente usando documentação ou convenções de nomenclatura. Com o VASA, o administrador de storage pode definir uma variedade de recursos de storage, incluindo desempenho, disposição em camadas, criptografia e replicação. Um conjunto de recursos para um volume ou um conjunto de volumes é chamado de Perfil de capacidade de armazenamento (SCP).

O SCP suporta QoS mínimo e/ou máximo para vVols de dados de uma VM. A QoS mínima é suportada apenas em sistemas AFF. As ferramentas do ONTAP para VMware vSphere incluem um painel que exibe o desempenho granular da VM e a capacidade lógica para vVols em sistemas ONTAP.

A figura a seguir mostra as ferramentas do ONTAP para o painel vVols do VMware vSphere 9,8.



Após a definição do perfil de funcionalidade de storage, ele pode ser usado para provisionar VMs usando a política de storage que identifica seus requisitos. O mapeamento entre a política de armazenamento de VM e o perfil de capacidade de armazenamento de dados permite que o vCenter exiba uma lista de datastores compatíveis para seleção. Essa abordagem é conhecida como gerenciamento baseado em políticas de storage.

O VASA fornece a tecnologia para consultar o armazenamento e retornar um conjunto de recursos de armazenamento ao vCenter. Os fornecedores do VASA fornecem a tradução entre as APIs e construções do sistema de storage e as APIs da VMware que são entendidas pelo vCenter. O fornecedor VASA da NetApp para ONTAP é oferecido como parte das ferramentas da ONTAP para a VM do dispositivo VMware vSphere, e o plug-in do vCenter fornece a interface para provisionar e gerenciar datastores vVol, bem como a capacidade de definir perfis de capacidade de armazenamento (SCPs).

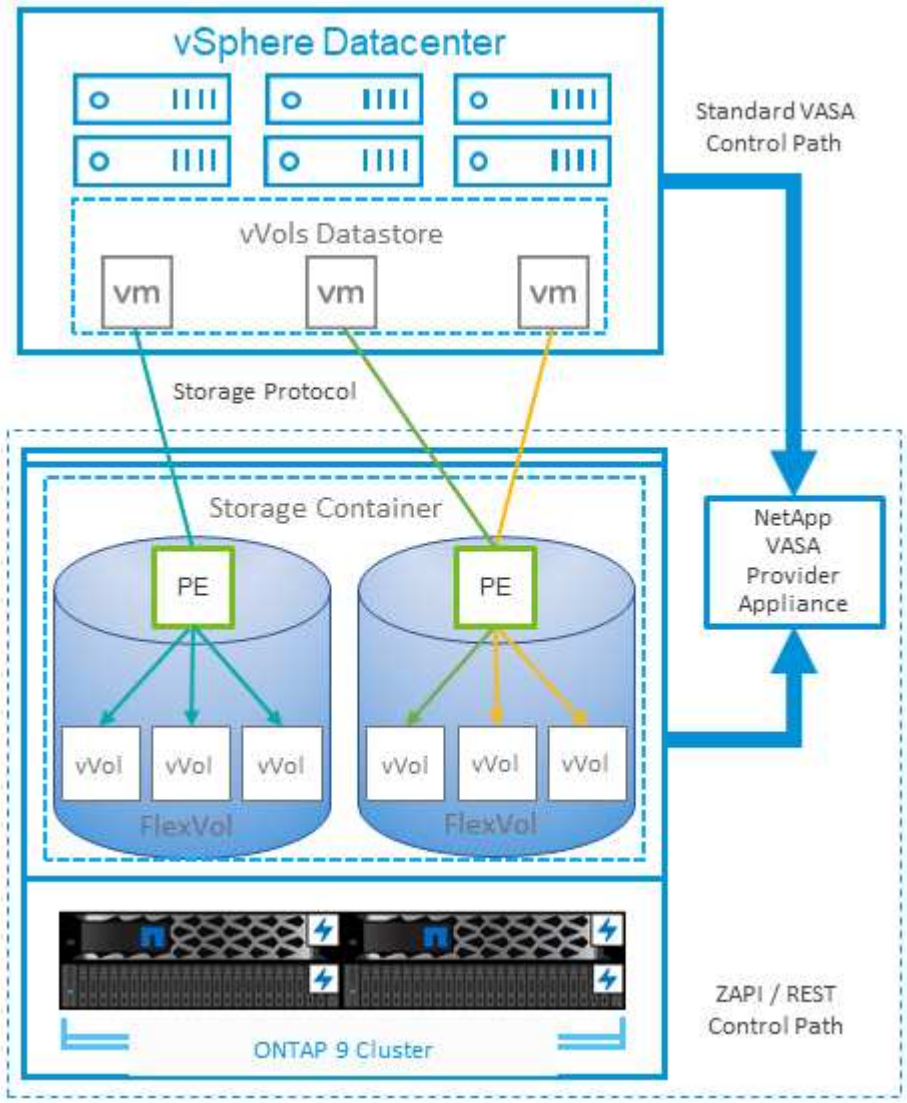
O ONTAP dá suporte aos armazenamentos de dados VMFS e NFS VVol. O uso do vVols com armazenamentos de dados SAN traz alguns dos benefícios do NFS, como granularidade no nível da VM. Aqui estão algumas práticas recomendadas a serem consideradas e você pode encontrar informações adicionais em"TR-4400":

- Um datastore da VVol pode consistir em vários volumes FlexVol em vários nós dos clusters. A abordagem mais simples é um único datastore, mesmo quando os volumes têm capacidades diferentes. O SPBM garante que um volume compatível seja usado para a VM. No entanto, todos os volumes precisam fazer parte de um único SVM do ONTAP e acessá-los usando um único protocolo. Um LIF por nó para cada protocolo é suficiente. Evite o uso de várias versões do ONTAP em um único datastore da vVol porque as funcionalidades do storage podem variar entre lançamentos.
- Use as ferramentas do ONTAP para o plug-in do VMware vSphere para criar e gerenciar datastores da evolução. Além de gerenciar o datastore e seu perfil, ele cria automaticamente um endpoint de protocolo para acessar os vVols, se necessário. Se os LUNs forem usados, observe que os PES de LUN são mapeados usando IDs de LUN 300 e superiores. Verifique se a configuração do sistema avançado do host ESXi `Disk.MaxLUN` permite um número de ID LUN maior que 300 (o padrão é 1.024). Execute esta etapa selecionando o host ESXi no vCenter, a guia Configurar e localize `Disk.MaxLUN` na lista de Configurações avançadas do sistema.
- Não instale nem migre o provedor VASA, o vCenter Server (baseado em appliance ou Windows) ou as

ferramentas do ONTAP para o próprio VMware vSphere em um datastore vVols, porque eles são mutuamente dependentes, limitando sua capacidade de gerenciá-los no caso de uma interrupção de energia ou outra interrupção do data center.

- Faça backup da VM do provedor VASA regularmente. No mínimo, crie instantâneos por hora do armazenamento de dados tradicional que contém o Fornecedor VASA. Para obter mais informações sobre como proteger e recuperar o provedor VASA, consulte este "Artigo da KB".

A figura a seguir mostra os componentes do vVols.



Backup e migração para a nuvem

Outro ponto forte da ONTAP é o amplo suporte à nuvem híbrida, unindo sistemas na nuvem privada local com funcionalidades de nuvem pública. Aqui estão algumas soluções de nuvem da NetApp que podem ser usadas em conjunto com o vSphere:

- **Ofertas de primeira linha.** Amazon FSx for NetApp ONTAP, Google Cloud NetApp Volumes e Azure NetApp Files fornecem serviços de armazenamento gerenciado de alto desempenho e multiprotocolo nos principais ambientes de nuvem pública. Eles podem ser usados diretamente pelo VMware Cloud on AWS (VMC on AWS), Azure VMware Solution (AVS) e Google Cloud VMware Engine (GCVE) como armazenamentos de dados ou armazenamento para sistemas operacionais convidados (GOS) e

instâncias de computação.

- **Serviços em Nuvem.** Use o NetApp Backup and Recovery ou o SnapMirror Cloud para proteger dados de sistemas locais usando armazenamento em nuvem pública. O NetApp Copy and Sync ajuda a migrar e manter seus dados sincronizados entre NAS e armazenamentos de objetos. O NetApp Disaster Recovery oferece uma solução econômica e eficiente para aproveitar as tecnologias NetApp como base para uma solução de recuperação de desastres robusta e capaz para DR para nuvem, DR para local e local para local.
- **FabricPool.** O FabricPool oferece disposição em camadas rápida e fácil para dados do ONTAP. Os blocos inativos podem ser migrados para um armazenamento de objetos em nuvens públicas ou em um armazenamento de objetos StorageGRID privado e são recuperados automaticamente quando os dados do ONTAP são acessados novamente. Ou use a categoria objeto como um terceiro nível de proteção para dados que já são gerenciados pelo SnapVault. Com essa abordagem, você pode "Armazene mais snapshots de suas VMs" fazer isso em sistemas de storage ONTAP primário e/ou secundário.
- **ONTAP Select.** Use o storage definido por software da NetApp para estender sua nuvem privada pela Internet para instalações e escritórios remotos, onde você pode usar o ONTAP Select para oferecer suporte a serviços de bloco e arquivos, bem como os mesmos recursos de gerenciamento de dados do vSphere que você tem em seu data center empresarial.

Ao projetar seus aplicativos baseados em VM, considere a mobilidade futura da nuvem. Por exemplo, em vez de colocar os arquivos de aplicativo e de dados juntos, use uma exportação LUN ou NFS separada para os dados. Isso permite que você migre a VM e os dados separadamente para serviços de nuvem.

Para um mergulho profundo em mais tópicos de segurança, consulte os seguintes recursos.

- "Documentação do ONTAP Select"
- "Documentação de backup e recuperação"
- "Documentação de recuperação de desastres"
- "Amazon FSX para NetApp ONTAP"
- "VMware Cloud na AWS"
- "O que é o Azure NetApp Files?"
- "Solução Azure VMware"
- "Google Cloud VMware Engine"
- "O que é o Google Cloud NetApp volumes?"

Criptografia para dados do vSphere

Hoje, há cada vez mais demandas para proteger dados em repouso por meio da criptografia. Embora o foco inicial tenha sido em informações financeiras e de saúde, há um interesse crescente em proteger todas as informações, sejam elas armazenadas em arquivos, bancos de dados ou outros tipos de dados.

Os sistemas executando o ONTAP facilitam a proteção de quaisquer dados com criptografia em repouso. O NetApp Storage Encryption (NSE) usa unidades com autocriptografia (SEDs) com ONTAP para proteger dados de SAN e nas. O NetApp também oferece o NetApp volume Encryption e o NetApp Aggregate Encryption como uma abordagem simples e baseada em software para encriptar volumes em qualquer unidade de disco. Esta criptografia de software não requer unidades de disco especiais ou gerenciadores de chaves externos e está disponível para clientes ONTAP sem nenhum custo adicional. Você pode fazer upgrade e começar a usá-lo sem qualquer interrupção para seus clientes ou aplicativos, e eles são validados de acordo com o padrão FIPS 140-2 nível 1, incluindo o Gerenciador de chaves integrado.

Existem várias abordagens para proteger os dados de aplicativos virtualizados em execução no VMware vSphere. Uma abordagem é proteger os dados com software dentro da VM no nível do SO convidado. Os hipervisores mais recentes, como o vSphere 6,5, agora oferecem suporte à criptografia no nível da VM como outra alternativa. No entanto, a criptografia do software NetApp é simples e fácil e tem esses benefícios:

- **Nenhum efeito na CPU do servidor virtual.** Alguns ambientes de servidor virtual precisam de cada ciclo de CPU disponível para seus aplicativos, mas os testes mostraram que até 5x recursos de CPU são necessários com criptografia no nível do hipervisor. Mesmo que o software de criptografia ofereça suporte ao conjunto de instruções AES-NI da Intel para descarregar a carga de trabalho de criptografia (como a criptografia do software NetApp), essa abordagem pode não ser viável devido à exigência de novas CPUs que não são compatíveis com servidores mais antigos.
- **Onboard Key Manager incluído.** A criptografia do software NetApp inclui um Gerenciador de chaves integrado sem custo adicional, o que facilita o início sem servidores de gerenciamento de chaves de alta disponibilidade que são complexos de comprar e usar.
- **Nenhum efeito na eficiência de armazenamento.** Técnicas de eficiência de storage, como deduplicação e compactação, são amplamente utilizadas atualmente e são essenciais para usar a Mídia de disco flash de maneira econômica. No entanto, os dados criptografados geralmente não podem ser desduplicados ou compatados. O hardware e a criptografia de storage da NetApp operam em um nível mais baixo e permitem o uso total dos recursos de eficiência de storage da NetApp líderes do setor, ao contrário de outras abordagens.
- **Criptografia granular fácil do datastore.** Com a criptografia de volume NetApp, cada volume recebe sua própria chave AES de 256 bits. Se você precisar alterá-lo, você pode fazê-lo com um único comando. Essa abordagem é ótima se você tiver vários locatários ou precisar provar criptografia independente para diferentes departamentos ou aplicativos. Essa criptografia é gerenciada no nível do datastore, o que é muito mais fácil do que gerenciar VMs individuais.

É simples começar a usar a criptografia de software. Depois que a licença for instalada, basta configurar o Gerenciador de chaves integrado especificando uma senha e, em seguida, criar um novo volume ou fazer uma movimentação de volume no lado do armazenamento para ativar a criptografia. A NetApp está trabalhando para adicionar suporte mais integrado aos recursos de criptografia em versões futuras de suas ferramentas VMware.

Para um mergulho profundo em mais tópicos de segurança, consulte os seguintes recursos.

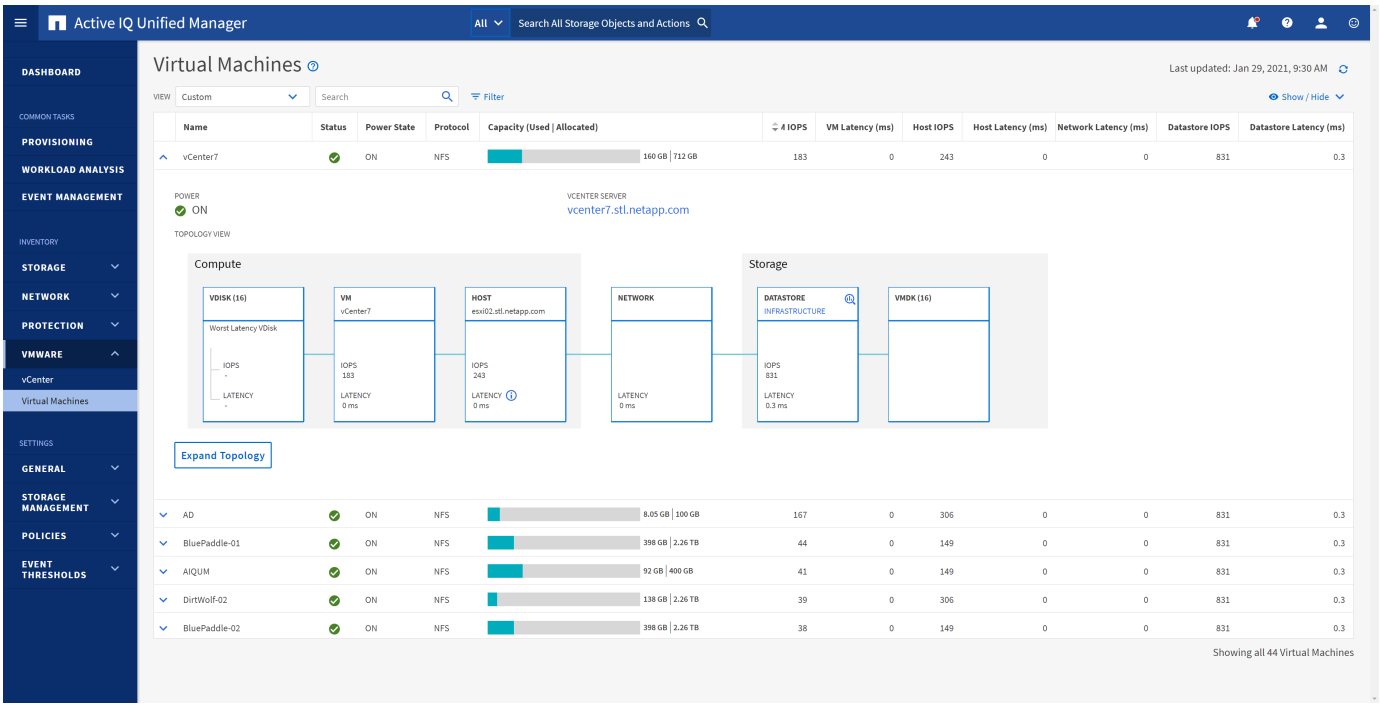
- "Relatórios técnicos de segurança"
- "Guias de proteção de segurança"
- "Documentação do produto de segurança e criptografia de dados do ONTAP"

Active IQ Unified Manager

O Active IQ Unified Manager fornece visibilidade das VMs em sua infraestrutura virtual e permite monitorar e solucionar problemas de storage e performance em seu ambiente virtual.

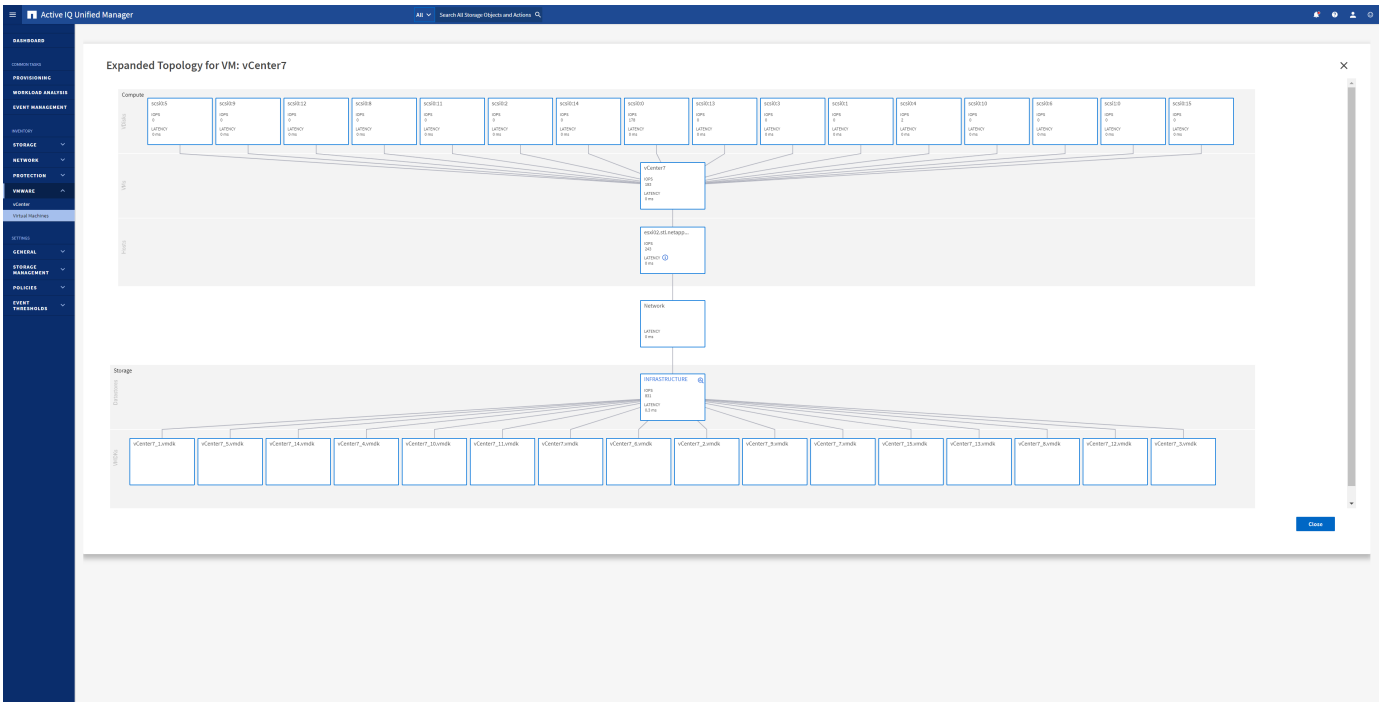
Uma implantação típica de infraestrutura virtual no ONTAP tem vários componentes espalhados pelas camadas de computação, rede e storage. Qualquer atraso de desempenho em uma aplicação de VM pode ocorrer devido a uma combinação de latências enfrentadas pelos vários componentes nas respetivas camadas.

A captura de tela a seguir mostra a exibição máquinas virtuais do Active IQ Unified Manager.



O Unified Manager apresenta o subsistema subjacente de um ambiente virtual em uma visualização topológica para determinar se ocorreu um problema de latência no nó de computação, na rede ou no storage. A visualização também destaca o objeto específico que causa o atraso de desempenho para tomar medidas corretivas e solucionar o problema subjacente.

A captura de tela a seguir mostra a topologia expandida do AIQUM.



VVols e gerenciamento baseado em políticas de storage

As VMware vSphere APIs for Storage Awareness (VASA) facilitam para um administrador de storage configurar datastores com recursos bem definidos e permitir

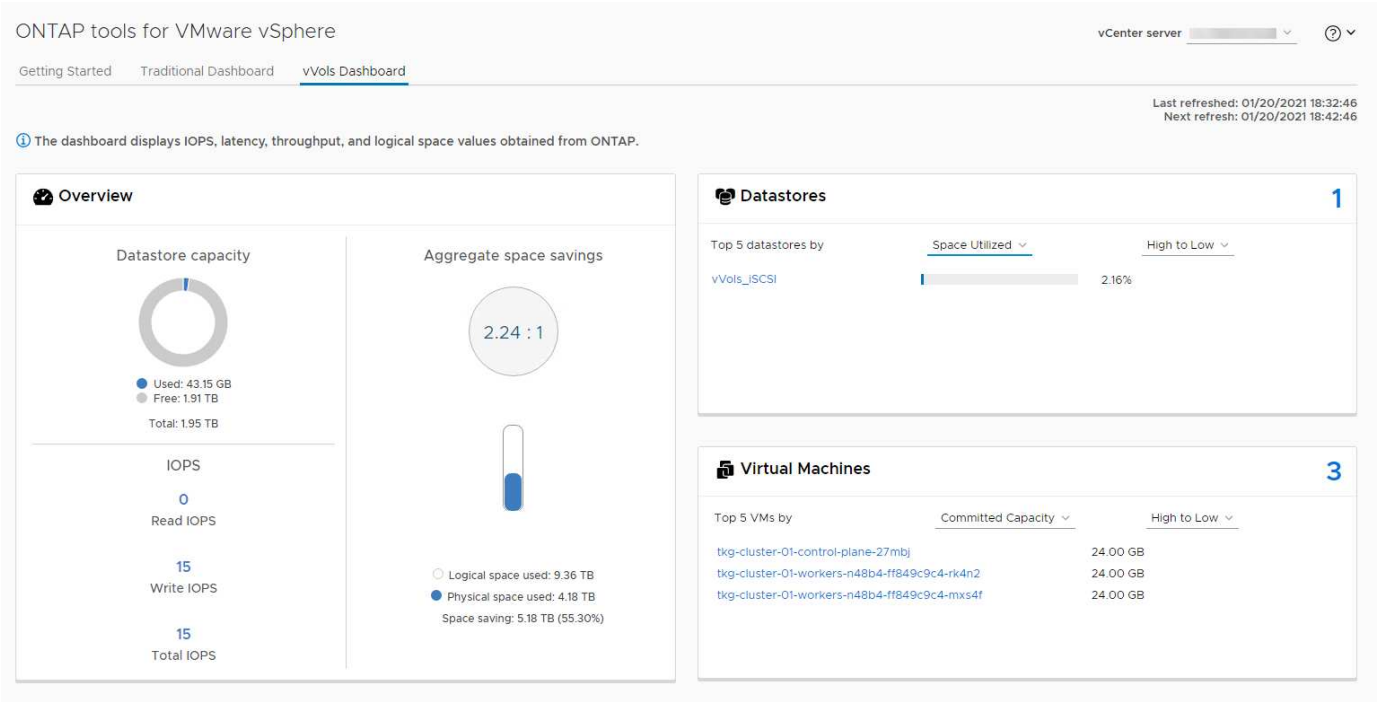
que o administrador da VM use-os sempre que necessário para provisionar VMs sem ter que interagir uns com os outros.

Vale a pena dar uma olhada nessa abordagem para ver como ela pode otimizar suas operações de storage de virtualização e evitar muito trabalho trivial.

Antes do VASA, os administradores de VM podiam definir políticas de armazenamento de VM, mas precisavam trabalhar com o administrador de armazenamento para identificar armazenamentos de dados apropriados, geralmente usando documentação ou convenções de nomenclatura. Com o VASA, o administrador de storage pode definir uma variedade de recursos de storage, incluindo desempenho, disposição em camadas, criptografia e replicação. Um conjunto de recursos para um volume ou um conjunto de volumes é chamado de Perfil de capacidade de armazenamento (SCP).

O SCP suporta QoS mínimo e/ou máximo para vVols de dados de uma VM. A QoS mínima é suportada apenas em sistemas AFF. As ferramentas do ONTAP para VMware vSphere incluem um painel que exibe o desempenho granular da VM e a capacidade lógica para vVols em sistemas ONTAP.

A figura a seguir mostra as ferramentas do ONTAP para o painel vVols do VMware vSphere 9,8.



Após a definição do perfil de funcionalidade de storage, ele pode ser usado para provisionar VMs usando a política de storage que identifica seus requisitos. O mapeamento entre a política de armazenamento de VM e o perfil de capacidade de armazenamento de dados permite que o vCenter exiba uma lista de datastores compatíveis para seleção. Essa abordagem é conhecida como gerenciamento baseado em políticas de storage.

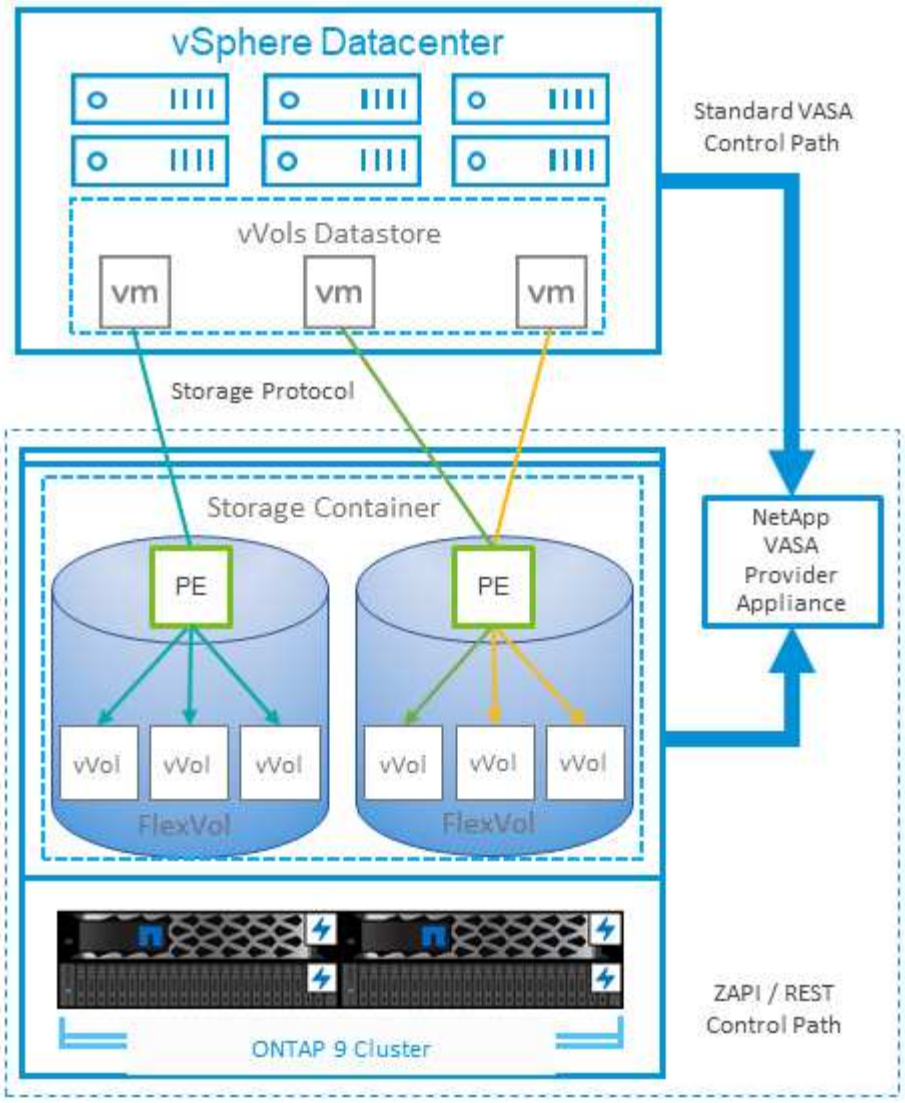
O VASA fornece a tecnologia para consultar o armazenamento e retornar um conjunto de recursos de armazenamento ao vCenter. Os fornecedores do VASA fornecem a tradução entre as APIs e construções do sistema de storage e as APIs da VMware que são entendidas pelo vCenter. O fornecedor VASA da NetApp para ONTAP é oferecido como parte das ferramentas da ONTAP para a VM do dispositivo VMware vSphere, e o plug-in do vCenter fornece a interface para provisionar e gerenciar datastores vVol, bem como a capacidade de definir perfis de capacidade de armazenamento (SCPs).

O ONTAP dá suporte aos armazenamentos de dados VMFS e NFS VVol. O uso do vVols com

armazenamentos de dados SAN traz alguns dos benefícios do NFS, como granularidade no nível da VM. Aqui estão algumas práticas recomendadas a serem consideradas e você pode encontrar informações adicionais em"TR-4400":

- Um datastore da VVol pode consistir em vários volumes FlexVol em vários nós dos clusters. A abordagem mais simples é um único datastore, mesmo quando os volumes têm capacidades diferentes. O SPBM garante que um volume compatível seja usado para a VM. No entanto, todos os volumes precisam fazer parte de um único SVM do ONTAP e acessá-los usando um único protocolo. Um LIF por nó para cada protocolo é suficiente. Evite o uso de várias versões do ONTAP em um único datastore da vVol porque as funcionalidades do storage podem variar entre lançamentos.
- Use as ferramentas do ONTAP para o plug-in do VMware vSphere para criar e gerenciar datastores da evolução. Além de gerenciar o datastore e seu perfil, ele cria automaticamente um endpoint de protocolo para acessar os vVols, se necessário. Se os LUNs forem usados, observe que os PES de LUN são mapeados usando IDs de LUN 300 e superiores. Verifique se a configuração do sistema avançado do host ESXi `Disk.MaxLUN` permite um número de ID LUN maior que 300 (o padrão é 1.024). Execute esta etapa selecionando o host ESXi no vCenter, a guia Configurar e localize `Disk.MaxLUN` na lista de Configurações avançadas do sistema.
- Não instale nem migre o provedor VASA, o vCenter Server (baseado em appliance ou Windows) ou as ferramentas do ONTAP para o próprio VMware vSphere em um datastore vVols, porque eles são mutuamente dependentes, limitando sua capacidade de gerenciá-los no caso de uma interrupção de energia ou outra interrupção do data center.
- Faça backup da VM do provedor VASA regularmente. No mínimo, crie instantâneos por hora do armazenamento de dados tradicional que contém o Fornecedor VASA. Para obter mais informações sobre como proteger e recuperar o provedor VASA, consulte este "Artigo da KB".

A figura a seguir mostra os componentes do vVols.



Programador de recursos distribuídos do VMware Storage

O VMware Storage Distributed Resource Scheduler (SDRS) é um recurso do vSphere que coloca automaticamente as VMs em um cluster de datastore com base na latência de e/S atual e no uso do espaço.

Em seguida, ele move a VM ou VMDKs sem interrupções entre os armazenamentos de dados em um cluster de datastore (também chamado de pod), selecionando o melhor datastore no qual colocar a VM ou VMDKs no cluster do datastore. Um cluster de datastore é um conjunto de datastores semelhantes que são agregados em uma única unidade de consumo da perspetiva do administrador do vSphere.

Ao usar SDRS com ferramentas do ONTAP para VMware vSphere, primeiro você deve criar um datastore com o plug-in, usar o vCenter para criar o cluster do datastore e, em seguida, adicionar o datastore a ele. Após a criação do cluster do datastore, armazenamentos de dados adicionais podem ser adicionados ao cluster do datastore diretamente do assistente de provisionamento na página Detalhes.

Outras práticas recomendadas da ONTAP para SDRS incluem o seguinte:

- Não use SDRS a menos que você tenha um requisito específico para fazê-lo.
  - OS SDRS não são necessários ao usar o ONTAP. OS SDRS não estão cientes dos recursos de

eficiência de storage da ONTAP, como deduplicação e compactação, portanto, podem tomar decisões que não são ideais para o seu ambiente.

- OS SDRS não estão cientes das políticas de QoS do ONTAP, portanto, podem tomar decisões que não são ideais para o desempenho.
- OS SDRS não conhecem as cópias snapshot do ONTAP, portanto, podem tomar decisões que fazem com que os snapshots cresçam exponencialmente. Por exemplo, mover uma VM para outro datastore cria novos arquivos no novo datastore, o que faz com que o snapshot cresça. Isso é especialmente verdadeiro para VMs com discos grandes ou muitos snapshots. Então, se a VM for movida de volta para o datastore original, o snapshot no datastore original aumentará ainda mais.

Se você usar SDRS, considere as seguintes práticas recomendadas:

- Todos os armazenamentos de dados no cluster devem usar o mesmo tipo de armazenamento (como SAS, SATA ou SSD), ser todos os armazenamentos de dados VMFS ou NFS e ter as mesmas configurações de replicação e proteção.
- Considere usar SDRS no modo padrão (manual). Essa abordagem permite que você analise as recomendações e decida se as aplicará ou não. Esteja ciente desses efeitos das migrações VMDK:
  - Quando OS SDRS movem VMDKs entre armazenamentos de dados, qualquer economia de espaço da clonagem ou deduplicação do ONTAP pode ser reduzida, dependendo de quão bem ele deduplica ou compacta no destino.
  - Depois que OS SDRS movem VMDKs, o NetApp recomenda recriar os snapshots no datastore de origem porque o espaço é bloqueado pela VM que foi movida.
  - Mover VMDKs entre armazenamentos de dados no mesmo agregado tem poucos benefícios, e OS SDRS não têm visibilidade de outras cargas de trabalho que possam compartilhar o agregado.

Mais informações sobre SDRS podem ser encontradas na documentação da VMware em "Storage DRS FAQ".

Host ESXi recomendado e outras configurações do ONTAP

A NetApp desenvolveu um conjunto de configurações de host ESXi ideais para protocolos NFS e Block. Orientações específicas também são fornecidas para configurações de multipathing e tempo limite de HBA para o comportamento adequado com o ONTAP com base nos testes internos do NetApp e VMware.

Esses valores são facilmente definidos usando as ferramentas do ONTAP para VMware vSphere: Na página de visão geral das ferramentas do ONTAP, role para baixo até a parte inferior e clique em aplicar configurações recomendadas no portlet de conformidade do host ESXi.

Aqui estão as configurações de host recomendadas para todas as versões atualmente suportadas do ONTAP.

* Configuração do host*	Valor recomendado NetApp	Reinicialização necessária
Configuração Avançada do ESXi		
VMFS3.HardwareAcceleratedLocking	Manter padrão (1)	Não
VMFS3.EnableBlockDelete	Mantenha o padrão (0), mas pode ser alterado se necessário. Para obter mais informações, consulte "Recuperação de espaço para VMFS5 máquinas virtuais"	Não

* Configuração do host*	Valor recomendado NetApp	Reinicialização necessária
VMFS3.EnableVMFS6Unmap	Mantenha a predefinição (1) para obter mais informações, consulte "VMware vSphere APIs: Integração de array (VAAI)"	Não
Configurações NFS		
NewSyncInterval	Se você não estiver usando o vSphere CSI for Kubernetes, defina per "VMware KB 386364"	Não
NET.TcpipHeapSize	VSphere 6,0 ou posterior, definido como 32. Todas as outras configurações NFS, definidas como 30	Sim
NET.TcpipHeapMax	Defina como 512MB para a maioria das versões do vSphere 6.X. Defina como padrão (1024MB) para 6.5U3, 6.7U3 e 7,0 ou posterior.	Sim
NFS.MaxVolumes	VSphere 6,0 ou posterior, defina como 256 todas as outras configurações NFS definidas como 64.	Não
NFS41.MaxVolumes	VSphere 6,0 ou posterior, definido como 256.	Não
1	VSphere 6,0 ou posterior, definido como 128	Sim
NFS.HeartbeatMaxFailures	Definido como 10 para todas as configurações NFS	Não
Frequência NFS.HeartbeatFrequency	Definido como 12 para todas as configurações NFS	Não
NFS.HeartbeatTimeout	Definido como 5 para todas as configurações NFS.	Não
Descrição: Sunrpc.MaxConnPerIP	vSphere 7.0 a 8.0, definido como 128. Esta configuração é ignorada nas versões do ESXi posteriores à 8.0.	Não
Configurações FC/FCoE		

* Configuração do host*	Valor recomendado NetApp	Reinicialização necessária
Política de seleção de caminho	Defina como RR (round robin) quando os caminhos FC com ALUA são usados. Defina como FIXO para todas as outras configurações. Definir esse valor como RR ajuda a fornecer balanceamento de carga em todos os caminhos ativos/otimizados. O VALOR FIXO é para configurações mais antigas e não-ALUA e ajuda a impedir e/S de proxy Em outras palavras, ele ajuda a evitar que a e/S vá para o outro nó de um par de HA (high-availability) em um ambiente com Data ONTAP operando no modo 7D.	Não
Disk.QFullSampleSize	Defina como 32 para todas as configurações. Definir este valor ajuda a evitar erros de e/S.	Não
Disk.QFullThreshold	Defina como 8 para todas as configurações. Definir este valor ajuda a evitar erros de e/S.	Não
Tempos limite Emulex FC HBA	Use o valor padrão.	Não
Tempos limite do QLogic FC HBA	Use o valor padrão.	Não
Definições iSCSI		
Política de seleção de caminho	Defina como RR (round robin) para todos os caminhos iSCSI. Definir esse valor como RR ajuda a fornecer balanceamento de carga em todos os caminhos ativos/otimizados.	Não
Disk.QFullSampleSize	Defina como 32 para todas as configurações. Definir este valor ajuda a evitar erros de e/S	Não
Disk.QFullThreshold	Defina como 8 para todas as configurações. Definir este valor ajuda a evitar erros de e/S.	Não

A opção de configuração avançada NFS MaxQueueDepth pode não funcionar como esperado ao usar o VMware vSphere ESXi 7.0.1 e o VMware vSphere ESXi 7,0.2. Referência "VMware KB 86331" para obter mais informações.

As ferramentas do ONTAP também especificam certas configurações padrão ao criar volumes e LUNs do ONTAP FlexVol:

Ferramenta ONTAP	Predefinição

Reserva de snapshot (-percentagem-Snapshot-space)	0
Reserva fracionária (-reserva fracionária)	0
Atualização da hora de acesso (-atime-update)	Falso
Leitura mínima (-min-readahead)	Falso
Instantâneos programados	Nenhum
Eficiência de storage	Ativado
Garantia de volume	Nenhum (thin Provisioning)
Tamanho automático do volume	grow_shrink
Reserva de espaço LUN	Desativado
Alocação de espaço LUN	Ativado

Configurações de multipath para desempenho

Embora não esteja configurado atualmente pelas ferramentas ONTAP disponíveis, o NetApp sugere estas opções de configuração:

- Ao usar sistemas não ASA em ambientes de alto desempenho ou ao testar 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. Ver"VMware KB 2069356" para mais informações.
- No vSphere 6.7 Update 1, a VMware introduziu um novo mecanismo de balanceamento de carga de latência para o Round Robin PSP. A opção de latência agora também está disponível ao usar o HPP (High Performance Plugin) com namespaces NVMe e com vSphere 8.0u2 e posteriores, LUNs conectados por iSCSI e FCP. A nova opção considera a largura de banda de E/S e a latência do caminho ao selecionar o caminho ideal para E/S. A NetApp recomenda usar a opção de latência em ambientes com conectividade de caminho não equivalente, como casos com mais saltos de rede em um caminho do que em outro, ou ao usar um sistema NetApp ASA . Ver "Alterar parâmetros padrão para latência Round Robin" para maiores informações.

Documentação adicional

Para FCP e iSCSI com vSphere, mais detalhes podem ser encontrados em para FCP e iSCSI com vSphere 8, mais detalhes podem ser encontrados em "Use o VMware vSphere 8.x com o ONTAP"para NVMe-of com vSphere 7. Para NVMe-of com vSphere 8, mais detalhes podem ser encontrados em "Para NVMe-of, mais detalhes podem ser encontrados em Configuração de host NVMe-of para ESXi 7.x com ONTAP" para NVMe-of com vSphere 7"Use o VMware vSphere 7.x com o ONTAP". Mais detalhes podem ser encontrados em "Para NVMe-of, mais detalhes podem ser encontrados em Configuração de host NVMe-of para ESXi 8.x com ONTAP"

Volumes virtuais (vVols) com as ferramentas do ONTAP 10

Visão geral

O ONTAP é uma solução de storage líder para ambientes VMware vSphere há mais de duas décadas e continua adicionando recursos inovadores para simplificar o

gerenciamento e reduzir custos.

Este documento abrange os recursos do ONTAP para volumes virtuais do VMware vSphere (vVols), incluindo as informações mais recentes sobre produtos e casos de uso, juntamente com as práticas recomendadas e outras informações para simplificar a implantação e reduzir erros.

> Essa documentação substitui os relatórios técnicos publicados anteriormente *TR-4400: VMware vSphere Virtual volumes (vVols) com o ONTAP*

As práticas recomendadas complementam outros documentos, como guias e listas de compatibilidade. Eles são desenvolvidos com base em testes de laboratório e extensa experiência de campo por engenheiros e clientes da NetApp. Eles podem não ser as únicas práticas que funcionam ou são suportadas, mas são geralmente as soluções mais simples que atendem às necessidades da maioria dos clientes.

> Este documento foi atualizado para incluir novos recursos do vVols encontrados na atualização 3 do vSphere 8,0, na versão 10,4 das ferramentas do ONTAP e nos novos sistemas NetApp ASA.

Visão geral dos volumes virtuais (vVols)

A NetApp começou a trabalhar com a VMware para oferecer suporte às APIs do vSphere for Storage Awareness (VASA) para o vSphere 5 em 2012. Este provedor VASA inicial permitiu a definição de recursos de armazenamento em um perfil que poderia ser usado para filtrar datastores ao provisionar e verificar a conformidade com a política posteriormente. Com o tempo, isso evoluiu para adicionar novos recursos para permitir mais automação no provisionamento, bem como adicionar volumes virtuais ou vVols, onde objetos de storage individuais são usados para arquivos de máquina virtual e discos virtuais. Esses objetos podem ser LUNs, arquivos e agora com os namespaces vSphere 8 - NVMe (usados com as ferramentas do ONTAP 9.13P2). A NetApp trabalhou em estreita colaboração com a VMware como parceiro de referência do vVols lançado com o vSphere 6 em 2015 e novamente como parceiro de design do vVols usando o NVMe sobre Fabrics no vSphere 8. A NetApp continua a aprimorar os vVols para aproveitar os recursos mais recentes do ONTAP.

Existem vários componentes a ter em conta:

Fornecedor VASA

Este é o componente de software que lida com a comunicação entre o VMware vSphere e o sistema de storage. Para o ONTAP, o provedor VASA é executado em um dispositivo conhecido como ferramentas ONTAP para VMware vSphere (ferramentas ONTAP para abreviação). As ferramentas do ONTAP também incluem um plug-in do vCenter, um adaptador de replicação de armazenamento (SRA) para o VMware Site Recovery Manager e um servidor de API REST para criar sua própria automação. Depois que as ferramentas do ONTAP são configuradas e registradas no vCenter, há pouca necessidade de interagir diretamente com o sistema ONTAP, já que quase todas as suas necessidades de armazenamento podem ser gerenciadas diretamente na IU do vCenter ou por meio da automação da API REST.

Ponto final do protocolo (PE)

O endpoint do protocolo é um proxy para e/S entre os hosts ESXi e o datastore vVols. O Fornecedor ONTAP VASA cria-os automaticamente, seja um LUN de ponto de extremidade de protocolo (4MB GB de tamanho) por FlexVol volume do armazenamento de dados vVols ou um ponto de montagem NFS por interface NFS (LIF) no nó de storage que hospeda um FlexVol volume no armazenamento de dados. O host ESXi monta esses pontos finais do protocolo diretamente em vez de LUNs e arquivos de disco virtuais individuais da Vevolve. Não é necessário gerenciar os endpoints do protocolo à medida que são criados, montados, desmontados e excluídos automaticamente pelo Provedor VASA, juntamente com quaisquer grupos de

interface ou políticas de exportação necessárias.

Ponto final do protocolo virtual (VPE)

Novidade no vSphere 8: Ao usar o NVMe sobre Fabrics (NVMe-of) com vVols, o conceito de endpoint de protocolo não é mais relevante no ONTAP. Em vez disso, um PE virtual é instanciado automaticamente pelo host ESXi para cada grupo ANA assim que a primeira VM é ativada. O ONTAP cria automaticamente grupos ANA para cada FlexVol volume usado pelo datastore.

Uma vantagem adicional ao usar o NVMe-of para vVols é que não há solicitações de vinculação necessárias do Fornecedor VASA. Em vez disso, o host ESXi lida internamente com a funcionalidade de vinculação do VPE. Isso reduz a oportunidade de uma tempestade de Vevolve para impactar o serviço.

Para obter mais informações, consulte a. "NVMe e Virtual volumes" "vmware.com"

Armazenamento de dados de volume virtual

O armazenamento de dados de Volume Virtual é uma representação lógica de um contêiner vVols , criado e mantido por um Provedor VASA. O contêiner representa um conjunto de capacidade de armazenamento fornecida por sistemas de armazenamento gerenciados pelo Provedor VASA. As ferramentas ONTAP suportam a alocação de múltiplos volumes FlexVol (referidos como volumes de suporte) a um único armazenamento de dados vVols , e esses armazenamentos de dados vVols podem abranger vários nós em um cluster ONTAP , combinando sistemas flash e híbridos com diferentes capacidades. O administrador pode criar novos volumes FlexVol usando o assistente de provisionamento ou a API REST, ou selecionar volumes FlexVol pré-criados para armazenamento de suporte, caso estejam disponíveis.

Volumes virtuais (vVols)

Os vVols são os arquivos e discos reais das máquinas virtuais armazenados no datastore vVols . O termo vVol (singular) refere-se a um único arquivo específico, LUN ou namespace. O ONTAP cria namespaces NVMe, LUNs ou arquivos, dependendo do protocolo usado pelo armazenamento de dados. Existem vários tipos distintos de vVols; os mais comuns são Config (o único com VMFS, contendo arquivos de metadados como o arquivo VMX da VM), Data (disco virtual ou VMDK) e Swap (criado quando a VM é ligada). Os vVols protegidos pela criptografia de VM da VMware serão do tipo Outro. A criptografia de máquinas virtuais VMware não deve ser confundida com a criptografia de volumes ou agregados do ONTAP .

Gestão baseada em políticas

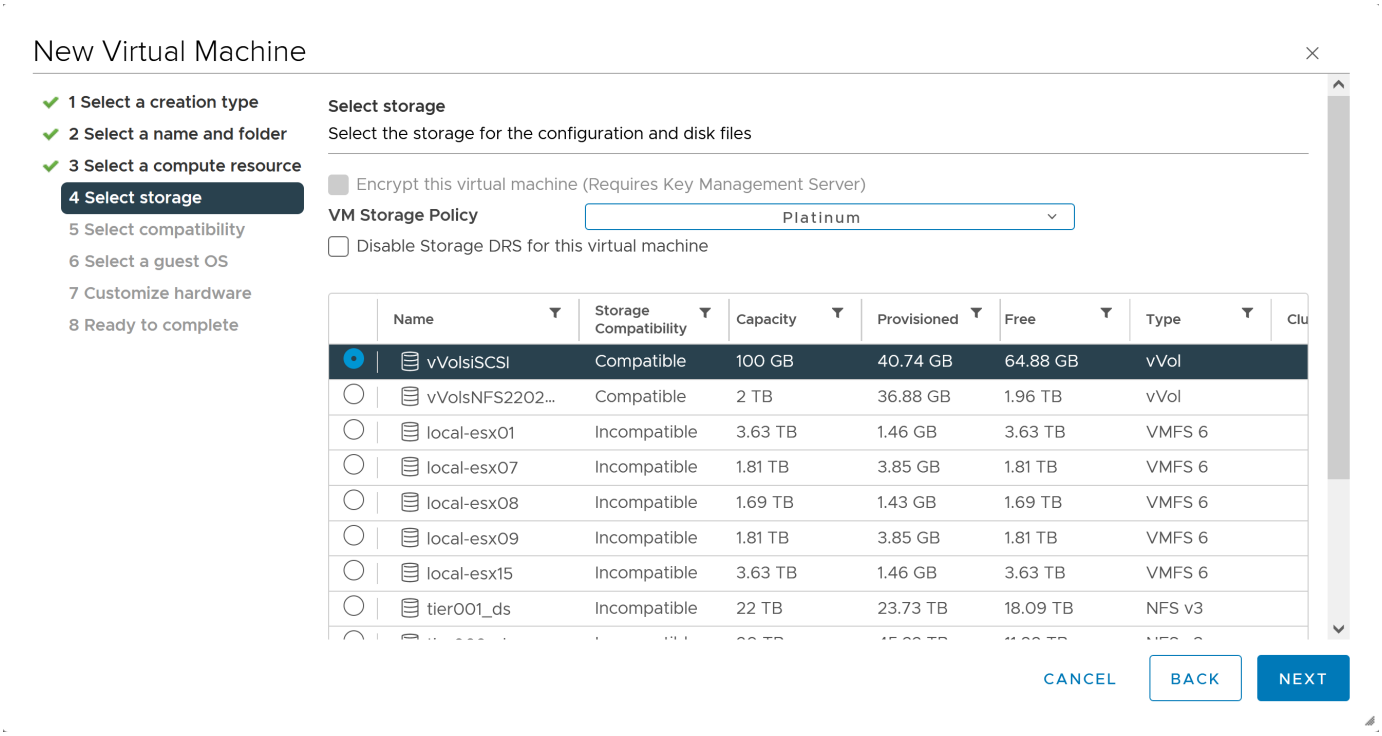
As APIs do VMware vSphere para Conscientização de Armazenamento (VASA) facilitam para um administrador de máquinas virtuais usar quaisquer recursos de armazenamento necessários para provisionar máquinas virtuais sem precisar interagir com sua equipe de armazenamento. Antes do VASA, os administradores de VMs podiam definir políticas de armazenamento de VMs, mas precisavam trabalhar com seus administradores de armazenamento para identificar os datastores apropriados, geralmente usando documentação ou convenções de nomenclatura. Com o VASA, os administradores do vCenter com as permissões apropriadas podem definir uma variedade de recursos de armazenamento que os usuários do vCenter podem usar para provisionar máquinas virtuais. O mapeamento entre a política de armazenamento da VM e os recursos do datastore permite que o vCenter exiba uma lista de datastores compatíveis para seleção, além de possibilitar que outras tecnologias, como o VCF (anteriormente conhecido como Aria e vRealize) Automation ou o VMware vSphere Kubernetes Service (VKS), selecionem automaticamente o armazenamento a partir de uma política atribuída. Essa abordagem é conhecida como gerenciamento baseado em políticas de armazenamento. Embora as regras do provedor VASA e as políticas de armazenamento de VM também possam ser usadas com datastores tradicionais, nosso foco aqui está nos datastores vVols .

Políticas de storage de VM

As políticas de armazenamento de VM são criadas no vCenter em políticas e perfis. Para vVols, crie um conjunto de regras usando regras do provedor do tipo de storage do NetApp vVols. As ferramentas do ONTAP 10.X agora oferecem uma abordagem mais simples do que as ferramentas do ONTAP 9.X, permitindo que você especifique diretamente atributos de armazenamento na própria política de armazenamento de VM.

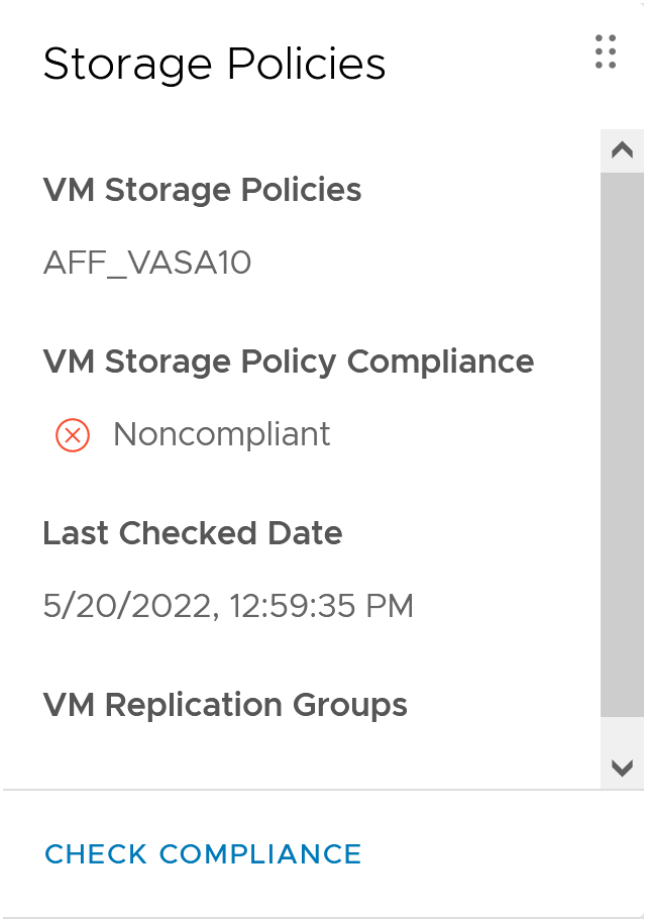
Como mencionado acima, o uso de políticas pode ajudar a simplificar a tarefa de provisionar uma VM ou VMDK. Basta selecionar uma política apropriada e o Fornecedor VASA mostrará os datastores da vols que suportam essa política e colocam a evolução em um FlexVol volume individual que esteja em conformidade.

Implante a VM usando a Política de storage



Após o provisionamento de uma VM, o provedor VASA continuará verificando a conformidade e alertará o administrador da VM com um alarme no vCenter quando o volume de suporte deixar de estar em conformidade com a política.

Conformidade com a política de storage da VM



Suporte para NetApp vVols

O ONTAP oferece suporte à especificação VASA desde seu lançamento inicial em 2012. Embora outros sistemas de armazenamento NetApp possam suportar VASA, este documento se concentra nas versões atualmente suportadas do ONTAP 9.

ONTAP

Além do ONTAP 9 nos sistemas AFF, ASA e FAS , o NetApp oferece suporte a cargas de trabalho VMware no ONTAP Select, Amazon FSx para NetApp com VMware Cloud na AWS, Azure NetApp Files com Azure VMware Solution, Google Cloud NetApp Volumes com Google Cloud VMware Engine e NetApp Private Storage no Equinix, mas a funcionalidade específica pode variar com base no provedor de serviços e na conectividade de rede disponível.

No momento da publicação, os ambientes de hiperescala estão limitados a datastores NFS v3 tradicionais; portanto, os vVols estão disponíveis apenas com sistemas ONTAP locais ou sistemas conectados à nuvem que oferecem a funcionalidade completa de um sistema local, como aqueles hospedados por parceiros e provedores de serviços da NetApp em todo o mundo.

_Para obter mais informações sobre o ONTAP, "Documentação do produto ONTAP" consulte _

_Para obter mais informações sobre as práticas recomendadas do ONTAP e do VMware vSphere, "TR-4597"consulte _

Benefícios de usar vVols com ONTAP

Quando a VMware introduziu o suporte a vVols com o VASA 2.0 em 2015, descreveu-o como "uma estrutura

de integração e gestão que oferece um novo modelo operacional para armazenamento externo (SAN/NAS)". Este modelo operacional oferece diversas vantagens em conjunto com o armazenamento ONTAP .

Gestão baseada em políticas

Conforme abordado na seção 1.2, o gerenciamento baseado em políticas permite que as VMs sejam provisionadas e posteriormente gerenciadas usando políticas predefinidas. Isso pode ajudar as operações de TI de diversas maneiras:

- **Aumente a velocidade.** As ferramentas ONTAP eliminam a necessidade de o administrador do vCenter abrir chamados com a equipe de armazenamento para atividades de provisionamento de armazenamento. No entanto, as funções RBAC das ferramentas ONTAP no vCenter e no sistema ONTAP ainda permitem equipes independentes (como equipes de armazenamento) ou atividades independentes da mesma equipe, restringindo o acesso a funções específicas, se desejado.
- **Provisionamento mais inteligente.** Os recursos do sistema de storage podem ser expostos por meio das APIs VASA, permitindo que os fluxos de trabalho de provisionamento aproveitem recursos avançados sem que o administrador da VM precise entender como gerenciar o sistema de storage.
- **Provisionamento mais rápido.** Diferentes recursos de storage podem ser suportados em um único armazenamento de dados e selecionados automaticamente, conforme apropriado, para uma VM com base na política de VM.
- **Evite erros.** As políticas de storage e VM são desenvolvidas com antecedência e aplicadas conforme necessário, sem precisar personalizar o storage sempre que uma VM é provisionada. Os alarmes de conformidade são gerados quando as funcionalidades de storage são desviadas das políticas definidas. Como mencionado anteriormente, as SCPs tornam o provisionamento inicial previsível e repetível, ao mesmo tempo que basear as políticas de armazenamento de VM nos SCPs garante um posicionamento preciso.
- * Melhor gerenciamento de capacidade. * As ferramentas VASA e ONTAP possibilitam visualizar a capacidade de armazenamento até o nível de agregado individual, se necessário, e fornecem várias camadas de alertas no evento que a capacidade começa a ficar baixa.

Gerenciamento granular de VM na SAN moderna

Os sistemas de armazenamento SAN que utilizam Fibre Channel e iSCSI foram os primeiros a serem suportados pela VMware para ESX, mas não possuíam a capacidade de gerenciar arquivos e discos individuais de máquinas virtuais a partir do sistema de armazenamento. Em vez disso, os LUNs são provisionados e o VMFS gerencia os arquivos individuais. Isso dificulta o gerenciamento direto, pelo sistema de armazenamento, do desempenho, da clonagem e da proteção do armazenamento de máquinas virtuais individuais. Os vVols oferecem a granularidade de armazenamento que os clientes que usam armazenamento NFS já desfrutam, com os recursos robustos e de alto desempenho de SAN do ONTAP.

Agora, com o vSphere 8 e as ONTAP tools for VMware vSphere 9.12 e versões posteriores, esses mesmos controles granulares usados pelos vVols para protocolos legados baseados em SCSI estão disponíveis no SAN Fibre Channel moderno usando NVMe over Fabrics para um desempenho ainda maior em escala. Com a atualização 1 do vSphere 8.0, agora é possível implantar uma solução NVMe completa de ponta a ponta usando vVols sem qualquer tradução de E/S na pilha de armazenamento do hipervisor.

Maiores funcionalidades de descarga de storage

Embora a VAAI ofereça uma variedade de operações que são descarregadas para armazenamento, existem algumas lacunas que são abordadas pelo provedor VASA. O SAN VAAI não consegue descarregar snapshots gerenciados pelo VMware para o sistema de armazenamento. O NFS VAAI pode descarregar snapshots gerenciados por VMs, mas existem limitações impostas a uma VM com snapshots nativos de armazenamento. Como os vVols usam LUNs, namespaces ou arquivos individuais para discos de máquinas virtuais, o ONTAP

pode clonar os arquivos ou LUNs de forma rápida e eficiente para criar snapshots granulares de VM que não exigem mais arquivos delta. O NFS VAAI também não oferece suporte ao descarregamento de operações de clonagem para migrações Storage vMotion a quente (com o sistema ligado). A máquina virtual deve ser desligada para permitir o descarregamento da migração ao usar o VAAI com armazenamentos de dados NFS tradicionais. O provedor VASA nas ferramentas ONTAP permite clones quase instantâneos e com uso eficiente de armazenamento para migrações a quente e a frio, além de suportar cópias quase instantâneas para migrações entre volumes virtuais (vVols). Graças a esses benefícios significativos de eficiência de armazenamento, você poderá aproveitar ao máximo as cargas de trabalho do vVols no âmbito do "Garantia de eficiência" programa. Da mesma forma, se as clonagens entre volumes usando VAAI não atenderem aos seus requisitos, você provavelmente conseguirá resolver seu desafio de negócios graças às melhorias na experiência de cópia com vVols.

Casos de uso comuns para vVols

Além desses benefícios, também vemos esses casos de uso comuns para o storage da evolução:

- **Provisionamento sob demanda de VMs**
  - IaaS provedor de serviços ou nuvem privada.
  - Aproveite a automação e a orquestração por meio do pacote Aria (anteriormente vRealize), OpenStack e assim por diante.
- **Discos de primeira Classe (FCDs)**
  - Volumes persistentes do VMware vSphere Kubernetes Service (VKS).
  - Fornecer serviços semelhantes ao Amazon EBS por meio de gerenciamento independente do ciclo de vida do VMDK.
- **Provisionamento sob demanda de VMs temporárias**
  - Laboratórios de teste/desenvolvimento
  - Ambientes de treinamento

Benefícios comuns com vVols

Quando usados em seu pleno benefício, como nos casos de uso acima, o vVols fornece as seguintes melhorias específicas:

- Os clones são criados rapidamente dentro de um único volume ou em vários volumes em um cluster ONTAP , o que representa uma vantagem em comparação com os clones tradicionais habilitados para VAAI. Eles também são eficientes em termos de armazenamento. Os clones dentro de um volume usam o clone de arquivo ONTAP , que é semelhante aos volumes FlexClone e armazena apenas as alterações do arquivo/LUN/namespace do vVol de origem. Dessa forma, máquinas virtuais (VMs) de longo prazo para produção ou outros fins de aplicação são criadas rapidamente, ocupam espaço mínimo e podem se beneficiar da proteção em nível de VM (usando o plug-in NetApp SnapCenter para VMware vSphere, snapshots gerenciados pela VMware ou backup VADP) e do gerenciamento de desempenho (com QoS do ONTAP). A clonagem entre volumes é muito mais rápida com vVols do que com VAAI, porque com VASA podemos criar o clone e permitir o acesso a ele no destino antes que a cópia seja concluída. Os blocos de dados são copiados como um processo em segundo plano para preencher o vVol de destino. Isso é semelhante à forma como a movimentação não disruptiva de LUNs do ONTAP funciona para LUNs tradicionais.
- Os vVols são a tecnologia de armazenamento ideal ao usar o TKG com o vSphere CSI, fornecendo classes de armazenamento discretas e capacidades gerenciadas pelo administrador do vCenter.
- Serviços semelhantes ao Amazon EBS podem ser fornecidos por meio de FCDs porque um VMDK de FCD, como o nome sugere, é um elemento de primeira classe no vSphere e possui um ciclo de vida que

pode ser gerenciado independentemente, separado das VMs às quais possa estar associado.

Lista de verificação

Use esta lista de verificação de instalação para garantir uma implantação bem-sucedida (atualizada para 10,3 e posterior).

1 **Planejamento inicial**

- Antes de iniciar a instalação, deve verificar o "Ferramenta de Matriz de interoperabilidade (IMT)" para garantir que a sua implementação foi certificada.
- Determine o tamanho e o tipo de configuração de ferramentas do ONTAP de que o seu ambiente precisa. Consulte a "Limites de configuração para implantar as ferramentas do ONTAP para o VMware vSphere" para obter mais informações.
- Determine se você usará SVMs multitenant ou permitirá acesso total ao cluster. Se você estiver usando SVMs multitenant, precisará ter um LIF de gerenciamento de SVM em cada SVM a ser usado. Esse LIF deve ser acessível pela porta 443 pelas ferramentas do ONTAP.
- Determine se você usará Fibre Channel (FC) para conectividade de storage. Em caso afirmativo, você "configure o zoneamento" precisará nos switches FC para habilitar a conectividade entre os hosts ESXi e os LIFs FC da SVM.
- Determine se você usará o adaptador de replicação de armazenamento (SRA) das ferramentas ONTAP para o Gerenciador de recuperação de Site (SRM) ou recuperação de Site ao vivo (VLSR). Se assim for, terá de aceder à interface de gestão do servidor SRM/VLSR para instalar o SRA.
- Se você estiver usando a replicação do SnapMirror gerenciada por ferramentas do ONTAP (incluindo, entre outras, a sincronização ativa do SnapMirror), o administrador do ONTAP deve "Crie um relacionamento de pares de cluster no ONTAP" e "Criar um relacionamento entre pares SVM entre clusters no ONTAP" antes de poder usar as ferramentas do ONTAP com o SnapMirror.
- "Transferir" As ferramentas ONTAP OVA, e se necessário, o arquivo SRA tar.gz.

2 **Provisione endereços IP e Registros DNS**

- Solicite as seguintes informações de IP da sua equipe de rede. Os três primeiros endereços IP são necessários; os nós dois e três são usados para implantações de alta disponibilidade (HA) com escalabilidade horizontal. Registros de host DNS são necessários e todos os nomes de nós e todos os endereços devem estar na mesma VLAN e sub-rede.
- ONTAP Tools Endereço da aplicação "_ . _ . . ___
- Endereço de Serviços internos ' . . . _
- Nome de host DNS do nó "
- Endereço IP do nó "_ . _ . . ___
- Máscara de sub-rede " . . . _
- Gateway padrão '_ . . . _
- Servidor DNS 1 . . . ___
- Servidor DNS 2 . . . ___
- Domínio de pesquisa DNS__

- Nome de host DNS do nó dois (opcional) '__
- Endereço IP do nó dois (opcional) ' . . . ___
- Nome de host DNS do nó três (opcional) '__
- Endereço IP do nó três (opcional) "_ . . . ___
- Crie Registros DNS para todos os endereços IP acima.

3 Configuração de firewall de rede

- Abra as portas necessárias para os endereços IP acima indicados no firewall de rede. "Requisitos portuários"Consulte para obter a atualização mais recente.

4 Armazenamento

- É necessário um datastore em um dispositivo de armazenamento compartilhado. Opcionalmente, você pode usar uma biblioteca de conteúdo no mesmo armazenamento de dados do nó um para facilitar a clonagem rápida do modelo com o VAAI.
- Biblioteca de conteúdo (apenas necessária para HA
- Nó um datastore '__
- Nó dois datastore (opcional, mas recomendado para HA) '__
- Nó três datastore (opcional, mas recomendado para HA) '___

5 Implante os ÓVULOS

- Note que este passo pode levar até 45 minutos para ser concluído
- "Implante os ÓVULOS" Usando o cliente vSphere.
- Na etapa 3 da implantação DO OVA, selecione a opção "personalizar o hardware desta máquina virtual" e defina o seguinte na etapa 10:
- "Enable CPU Hot Add" (Ativar adição automática da CPU)
- "Memory Hot Plug" (ficha quente da memória)

6 Adicione vCenters às ferramentas do ONTAP

- "Adicione instâncias do vCenter Server" No Gerenciador de ferramentas do ONTAP.

7 Adicione backends de armazenamento às ferramentas do ONTAP

- "Configurar as funções de usuário do ONTAP e o Privileges" Usando o arquivo JSON incluído se não estiver usando admin.
- Se você pretende atribuir SVMs específicas aos vCenters usando multilocação de armazenamento em vez de usar credenciais de cluster ONTAP no vCenter, siga estas etapas:
- "clusters integrados" No Gerenciador de ferramentas do ONTAP e associá-las ao vCenters.
- "SVMs integradas" Nas ferramentas do ONTAP vCenter UI.

- Se **não** estiver usando SVMs multilocatários no vCenter:
- "clusters integrados" Diretamente nas ferramentas do ONTAP vCenter UI. Alternativamente, neste cenário, é possível adicionar SVMs diretamente quando não estiver utilizando vVols.

8 **Configurar serviços de dispositivo (opcional)**

- Para usar vVols, você deve primeiro "Edite as definições do aparelho e ative o serviço VASA". Ao mesmo tempo, revise os dois itens a seguir.
- Se você planeja usar vVols na produção, "ative a alta disponibilidade" com os dois endereços IP opcionais acima.
- Se você planeja usar o adaptador de replicação de armazenamento (SRA) das ferramentas do ONTAP para o Gerenciador de recuperação de Site da VMware ou recuperação de Site ao vivo, "Ative os serviços SRA".

9 **Certificados (opcional)**

- De acordo com a VMware, os certificados assinados pela CA são necessários se estiverem usando vVols com vários vCenters.
- Serviços VASA
- Os serviços administrativos '__

10 **Outras tarefas pós-implantação**

- Crie regras antiafinidade para VMs em uma implantação de HA.
- Se estiver usando HA, os nós vMotion do storage dois e três para separar armazenamentos de dados (opcional, mas recomendado).
- "utilize gerir certificados" No Gerenciador de ferramentas do ONTAP para instalar todos os certificados assinados pela CA necessários.
- Se você ativou o SRA para SRM/VLSR para proteger armazenamentos de dados tradicionais, "Configure o SRA no VMware Live Site Recovery Appliance".
- Configure backups nativos para "Perto de RPO zero".
- Configure backups regulares para outras Mídias de armazenamento.

Usando vVols com ONTAP

A chave para usar o vVols com o NetApp são as ferramentas do ONTAP para VMware vSphere, que servidores como a interface do provedor VASA (vSphere API for Storage Awareness) para os sistemas ONTAP 9 da NetApp.

As ferramentas do ONTAP também incluem extensões de IU do vCenter, serviços de API REST, adaptadores de replicação de armazenamento para VMware Site Recovery Manager / Live Site Recovery, ferramentas de monitoramento e configuração de host e uma série de relatórios que ajudam você a gerenciar melhor seu ambiente VMware.

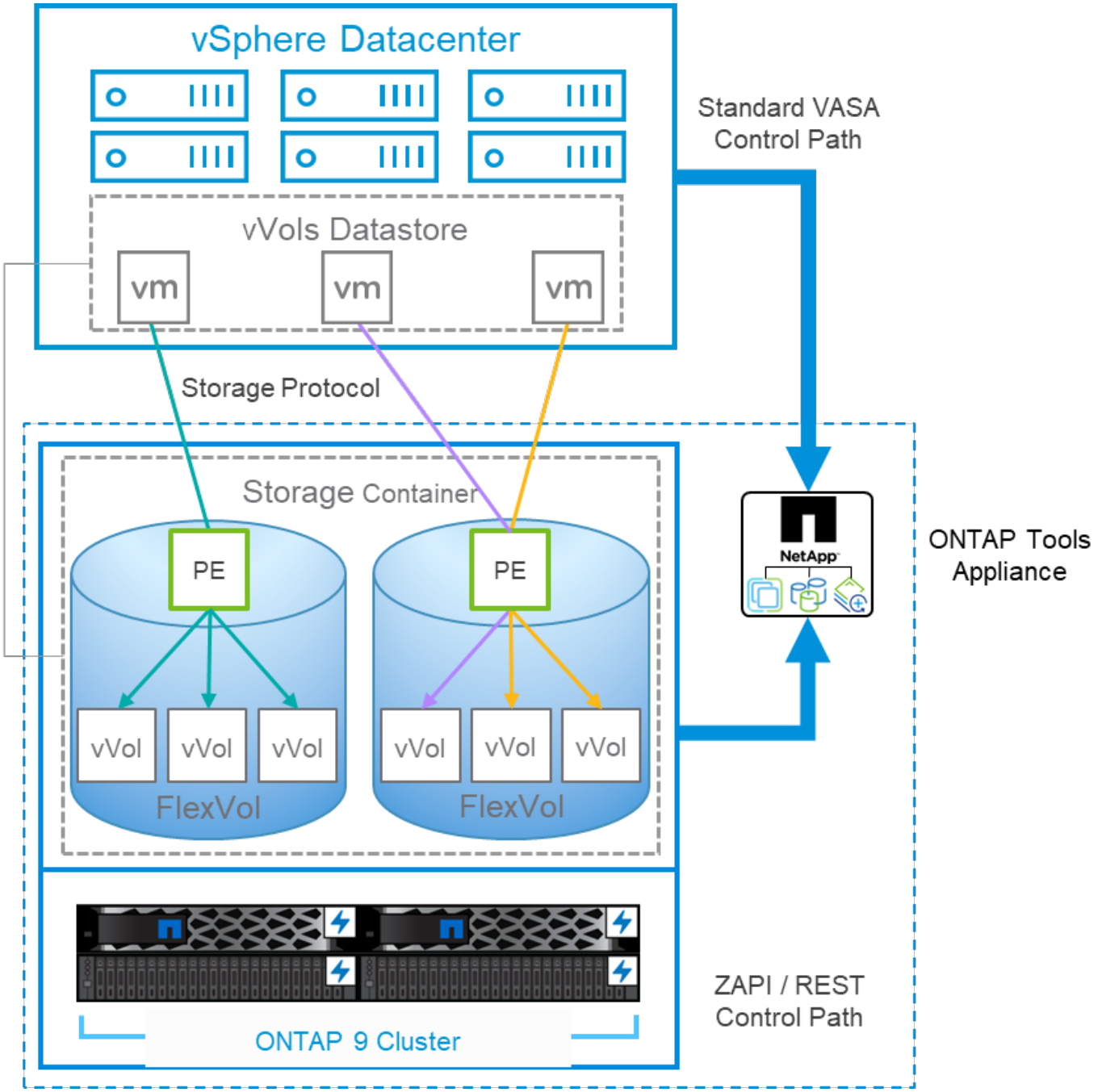
Produtos e Documentação

A licença do ONTAP One inclui todas as licenças necessárias para usar vVols com sistemas ONTAP. O único requisito adicional é o OVA de ferramentas ONTAP gratuitas, que atua como o provedor VASA. Em um ambiente vVols, o software VASA Provider traduz recursos de array em atributos orientados a políticas que podem ser aproveitados por meio das APIs VASA sem que o administrador do vSphere precise saber como os recursos são gerenciados nos bastidores. Isso permite o consumo dinâmico da capacidade de storage alocada com base na política, eliminando a necessidade de criar manualmente armazenamentos de dados tradicionais e gerenciar suas taxas de consumo de storage individuais. Em resumo, o vVols elimina toda a complexidade do gerenciamento do storage empresarial e o abstrai do administrador do vSphere para que eles possam se concentrar na camada de virtualização.

Para clientes que usam o VMware Cloud Foundation com VSAN, o vVols pode ser adicionado a qualquer domínio de gerenciamento ou workload como storage complementar. O vVols se integra perfeitamente ao VSAN por meio de uma estrutura de gerenciamento comum baseada em políticas de storage.

A próxima geração da família de versões do ONTAP Tools 10 moderniza os recursos anteriores com uma arquitetura escalável, em contentor, baseada em microsserviços, que é implementável através de um simples dispositivo de formato OVA no ESXi. O ONTAP Tools 10 combina todas as funcionalidades de três dispositivos e produtos antigos em uma única implantação. Para o gerenciamento do vVols, você usará as extensões intuitivas da IU do vCenter ou as APIs REST para as ferramentas do provedor VASA da ONTAP. Observe que o componente SRA é para datastores tradicionais; o VMware Site Recovery Manager não usa o SRA para vVols.

Arquitetura do provedor VASA ao usar iSCSI ou FCP com sistemas unificados ONTAP



Instalação do produto

Para novas instalações, implante o dispositivo virtual em seu ambiente vSphere. Depois de implantado, você pode fazer login na IU do gerente ou usar as APIS REST para escalar ou escalar sua implantação, vCenters integrados (isso Registra o plug-in com o vCenter), sistemas de armazenamento integrados e associar sistemas de storage aos seus vCenters. A integração de sistemas de storage na IU do Gerenciador de ferramentas do ONTAP e a associação de clusters com vCenters só é necessária se você planeja usar a alocação segura a vários clientes com SVMs dedicadas. Caso contrário, você pode simplesmente integrar o(s) cluster(s) de storage desejado(s) nas extensões de IU do ONTAP Tools vCenter ou usar as APIs REST.

Consulte "Implantando o storage vVols"neste documento, ou "Ferramentas do ONTAP para documentação do VMware vSphere".

A prática recomendada é armazenar suas ferramentas do ONTAP e dispositivos vCenter em datastores NFS ou VMFS tradicionais para evitar qualquer conflito de interdependência. Como as ferramentas do vCenter e do ONTAP precisam se comunicar entre si durante as operações do vVols, não instale nem mova os dispositivos de ferramentas do ONTAP ou os dispositivos do vCenter Server (VCSA) para o storage do vVols que estão gerenciando. Se isso acontecer, reinicializar os dispositivos de ferramentas do vCenter ou do ONTAP pode resultar em uma interrupção do acesso ao plano de controle e na incapacidade de inicializar o dispositivo.

As atualizações no local das ferramentas do ONTAP são suportadas usando o arquivo ISO de atualização disponível para download no "Ferramentas do ONTAP para VMware vSphere 10 - Downloads" site de suporte da NetApp (login necessário). Siga as "Atualize das ferramentas do ONTAP para o VMware vSphere 10.x para o 10,3" instruções do guia para atualizar o aparelho. Também é possível fazer uma atualização lado a lado das ferramentas ONTAP 9,13 para 10,3. "Migrar das ferramentas do ONTAP para o VMware vSphere 9.x para o 10,3"Consulte para obter um mergulho mais profundo sobre esse assunto.

Para dimensionar seu dispositivo virtual e entender os limites de configuração, consulte "Limites de configuração para implantar as ferramentas do ONTAP para o VMware vSphere"

Documentação do produto

A documentação a seguir está disponível para ajudá-lo a implantar ferramentas do ONTAP.

"Ferramentas do ONTAP para documentação do VMware vSphere"

Comece agora

- "Notas de lançamento"
- "Visão geral das ferramentas do ONTAP para VMware vSphere"
- "Implantar ferramentas do ONTAP"
- "Atualizar as ferramentas do ONTAP"

Use as ferramentas do ONTAP

- "Provisionar armazenamentos de dados"
- "Configurar controles de acesso baseados em função"
- "Configurar a alta disponibilidade"
- "Modifique as configurações do host ESXi"

Proteja e gerencie armazenamentos de dados

- "Configure o vSphere Metro Storage Cluster (vmsc) usando as ferramentas do ONTAP e a sincronização ativa do SnapMirror"
- "Proteja máquinas virtuais" Com SRM
- "Monitore clusters, armazenamentos de dados e máquinas virtuais"

Painel do Fornecedor VASA

O provedor VASA inclui um painel com informações de desempenho e capacidade para VMs vVols individuais. Essas informações são fornecidas diretamente do ONTAP para arquivos e LUNs da VEV, incluindo latência, IOPS, taxa de transferência e muito mais. Ele é habilitado por padrão ao usar todas as versões atualmente

suportadas do ONTAP 9. Observe que, após a configuração inicial, os dados podem levar até 30 minutos para preencher o painel.

Outras práticas recomendadas

O uso do ONTAP vVols com o vSphere é simples e segue os métodos do vSphere publicados (consulte trabalhando com volumes virtuais no vSphere Storage na documentação da sua versão do ESXi). Aqui estão algumas práticas adicionais a serem consideradas em conjunto com o ONTAP.

Limites

Em geral, o ONTAP oferece suporte aos limites do vVols conforme definido pela VMware (consulte publicado "Máximos de configuração"). Verifique sempre o "NetApp Hardware Universe" para obter limites atualizados sobre números e tamanhos de LUNs, namespaces e arquivos.

Use as ferramentas do ONTAP para extensões de IU do VMware vSphere ou APIs REST para provisionar armazenamentos de dados vVols e Protocol Endpoints.*

Embora seja possível criar armazenamentos de dados vVols com a interface geral do vSphere, o uso de ferramentas do ONTAP criará automaticamente pontos de extremidade de protocolo conforme necessário e criará volumes FlexVol (não necessários com o ASA R2) usando as práticas recomendadas do ONTAP. Basta clicar com o botão direito do Mouse no host/cluster/data center e selecionar *ONTAP Tools* e *provision datastore*. A partir daí, basta escolher as opções vVols desejadas no assistente.

Nunca armazene o dispositivo ONTAP Tools ou o vCenter Server Appliance (VCSA) em um datastore vVols que eles estejam gerenciando.

Isso pode resultar em uma "situação de galinha e ovo" se você precisar reiniciar os aparelhos, porque eles não serão capazes de revincular seus próprios vVols enquanto eles estão reiniciando. Você pode armazená-los em um datastore vVols gerenciado por diferentes ferramentas do ONTAP e implantação do vCenter.

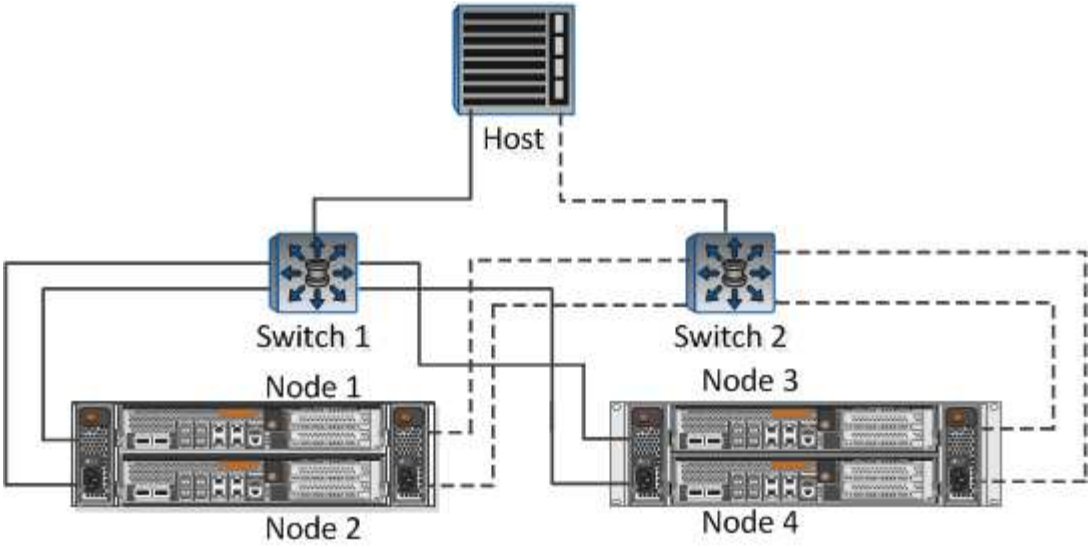
Evite operações vVols em diferentes versões do ONTAP.

Funcionalidades de storage compatíveis, como QoS, personalidade e muito mais, mudaram em várias versões do fornecedor VASA, e algumas dependem do lançamento do ONTAP. Usar versões diferentes em um cluster ONTAP ou mover vVols entre clusters com versões diferentes pode resultar em alarmes de conformidade ou comportamento inesperado.

Marque sua malha Fibre Channel antes de usar FCP para vVols.

O fornecedor de ferramentas ONTAP VASA cuida do gerenciamento de grupos FCP e iSCSI, bem como subsistemas NVMe no ONTAP com base em iniciadores descobertos de hosts ESXi gerenciados. No entanto, ele não se integra com switches Fibre Channel para gerenciar o zoneamento. O zoneamento deve ser feito de acordo com as melhores práticas antes que qualquer provisionamento possa ocorrer. O seguinte é um exemplo de zoneamento de iniciador único para quatro sistemas ONTAP:

Zoneamento do iniciador único:



Consulte os seguintes documentos para obter mais práticas recomendadas:

"*TR-4080 melhores práticas para SAN ONTAP 9* moderna"

"*TR-4684 implementação e configuração de SANs modernas com NVMe-of*"

Planeje seus volumes de apoio FlexVol de acordo com suas necessidades.

Para sistemas que não sejam ASA R2, pode ser desejável adicionar vários volumes de backup ao armazenamento de dados vVols para distribuir a carga de trabalho pelo cluster ONTAP, dar suporte a diferentes opções de política ou aumentar o número de LUNs ou arquivos permitidos. No entanto, se for necessária eficiência máxima de storage, coloque todos os volumes de backup em um único agregado. Ou, se for necessária a performance máxima de clonagem, considere usar um único FlexVol volume e manter seus modelos ou biblioteca de conteúdo no mesmo volume. O fornecedor VASA descarrega muitas operações de storage vVols para o ONTAP, incluindo migração, clonagem e snapshots. Quando isso é feito em um único FlexVol volume, clones de arquivo com uso eficiente de espaço são usados e ficam quase instantaneamente disponíveis. Quando isso é feito em volumes do FlexVol, as cópias ficam rapidamente disponíveis e usam deduplicação e compactação in-line, mas a eficiência máxima de storage não pode ser recuperada até que as tarefas em segundo plano sejam executadas em volumes usando deduplicação e compactação em segundo plano. Dependendo da origem e destino, alguma eficiência pode ser degradada.

Com os sistemas ASA R2, essa complexidade é removida, pois o conceito de um volume ou agregado é abstraído do usuário. O posicionamento dinâmico é Tratado automaticamente e os endpoints do protocolo são criados conforme necessário. Endpoints de protocolo adicionais podem ser criados automaticamente em tempo real se for necessária uma escala adicional.

Considere usar o máximo de IOPS para controlar VMs desconhecidas ou testar.

Disponível pela primeira vez no provedor VASA 7,1, o IOPS máximo pode ser usado para limitar as IOPS a uma evolução específica para uma carga de trabalho desconhecida, a fim de evitar impactos em outras cargas de trabalho mais críticas. Consulte a Tabela 4 para obter mais informações sobre o gerenciamento de desempenho.

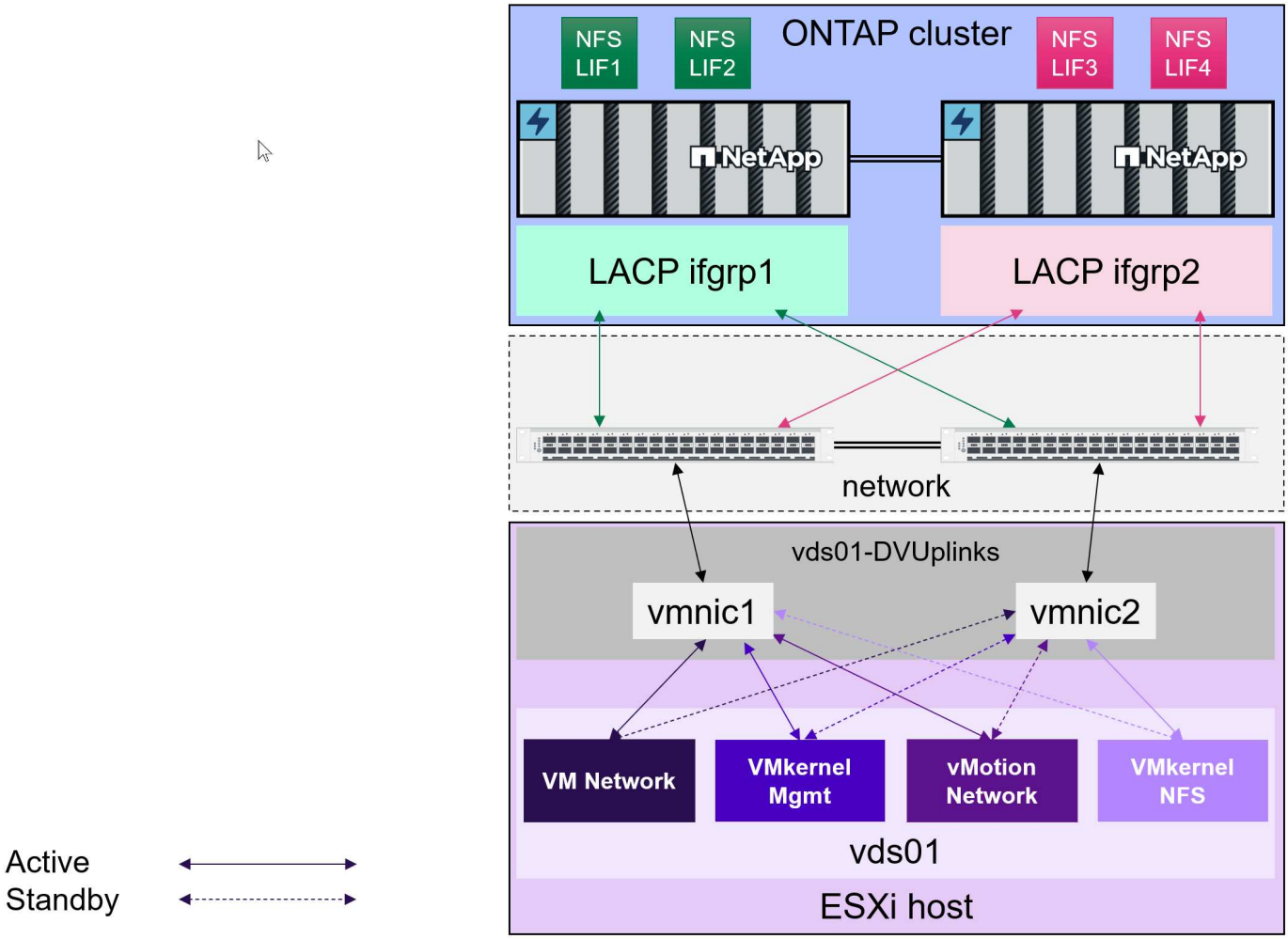
Certifique-se de ter LIFs de dados suficientes. "Implantando o storage vVols"Consulte a .

Siga todas as melhores práticas de protocolo.

Consulte os outros guias de práticas recomendadas da NetApp e da VMware específicos do protocolo

selecionado. Em geral, não existem outras alterações além das já mencionadas.

- Exemplo de configuração de rede usando vVols sobre NFS v3*



Implantação de vVols em sistemas AFF, ASA, ASA R2 e FAS

Siga estas práticas recomendadas para criar armazenamento vVols para suas máquinas virtuais.

O provisionamento de armazenamentos de dados vVols envolve várias etapas. Os sistemas ASA R2 da NetApp foram projetados para cargas de trabalho VMware e oferecem uma experiência do usuário diferente dos sistemas ONTAP tradicionais. Ao usar os sistemas ASA R2, as ferramentas do ONTAP 10,3 ou posterior exigem menos etapas para configurar e incluem extensões de IU e suporte à API REST otimizadas para a nova arquitetura de storage.

Preparando-se para criar datastores vVols com as ferramentas do ONTAP

Você pode ignorar as duas primeiras etapas do processo de implantação se você já estiver usando ferramentas do ONTAP para gerenciar, automatizar e gerar relatórios sobre o seu storage VMFS existente ou baseado em NFS tradicional. Você também pode consultar este completo "lista de verificação" para implantar e configurar ferramentas do ONTAP.

1. Crie a Máquina Virtual de Armazenamento (SVM) e sua configuração de protocolo. Note que isso pode não ser necessário para sistemas ASA r2, já que eles normalmente já possuem uma única SVM para

serviços de dados. Você deverá selecionar NVMe/FC (somente para ONTAP tools 9.13), NFSv3, NFSv4.1, iSCSI, FCP ou uma combinação dessas opções. NVMe/TCP e NVMe/FC também podem ser usados para armazenamentos de dados VMFS tradicionais com as ferramentas ONTAP 10.3 e posteriores. Você pode usar os assistentes do ONTAP System Manager ou a linha de comando do shell do cluster.

- "Atribua camadas locais (agregados) a SVMs" Para todos os sistemas que não sejam ASA R2.
- Pelo menos um LIF por nó para cada conexão de switch/malha. Como prática recomendada, crie dois ou mais por nó para protocolos baseados em FCP, iSCSI ou NVMe. Um LIF por nó é suficiente para vVols baseados em NFS, mas esse LIF deve ser protegido por um ifgroup LACP. "Configure a visão geral dos LIFs"Consulte e "Combine portas físicas para criar grupos de interface" para obter detalhes.
- É necessário pelo menos um LIF de gerenciamento por SVM se você pretende usar credenciais com escopo de SVM para seus vCenters de locatário.
- Se você planeja usar o SnapMirror, verifique se o código fonte e o destino "Os clusters e SVMs do ONTAP são peered".
- Para sistemas que não sejam ASA r2, os volumes podem ser criados neste momento, mas a melhor prática é deixar que o assistente *Provision Datastore* nas ferramentas ONTAP os crie. A única exceção a essa regra é se você planeja usar a replicação de vVols com o VMware Site Recovery Manager e as ferramentas ONTAP 9.13. Isso é mais fácil de configurar com volumes FlexVol preexistentes que já possuam relações SnapMirror . Tenha cuidado para não ativar o QoS em nenhum volume que será usado para vVols, pois isso deve ser gerenciado pelas ferramentas SPBM e ONTAP .

2. "Implantar as ferramentas do ONTAP para o VMware vSphere" Usando o OVA baixado do site de suporte da NetApp.
   - O ONTAP Tools 10.0 e versões posteriores suportam vários servidores vCenter por appliance; não é mais necessário implantar um appliance ONTAP Tools por vCenter.
     - Se você planeja conectar vários vCenters a uma única instância do ONTAP Tools, você deve criar e instalar certificados assinados por uma Autoridade Certificadora (CA). Consulte "Gerenciar certificados" para etapas.
   - A partir da versão 10.3, as ferramentas ONTAP agora são implantadas como um dispositivo de pequeno porte com um único nó, adequado para a maioria das cargas de trabalho que não utilizam vVols.

- A melhor prática recomendada é: "Ferramentas de ONTAP com escalabilidade horizontal" A partir da versão 10.3, foi implementada a configuração de alta disponibilidade (HA) de 3 nós para todas as cargas de trabalho de produção. Para fins de laboratório ou teste, é possível usar uma implantação de nó único.
- A melhor prática recomendada para o uso de vVols em produção é eliminar qualquer ponto único de falha. Crie regras de antiafinidade para impedir que as VMs das ferramentas ONTAP sejam executadas juntas no mesmo host. Após a implantação inicial, também é recomendável usar o Storage vMotion para mover as VMs das ferramentas ONTAP para diferentes datastores. Leia mais sobre "Usando o Affinity Rules sem o vSphere DRS" ou "Crie uma regra de afinidade VM-VM". Você também deve agendar backups frequentes e/ou "utilize o utilitário de cópia de segurança de configuração incorporado".

1. Configure as ferramentas do ONTAP 10,3 para o seu ambiente.
   - "Adicione instâncias do vCenter Server" Na IU do Gerenciador de ferramentas do ONTAP.
   - As ferramentas do ONTAP 10,3 são compatíveis com a alocação segura a vários clientes. Se você não precisar de alocação segura a vários clientes, basta "Adicione seus clusters ONTAP" ir ao menu Ferramentas do ONTAP no vCenter e clicar em *backends de armazenamento* e clicar no botão *add*.
   - Em um ambiente multitenant seguro onde você deseja delegar SVMs (Storage Virtual Machines)

específicas em vCenters específicos, você deve fazer o seguinte.

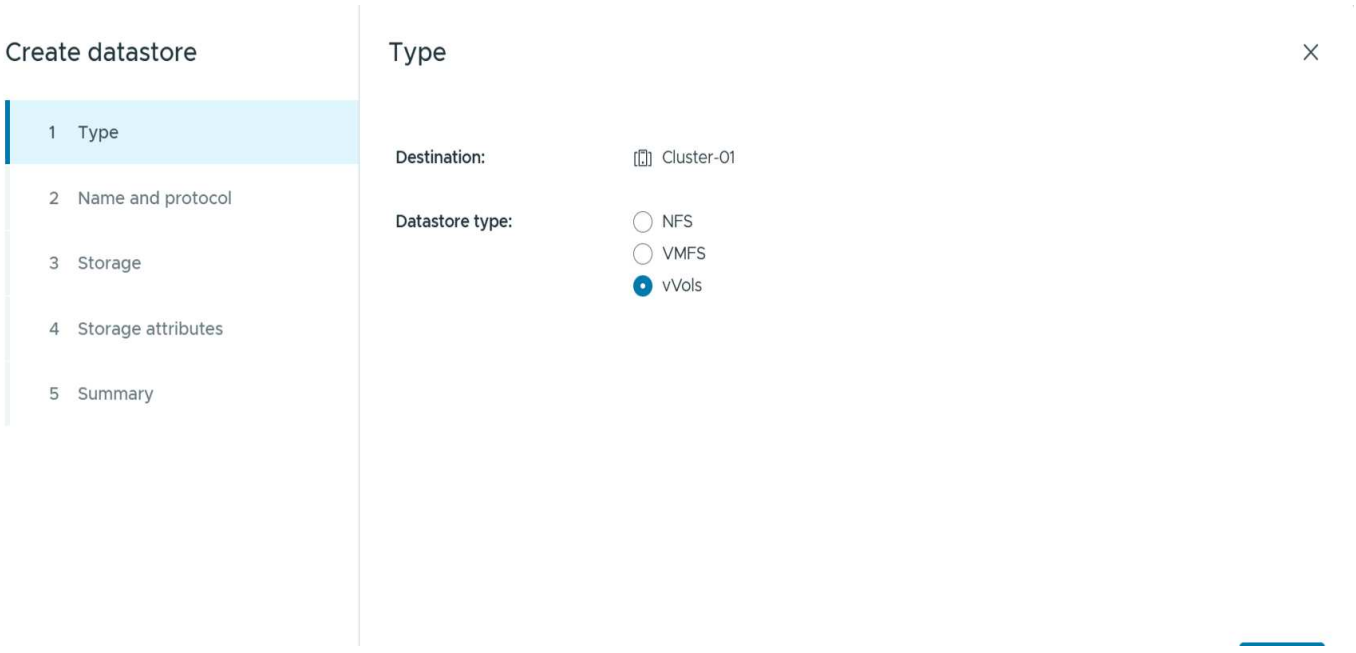
- Faça login na IU do Gerenciador de ferramentas do ONTAP
- "Integrar o cluster de storage"
- "Associar um back-end de storage a uma instância do vCenter Server"
- Forneça as credenciais específicas da SVM ao administrador do vCenter, que então adicionará a SVM como um backend de armazenamento no menu de backends de armazenamento das ferramentas ONTAP no vCenter.

- É uma prática recomendada criar funções de RBAC para suas contas de storage.
- As ferramentas ONTAP incluem um arquivo JSON contendo as permissões de função necessárias para as contas de armazenamento das ferramentas ONTAP . Você pode carregar o arquivo JSON no ONTAP System Manager para simplificar a criação de funções e usuários RBAC.
- Você pode ler mais sobre as funções RBAC do ONTAP em "Configurar as funções de usuário do ONTAP e o Privileges".

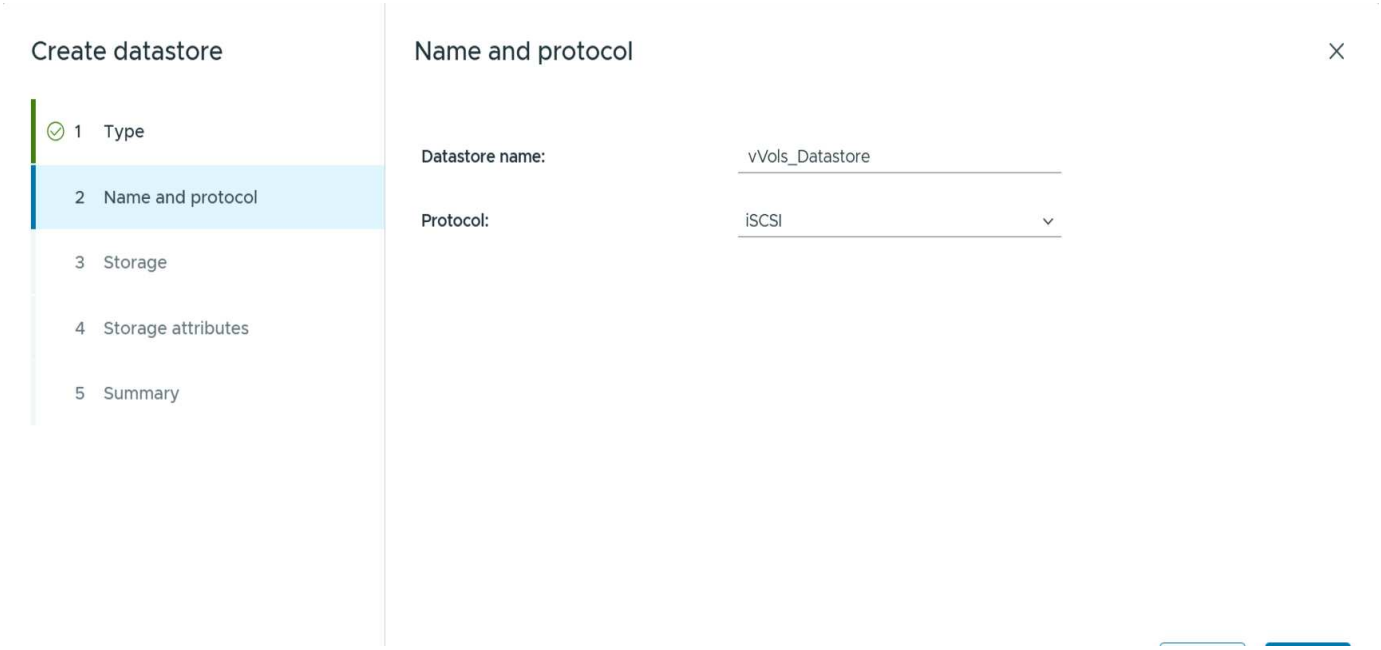
O motivo pelo qual todo o cluster precisa ser integrado à interface do usuário do gerenciador de ferramentas ONTAP é que muitas das APIs usadas para vVols estão disponíveis apenas no nível do cluster.

Criação de datastores vVols com as ferramentas do ONTAP

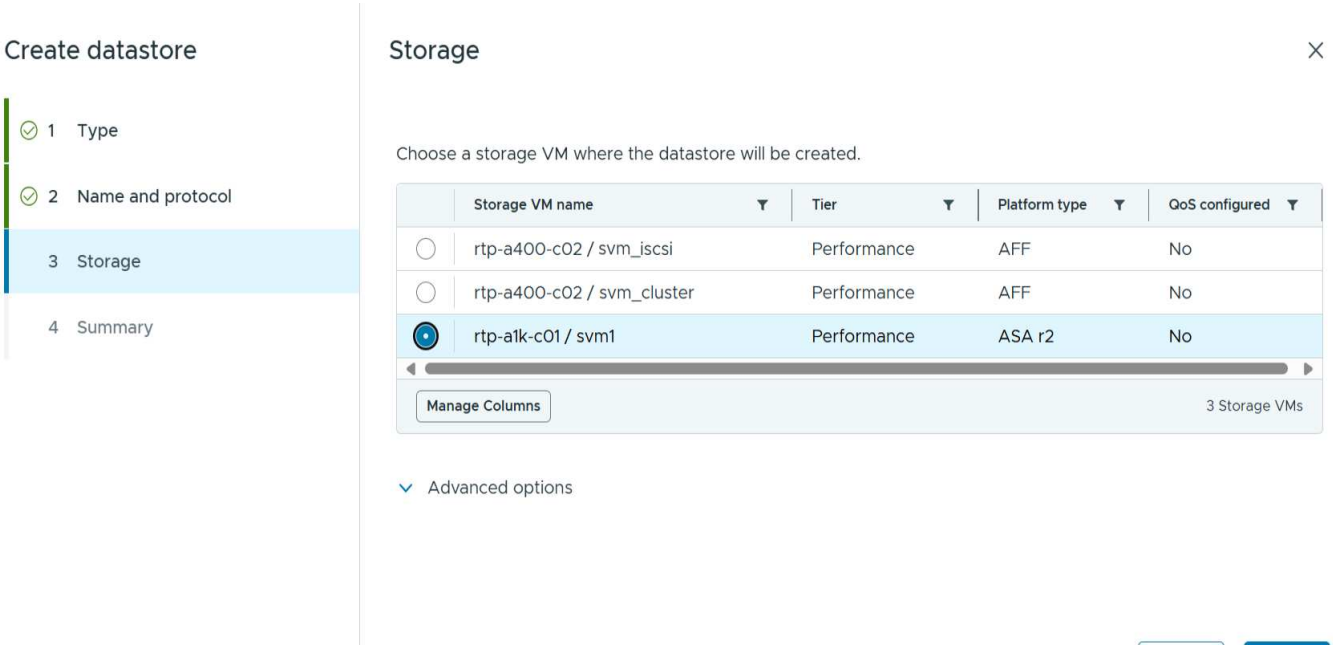
Clique com o botão direito do Mouse no host, cluster ou datacenter no qual você deseja criar o datastore vVols e selecione *ONTAP Tools > provision datastore*.



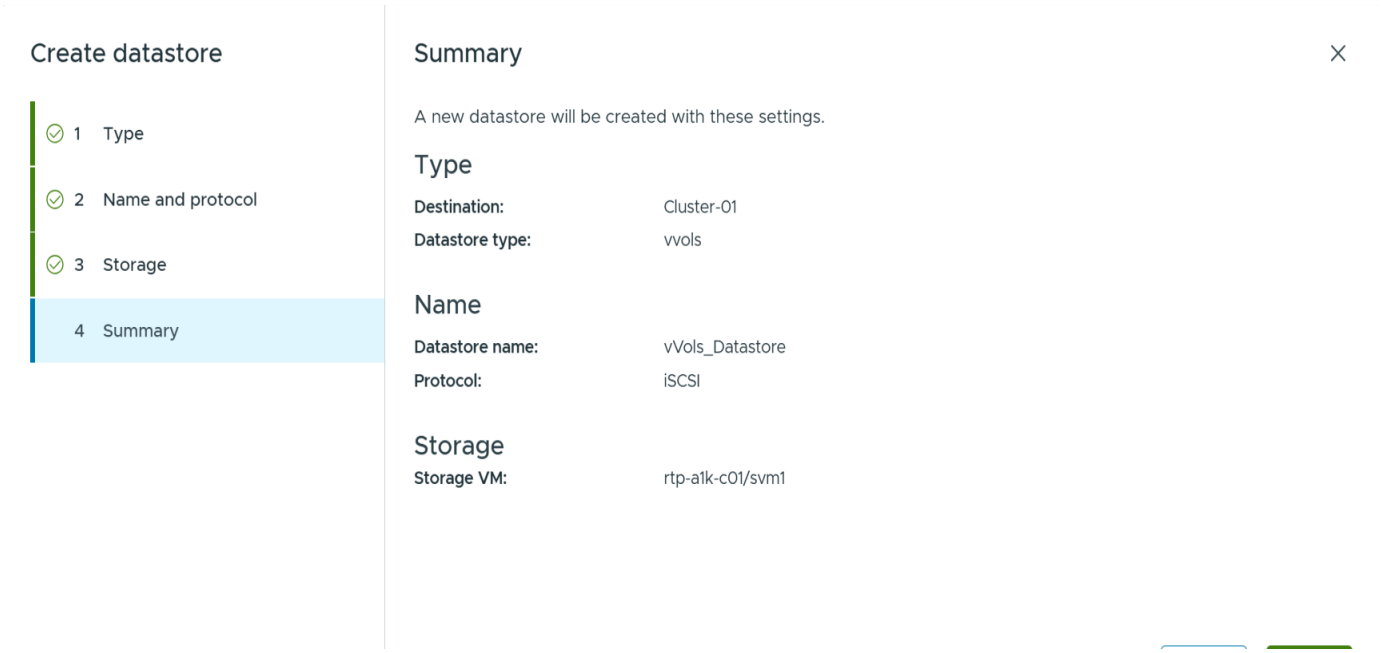
- Escolha vVols e forneça um nome significativo e selecione o protocolo desejado. Você também pode fornecer uma descrição do datastore.
  - Ferramentas ONTAP 10,3 com ASA R2.



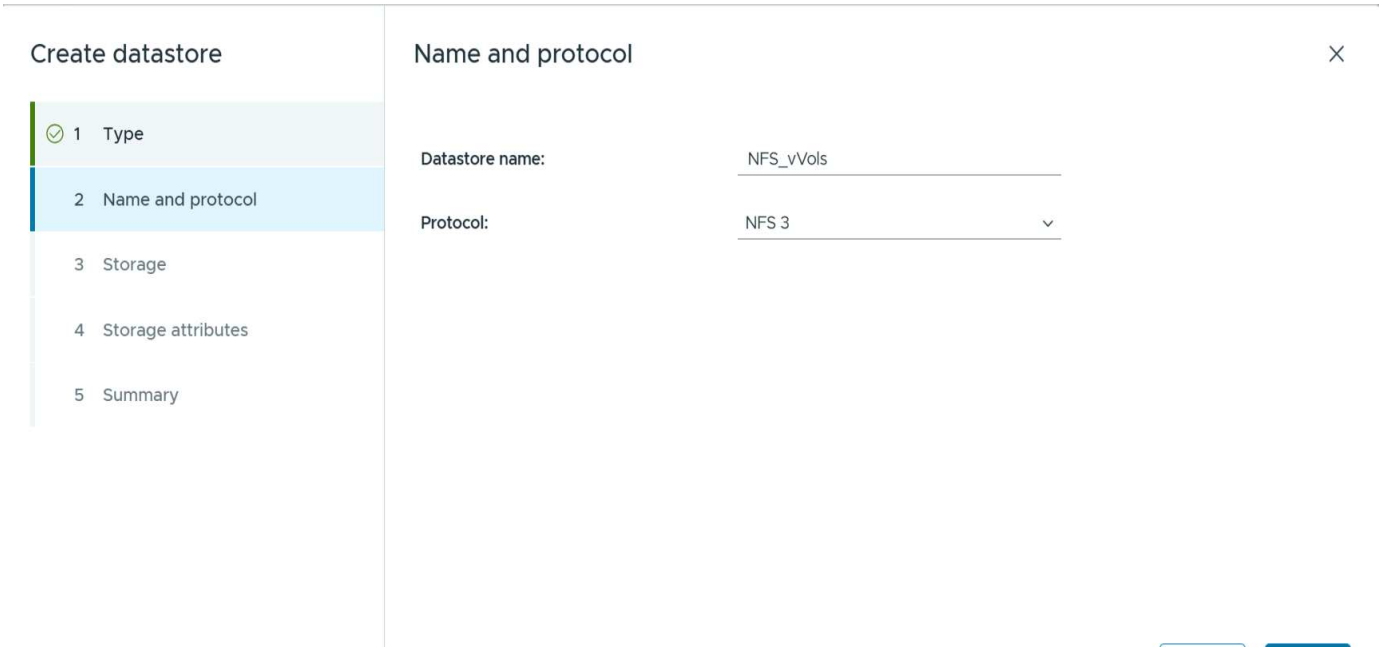
- Selecione o SVM do sistema ASA R2 e clique em *next*.



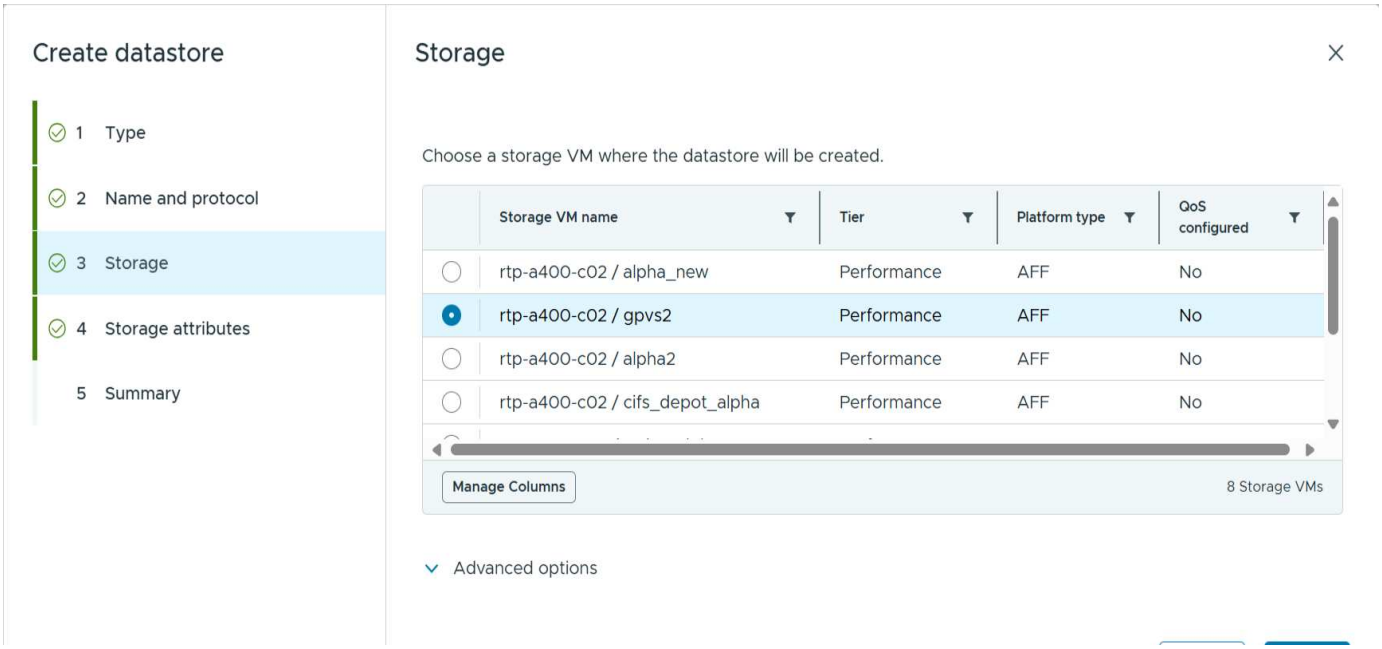
- Clique em *finish*



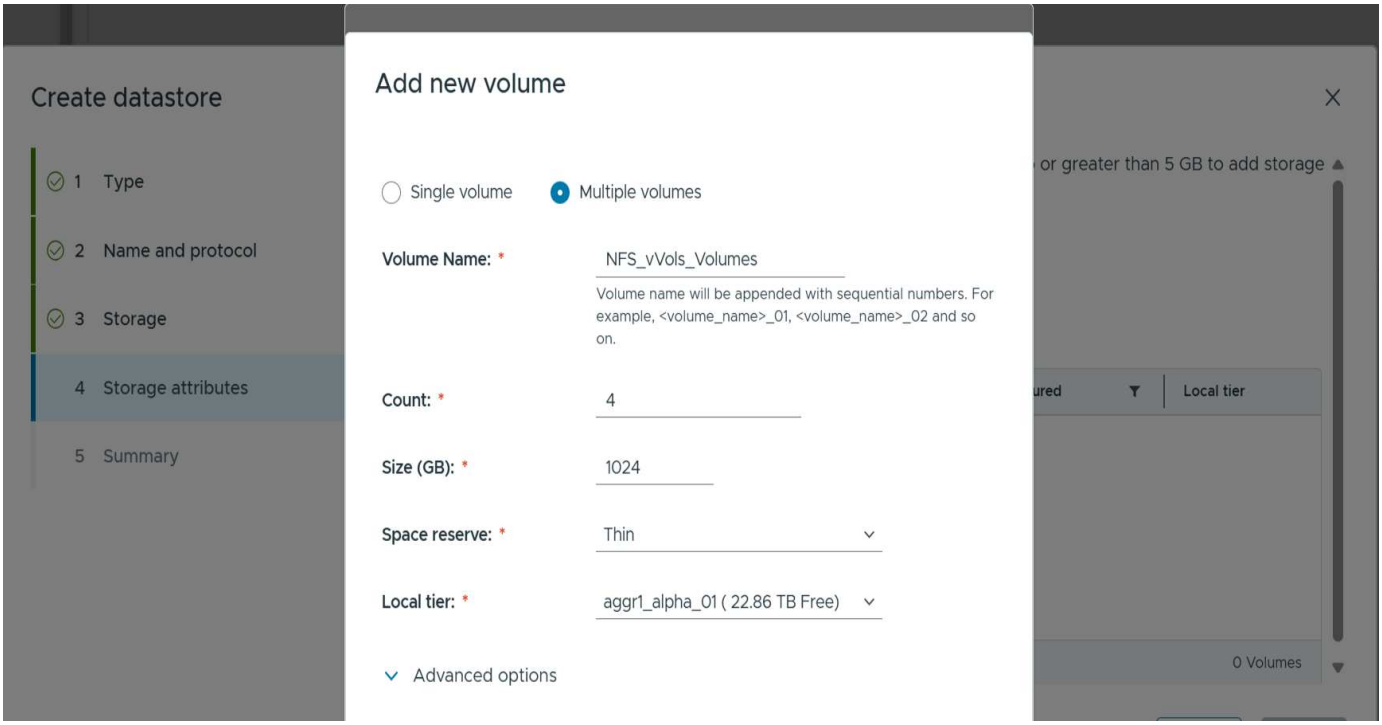
- É tão fácil!
  - Ferramentas ONTAP 10.3 com ONTAP FAS, AFF e ASA anteriores ao ASA r2.
- Selecione o protocolo

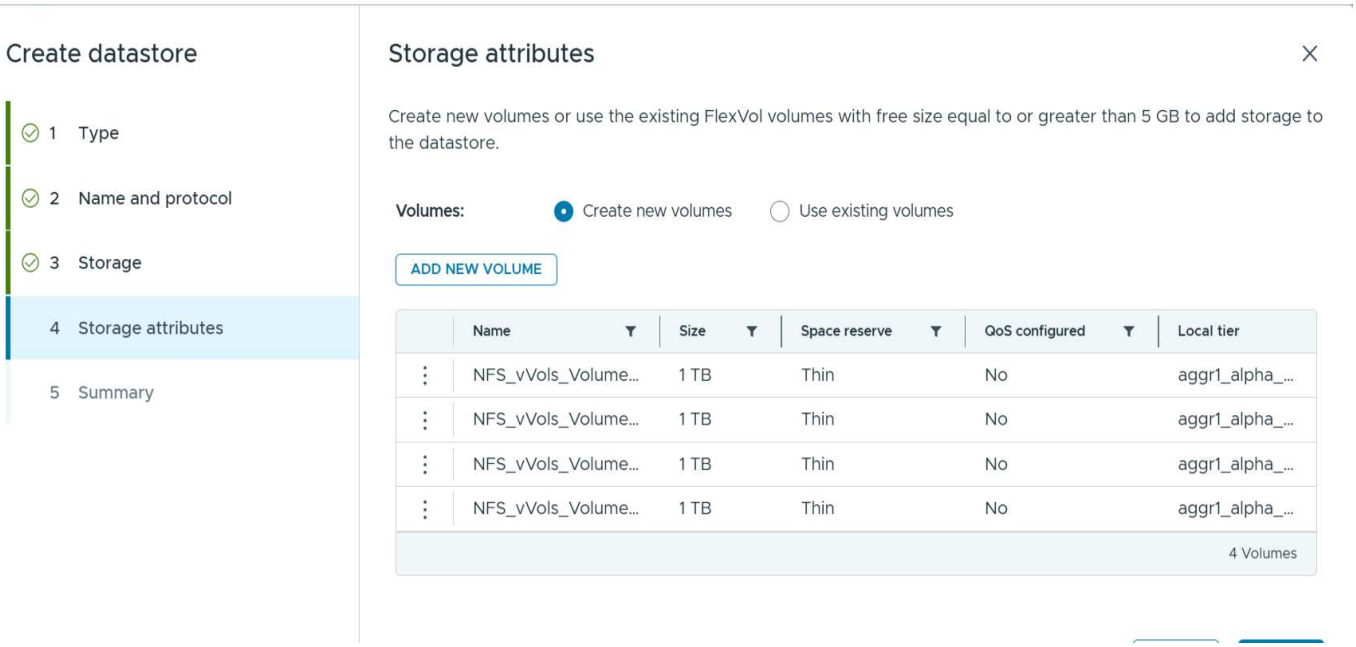


- Selecione o SVM e clique em *next*.

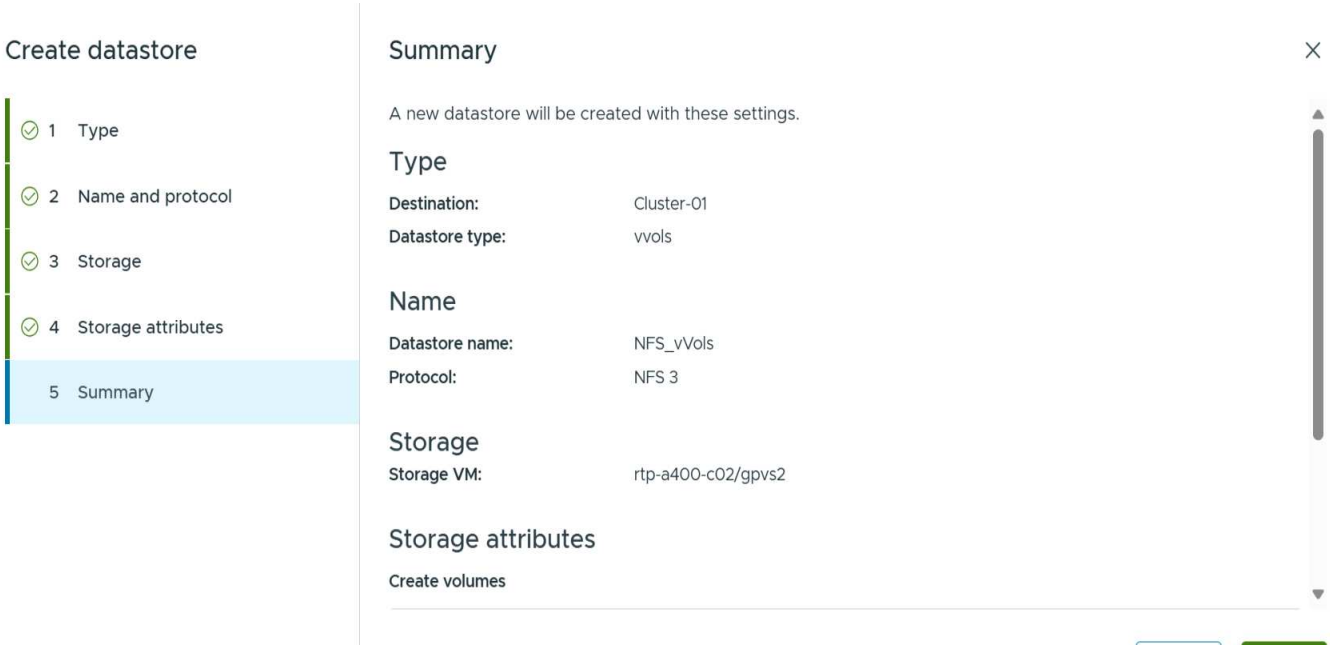


- Clique em *adicionar novos volumes* ou *usar volume existente* e especifique os atributos. Note que nas ferramentas ONTAP 10.3, você pode solicitar a criação de vários volumes simultaneamente. Você também pode adicionar manualmente vários volumes para distribuí-los pelo cluster ONTAP . Clique em *próximo*

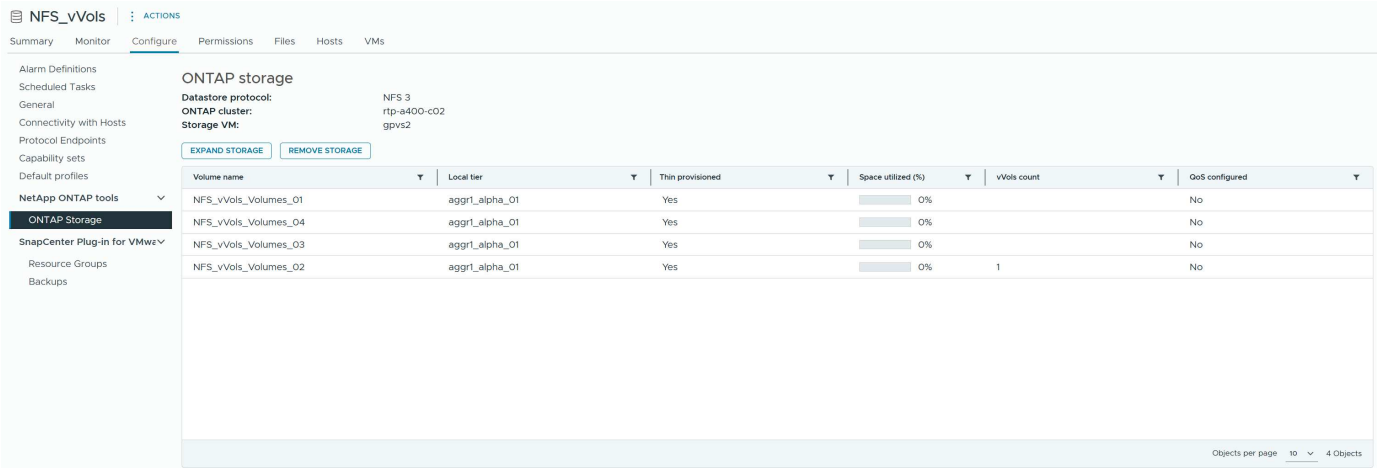




- Clique em *finish*



- Você pode ver os volumes atribuídos no menu Ferramentas do ONTAP da guia configurar para o datastore.



- Agora você pode criar políticas de armazenamento de VM a partir do menu *políticas e Perfis* na IU do vCenter.

Migração de VMs de datastores tradicionais para vVols

A migração de VMs de datastores tradicionais para um datastore vVols é tão simples quanto mover VMs entre datastores tradicionais. Basta selecionar a(s) VM(s), depois selecionar migrar da lista de ações e selecionar um tipo de migração de *change storage only*. Quando solicitado, selecione uma política de armazenamento de VM que corresponda ao armazenamento de dados do vVols. As operações de cópia de migração podem ser descarregadas com o vSphere 6,0 e posterior para migrações SAN VMFS para vVols, mas não de VMDKs nas para vVols.

Gerenciamento de VMs com políticas

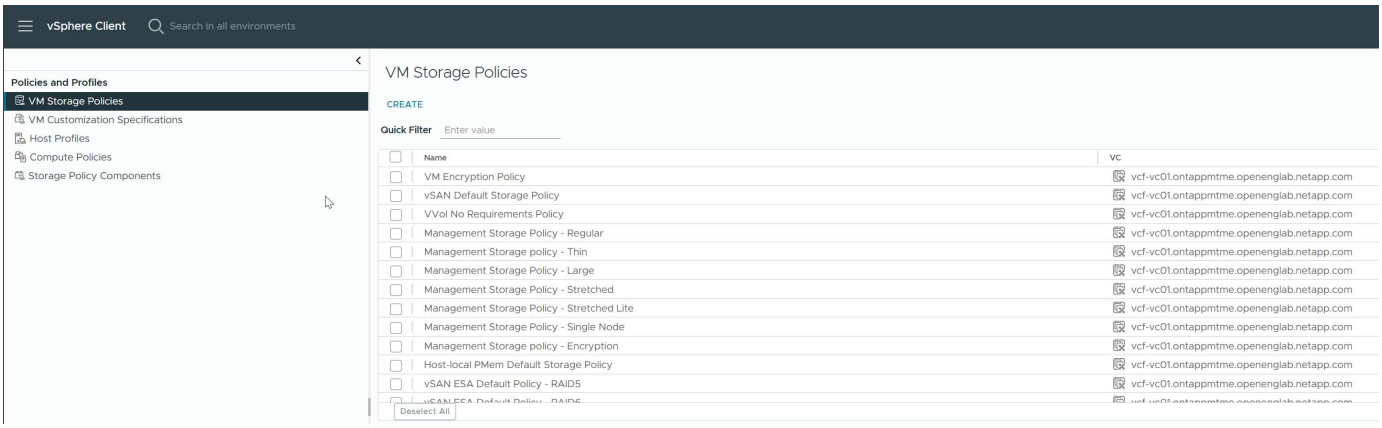
Para automatizar o provisionamento de armazenamento com gerenciamento baseado em políticas, você precisa criar políticas de armazenamento de VM que correspondam aos recursos de armazenamento desejados.

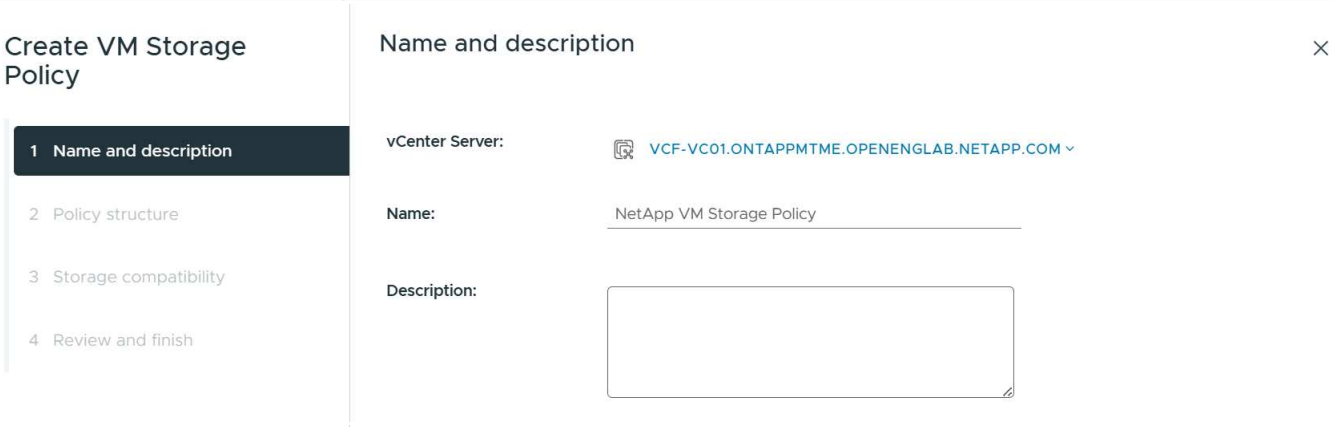
> As ferramentas do ONTAP 10,0 e posteriores não usam mais perfis de capacidade de armazenamento como as versões anteriores. Em vez disso, os recursos de storage são definidos diretamente na própria política de storage da VM.

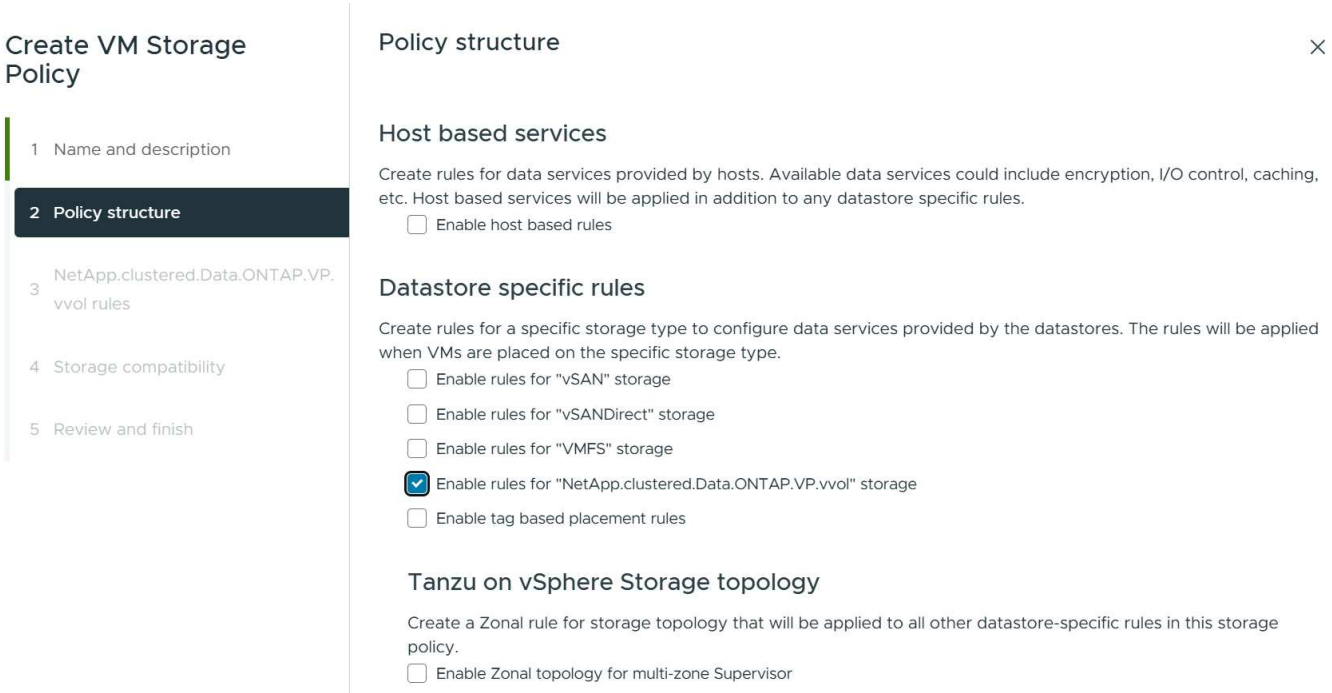
Criando políticas de armazenamento de VM

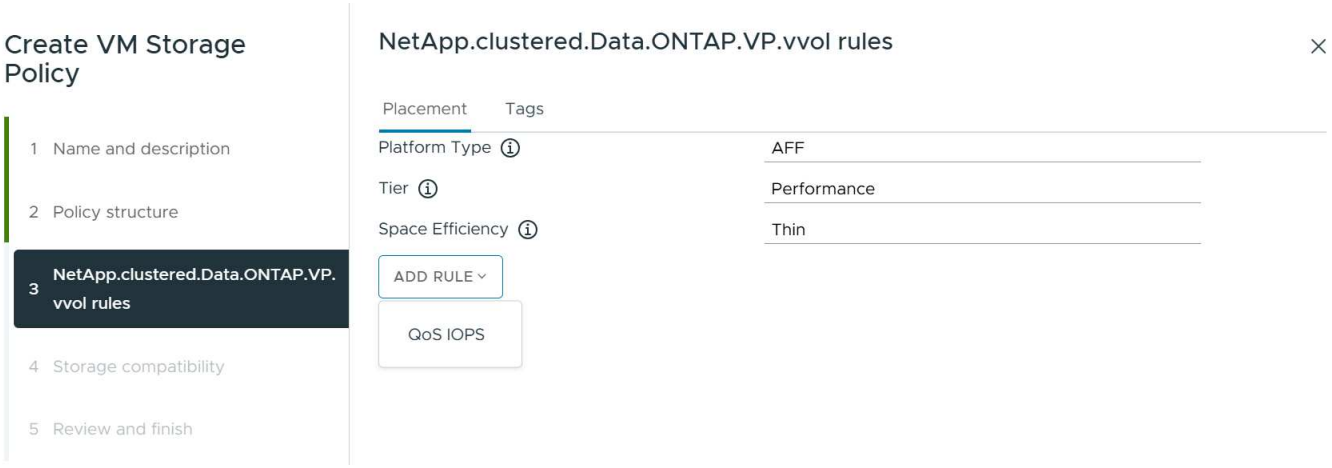
As políticas de armazenamento de máquinas virtuais (VMs) são usadas no vSphere para gerenciar recursos opcionais, como o controle de E/S de armazenamento ou a criptografia do vSphere. Eles também são usados com vVols para aplicar recursos de armazenamento específicos à máquina virtual. Utilize o tipo de armazenamento " NetApp ". Veja o exemplo de configuração de rede usando vVols sobre NFS v3 para um exemplo disso com o provedor VASA das ferramentas ONTAP . As regras para o armazenamento "NetApp" devem ser usadas com datastores que não ONTAP baseados em vVols.

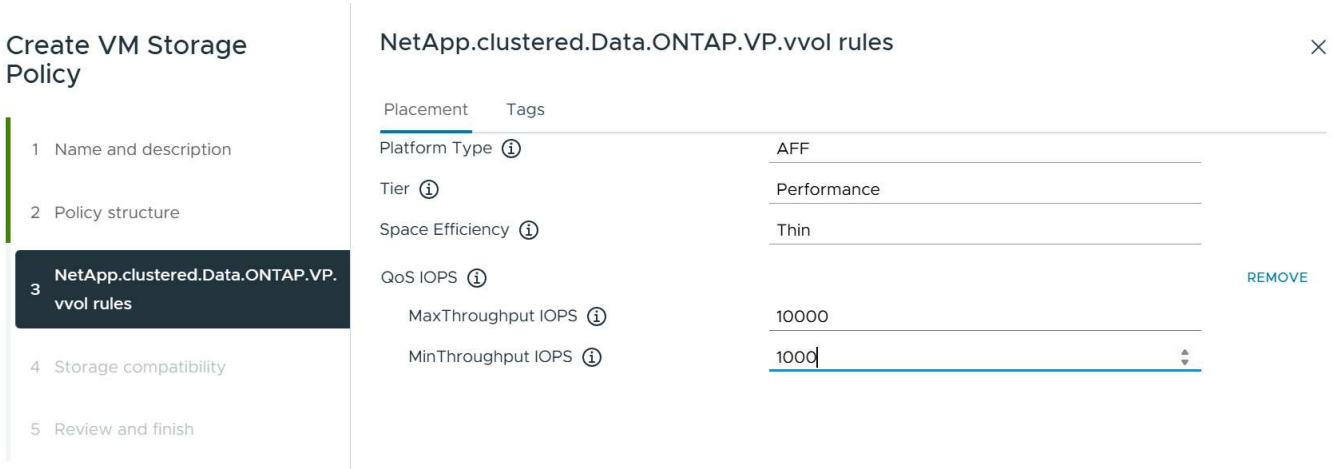
Uma vez criada a política de storage, ela pode ser usada ao provisionar novas VMs.

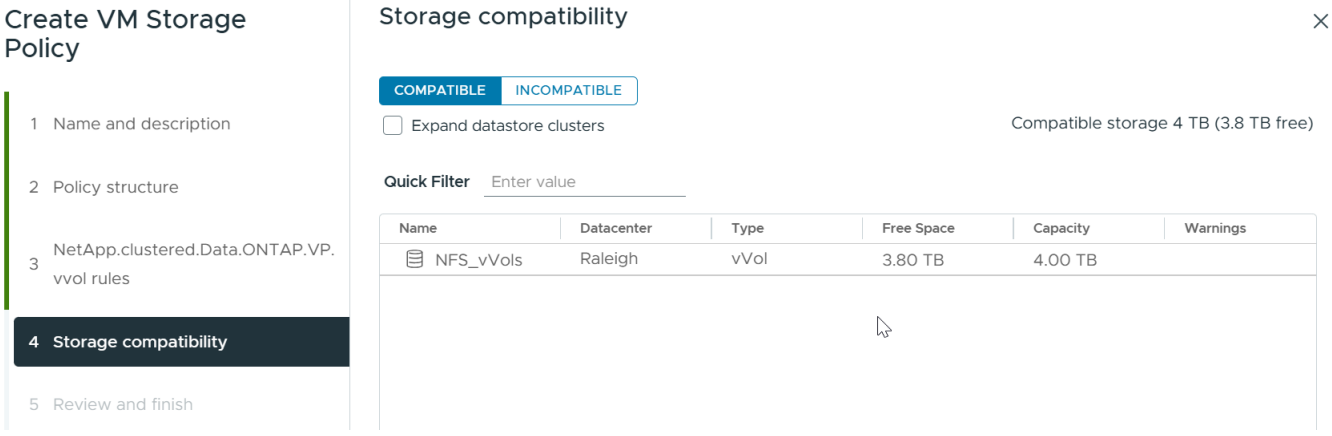

vSphere Client
Search in all environments
Policies and Profiles
VM Storage Policies
VM Customization Specifications
Host Profiles
Compute Policies
Storage Policy Components
VM Storage Policies
CREATE
Quick Filter
Enter value
Name
VC
VM Encryption Policy
vSAN Default Storage Policy
VVol No Requirements Policy
Management Storage Policy - Regular
Management Storage policy - Thin
Management Storage Policy - Large
Management Storage Policy - Stretched
Management Storage Policy - Stretched Lite
Management Storage Policy - Single Node
Management Storage policy - Encryption
Host-local PMem Default Storage Policy
vSAN ESA Default Policy - RAID5
vcf-vc01.ontappmtme.openenglab.netapp.com
Deselect All

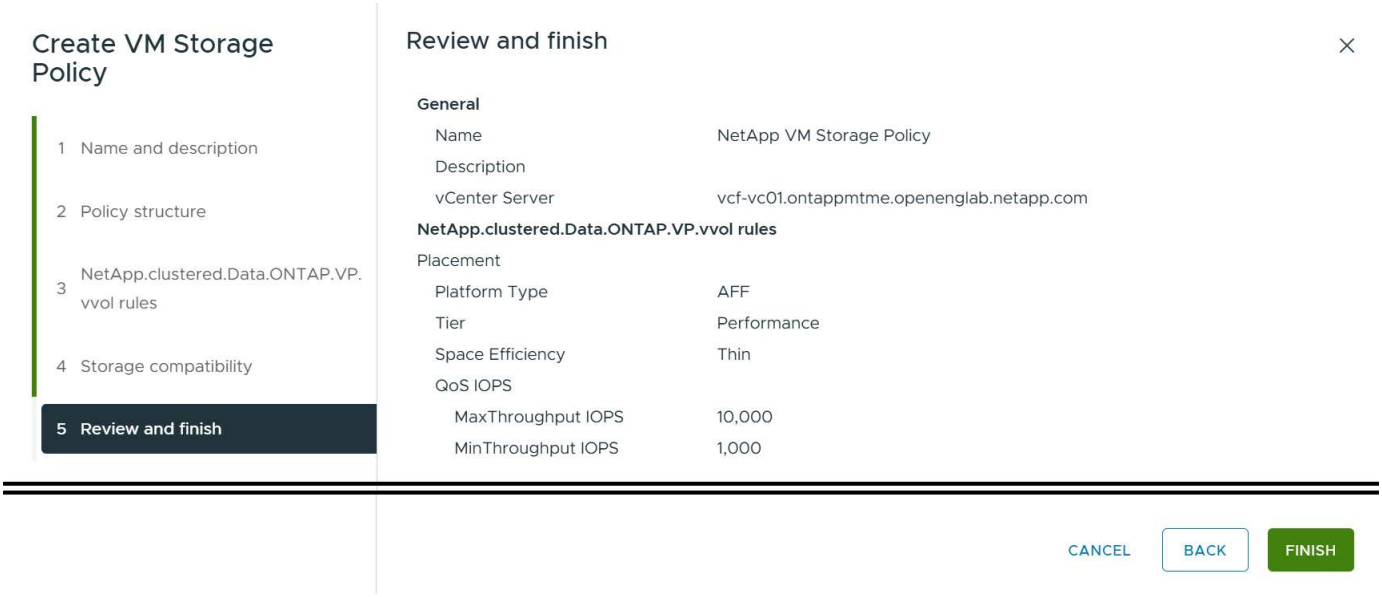

Create VM Storage Policy
1 Name and description
2 Policy structure
3 Storage compatibility
4 Review and finish
Name and description
vCenter Server:
VCF-VC01.ONTAPPMTME.OPENENGLAB.NETAPP.COM
Name:
NetApp VM Storage Policy
Description:


Create VM Storage Policy
1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP.vvol rules
4 Storage compatibility
5 Review and finish
Policy structure
Host based services
Create rules for data services provided by hosts. Available data services could include encryption, I/O control, caching, etc. Host based services will be applied in addition to any datastore specific rules.
Enable host based rules
Datastore specific rules
Create rules for a specific storage type to configure data services provided by the datastores. The rules will be applied when VMs are placed on the specific storage type.
Enable rules for "vSAN" storage
Enable rules for "vSANDirect" storage
Enable rules for "VMFS" storage
Enable rules for "NetApp.clustered.Data.ONTAP.VP.vvol" storage
Enable tag based placement rules
Tanzu on vSphere Storage topology
Create a Zonal rule for storage topology that will be applied to all other datastore-specific rules in this storage policy.
Enable Zonal topology for multi-zone Supervisor


Create VM Storage Policy
1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP.vvol rules
4 Storage compatibility
5 Review and finish
NetApp.clustered.Data.ONTAP.VP.vvol rules
Placement
Tags
Platform Type
AFF
Tier
Performance
Space Efficiency
Thin
ADD RULE
QoS IOPS


Create VM Storage Policy
1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP.vvol rules
4 Storage compatibility
5 Review and finish
NetApp.clustered.Data.ONTAP.VP.vvol rules
Placement
Tags
Platform Type
AFF
Tier
Performance
Space Efficiency
Thin
QoS IOPS
REMOVE
MaxThroughput IOPS
10000
MinThroughput IOPS
1000


Create VM Storage Policy
1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP.vvol rules
4 Storage compatibility
5 Review and finish
Storage compatibility
COMPATIBLE
INCOMPATIBLE
Expand datastore clusters
Compatible storage 4 TB (3.8 TB free)
Quick Filter
Enter value
Name
Datacenter
Type
Free Space
Capacity
Warnings
NFS_vVols
Raleigh
vVol
3.80 TB
4.00 TB



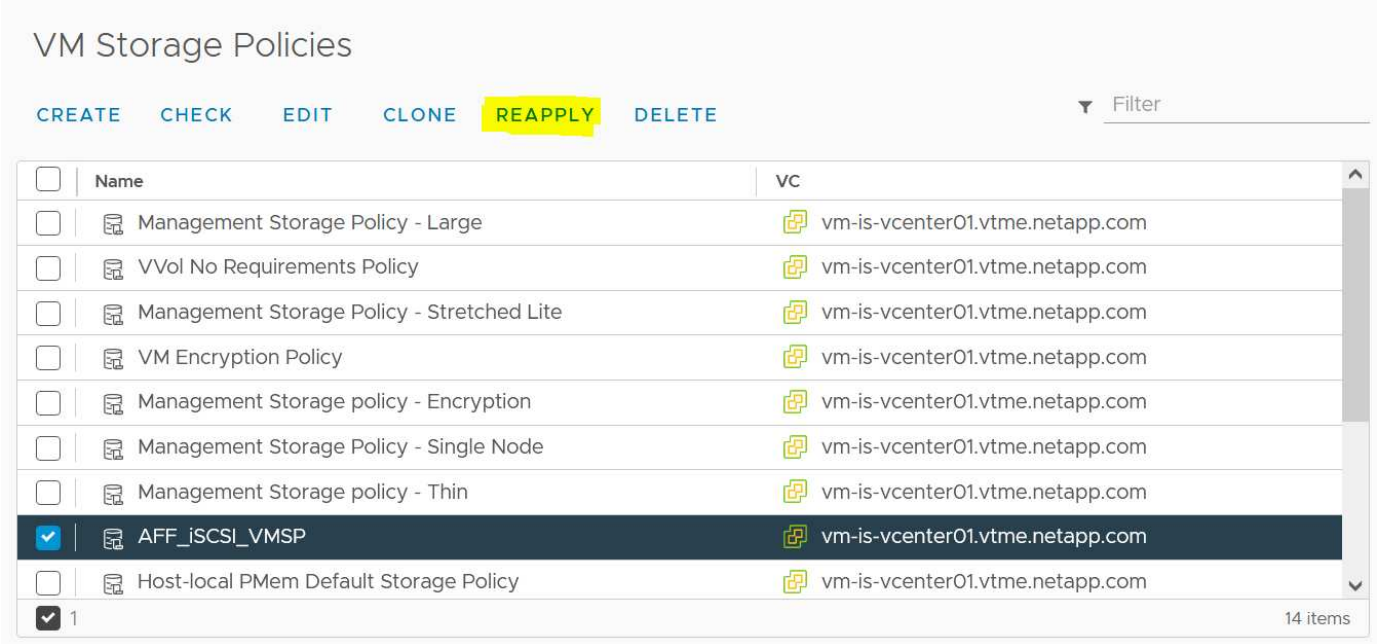
Gerenciamento de performance com ferramentas ONTAP

As ferramentas da ONTAP usam seu próprio algoritmo de colocação equilibrada para colocar uma nova evolução no melhor FlexVol volume com sistemas ASA unificados ou clássicos, ou zona de disponibilidade de armazenamento (SAZ) com sistemas ASA R2, dentro de um datastore da vVols. O posicionamento é baseado na correspondência do armazenamento de backup com a política de armazenamento de VM. Isso garante que o armazenamento de dados e o armazenamento de backup possam atender aos requisitos de desempenho especificados.

Alterar as capacidades de desempenho, como IOPS mínimo e máximo, requer atenção à configuração específica.

- **IOPS mínimo e máximo** podem ser especificados em uma política de VM.
  - Alterar o IOPS na política não alterará a QoS nos vVols até que a Política de VM seja reaplicada às VMs que a utilizam. Ou você pode criar uma nova política com o IOPS desejado e aplicá-la às VMs de destino. Em geral, recomenda-se simplesmente definir políticas de armazenamento de VM separadas para diferentes níveis de serviço e alterar a política de armazenamento da VM diretamente na VM.
  - As personalidades ASA, ASA r2, AFF e FAS possuem configurações de PIO (pressão intraocular) diferentes. As opções Min e Max estão disponíveis em todos os sistemas flash; no entanto, sistemas que não sejam AFF só podem usar as configurações de IOPS máximo.
- As ferramentas do ONTAP criam políticas individuais de QoS não compartilhadas com versões atualmente suportadas do ONTAP. Portanto, cada VMDK individual receberá sua própria alocação de IOPs.

Reaplicar a política de armazenamento de VM



Protegendo vVols

As seções a seguir descrevem os procedimentos e as práticas recomendadas para o uso do VMware vVols com storage ONTAP.

Alta disponibilidade do fornecedor VASA

O Fornecedor NetApp VASA é executado como parte do dispositivo virtual juntamente com o plug-in do vCenter e o servidor de API REST (anteriormente conhecido como o console de armazenamento virtual [VSC]) e o adaptador de replicação de armazenamento. Se o provedor VASA não estiver disponível, as VMs que usam vVols continuarão a ser executadas. No entanto, novos datastores vVols não podem ser criados e o vVols não pode ser criado ou vinculado pelo vSphere. Isso significa que as VMs que usam vVols não podem ser ativadas, uma vez que o vCenter não poderá solicitar a criação da vVol de swap. E as VMs em execução não podem usar o vMotion para migração para outro host porque os vVols não podem ser vinculados ao novo host.

O VASA Provider 7,1 e posterior suportam novos recursos para garantir que os serviços estejam disponíveis quando necessário. Inclui novos processos watchdog que monitorizam o fornecedor VASA e os serviços de base de dados integrados. Se detetar uma falha, ele atualiza os arquivos de log e reinicia os serviços automaticamente.

Proteção adicional deve ser configurada pelo administrador do vSphere usando os mesmos recursos de disponibilidade usados para proteger outras VMs de missão crítica contra falhas no software, hardware do host e rede. Nenhuma configuração adicional é necessária no dispositivo virtual para usar esses recursos; basta configurá-los usando abordagens padrão do vSphere. Eles foram testados e são suportados pelo NetApp.

O vSphere High Availability é facilmente configurado para reiniciar uma VM em outro host no cluster de host em caso de falha. A tolerância a falhas do vSphere fornece maior disponibilidade criando uma VM secundária que é continuamente replicada e pode assumir o controle a qualquer momento. Informações adicionais sobre esses recursos estão disponíveis no "Ferramentas do ONTAP para documentação do VMware vSphere (Configurar alta disponibilidade para ferramentas do ONTAP)", bem como na documentação do VMware vSphere (procure disponibilidade do vSphere em ESXi e vCenter Server).

O ONTAP provedor VASA faz o backup automático da configuração do vVols em tempo real para sistemas ONTAP gerenciados, onde as informações do vVols são armazenadas nos metadados do FlexVol volume. Caso o ONTAP Tools Appliance fique indisponível por qualquer motivo, você pode implantar uma nova ferramenta de forma fácil e rápida e importar a configuração. Consulte este artigo da KB para obter mais informações sobre as etapas de recuperação do provedor VASA:

"Como executar uma recuperação de desastres do provedor VASA - Guia de resolução"

Replicação do vVols

Muitos clientes da ONTAP replicam seus armazenamentos de dados tradicionais para sistemas de storage secundário usando o NetApp SnapMirror e, em seguida, usam o sistema secundário para recuperar VMs individuais ou um local inteiro em caso de desastre. Na maioria dos casos, os clientes usam uma ferramenta de software para gerenciar isso, como um produto de software de backup, como o plug-in do NetApp SnapCenter para VMware vSphere ou uma solução de recuperação de desastres, como o Gerenciador de recuperação de site da VMware (juntamente com o adaptador de replicação de armazenamento nas ferramentas do ONTAP).

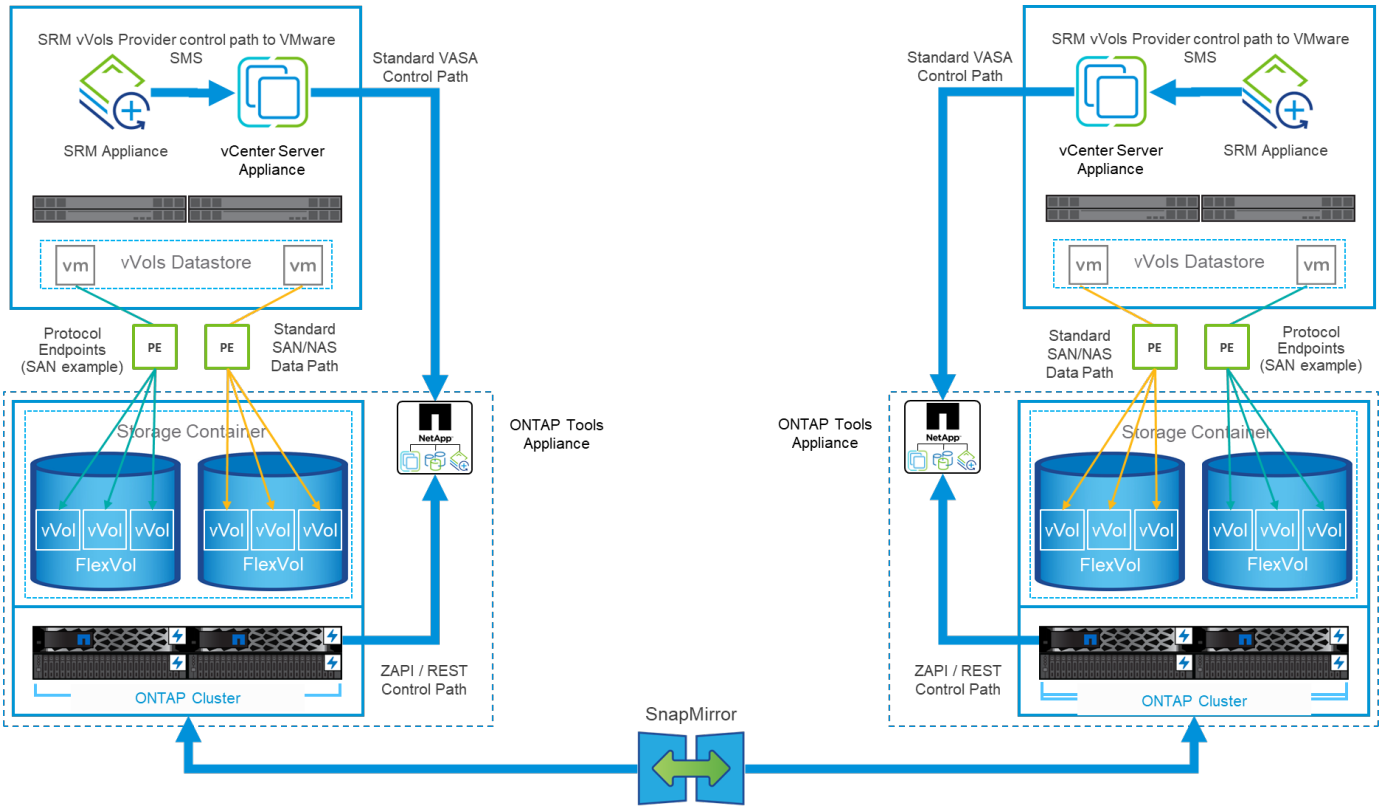
Esse requisito para uma ferramenta de software é ainda mais importante para gerenciar a replicação do vVols. Embora alguns aspectos possam ser gerenciados por recursos nativos (por exemplo, os snapshots gerenciados do vVols da VMware são descarregados para o ONTAP, que usa clones rápidos e eficientes de arquivos ou LUN), em geral, a orquestração é necessária para gerenciar a replicação e a recuperação. Os metadados sobre o vVols são protegidos pelo ONTAP, bem como pelo Fornecedor VASA, mas é necessário um processamento adicional para usá-los em um local secundário.

As ferramentas do ONTAP 9.7.1 em conjunto com a versão 8,3 do VMware Site Recovery Manager (SRM) adicionou suporte para orquestração do fluxo de trabalho de migração e recuperação de desastres aproveitando a tecnologia NetApp SnapMirror.

Na versão inicial do suporte do SRM com as ferramentas do ONTAP 9.7.1, era necessário pré-criar volumes do FlexVol e habilitar a proteção do SnapMirror antes de usá-los como volumes de backup para um datastore vVols. A partir das ferramentas ONTAP 9,10, esse processo não é mais necessário. Agora, você pode adicionar proteção SnapMirror aos volumes de backup existentes e atualizar suas políticas de storage de VM para aproveitar o gerenciamento baseado em políticas com orquestração e recuperação de desastres e automação integradas ao SRM.

Atualmente, o VMware SRM é a única solução de automação de recuperação de desastres e migração para vVols suportada pelo NetApp, e as ferramentas ONTAP verificarão a existência de um servidor SRM 8,3 ou posterior registrado no vCenter antes de permitir a replicação do vVols, embora seja possível aproveitar as APIS REST do ONTAP Tools para criar seus próprios serviços.

Replicação do vVols com o SRM



Suporte à MetroCluster

Embora as ferramentas do ONTAP não sejam capazes de acionar um switchover do MetroCluster, ele oferece suporte a sistemas NetApp MetroCluster para vVols que suportam volumes em uma configuração uniforme de cluster de storage metro do vSphere (vmsc). O switchover de um sistema MetroCluster é Tratado da maneira normal.

Embora o NetApp SnapMirror Business Continuity (SM-BC) também possa ser usado como base para uma configuração vmsc, ele não é atualmente suportado com vVols.

Consulte estes guias para obter mais informações sobre o NetApp MetroCluster:

"*Arquitetura e design da solução IP MetroCluster TR-4689*"

"*TR-4705 arquitetura e design da solução NetApp MetroCluster*"

"*VMware KB 2031038 suporte ao VMware vSphere com NetApp MetroCluster*"

Visão geral do vVols Backup

Existem várias abordagens para proteger VMs, como usar agentes de backup in-Guest, anexar arquivos de dados da VM a um proxy de backup ou usar APIs definidas como VMware VADP. O vVols pode ser protegido usando os mesmos mecanismos e muitos parceiros da NetApp suportam backups de VM, incluindo vVols.

Como mencionado anteriormente, os snapshots gerenciados do VMware vCenter são descarregados para ONTAP clones de arquivo/LUN rápidos e eficientes em termos de espaço. Eles podem ser usados para backups rápidos e manuais, mas são limitados pelo vCenter a um máximo de 32 snapshots. Você pode usar o vCenter para tirar snapshots e reverter conforme necessário.

A partir do plug-in SnapCenter para VMware vSphere (SCV) 4,6, quando usado em conjunto com as ferramentas ONTAP 9,10 e posteriores, adiciona suporte para backup e recuperação consistentes com falhas

de VMs baseadas em vVols, utilizando snapshots ONTAP FlexVol volume com suporte para replicação SnapMirror e SnapVault. Suporte para até 1023 instantâneos por volume. O SCV também pode armazenar mais snapshots com retenção mais longa em volumes secundários usando o SnapMirror com uma política de cofre-espelho.

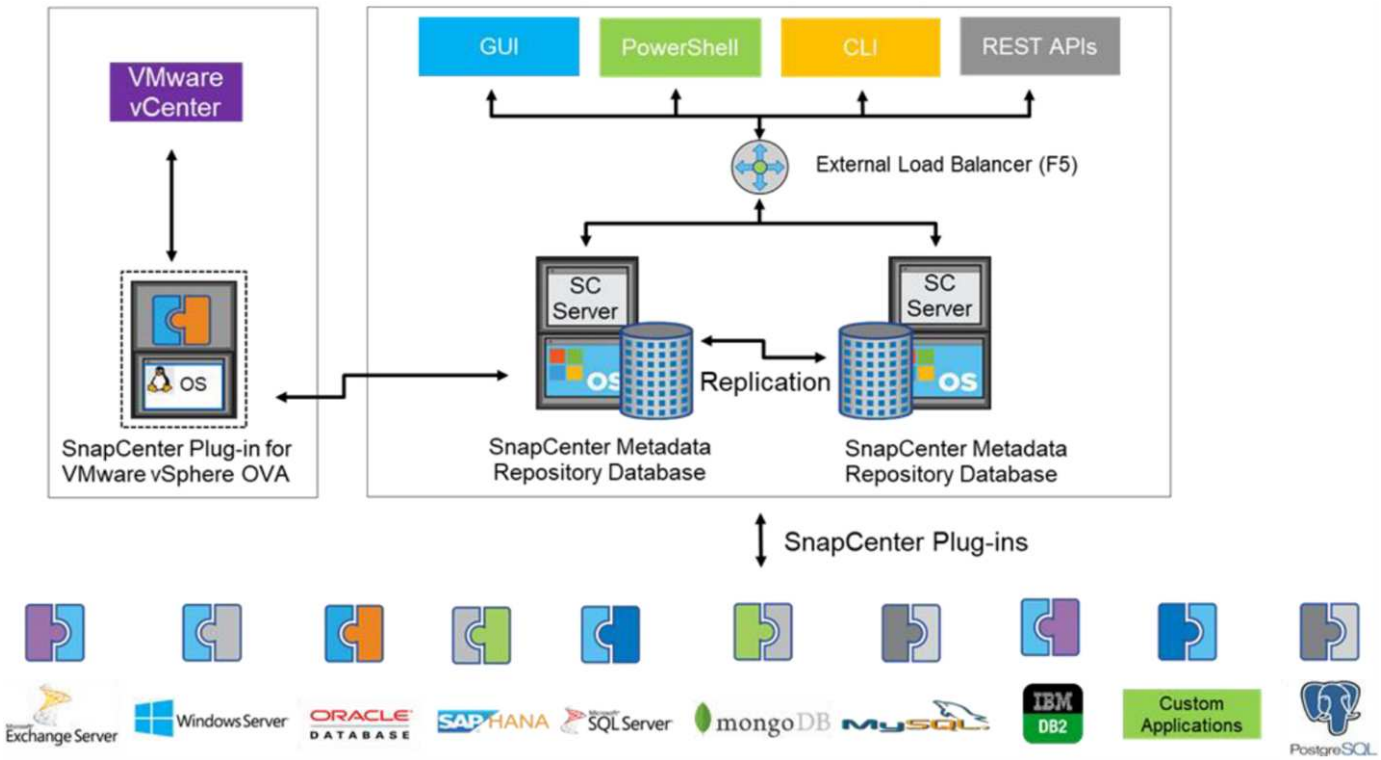
O suporte ao vSphere 8,0 foi introduzido com o SCV 4,7, que usou uma arquitetura de plug-in local isolada. O suporte ao vSphere 8.0U1 foi adicionado ao SCV 4,8, que fez a transição completa para a nova arquitetura de plug-in remoto.

Backup do vVols com o plug-in do SnapCenter para VMware vSphere

Com o NetApp SnapCenter, agora você pode criar grupos de recursos para vVols com base em tags e/ou pastas para aproveitar automaticamente os snapshots baseados no FlexVol do ONTAP para VMs baseadas em vVols. Isso permite que você defina serviços de backup e recuperação que protegerão as VMs automaticamente à medida que elas são provisionadas dinamicamente em seu ambiente.

O plug-in do SnapCenter para VMware vSphere é implantado como um dispositivo autônomo registrado como uma extensão do vCenter, gerenciado por meio da IU do vCenter ou por meio de APIs REST para automação de serviços de backup e recuperação.

Arquitetura da SnapCenter



Como os outros plugins do SnapCenter ainda não suportam vVols no momento desta escrita, vamos nos concentrar no modelo de implantação independente neste documento.

Como o SnapCenter usa snapshots do ONTAP FlexVol, não há sobrecarga no vSphere, nem há nenhuma penalidade de desempenho como se pode ver nas VMs tradicionais que usam snapshots gerenciados do vCenter. Além disso, como a funcionalidade do SCV é exposta por meio de APIs REST, ele facilita a criação de fluxos de trabalho automatizados usando ferramentas como VMware Aria Automation, Ansible, Terraform e praticamente qualquer outra ferramenta de automação capaz de usar APIs REST padrão.

Para obter informações sobre APIS REST do SnapCenter, consulte "Visão geral das APIs REST"

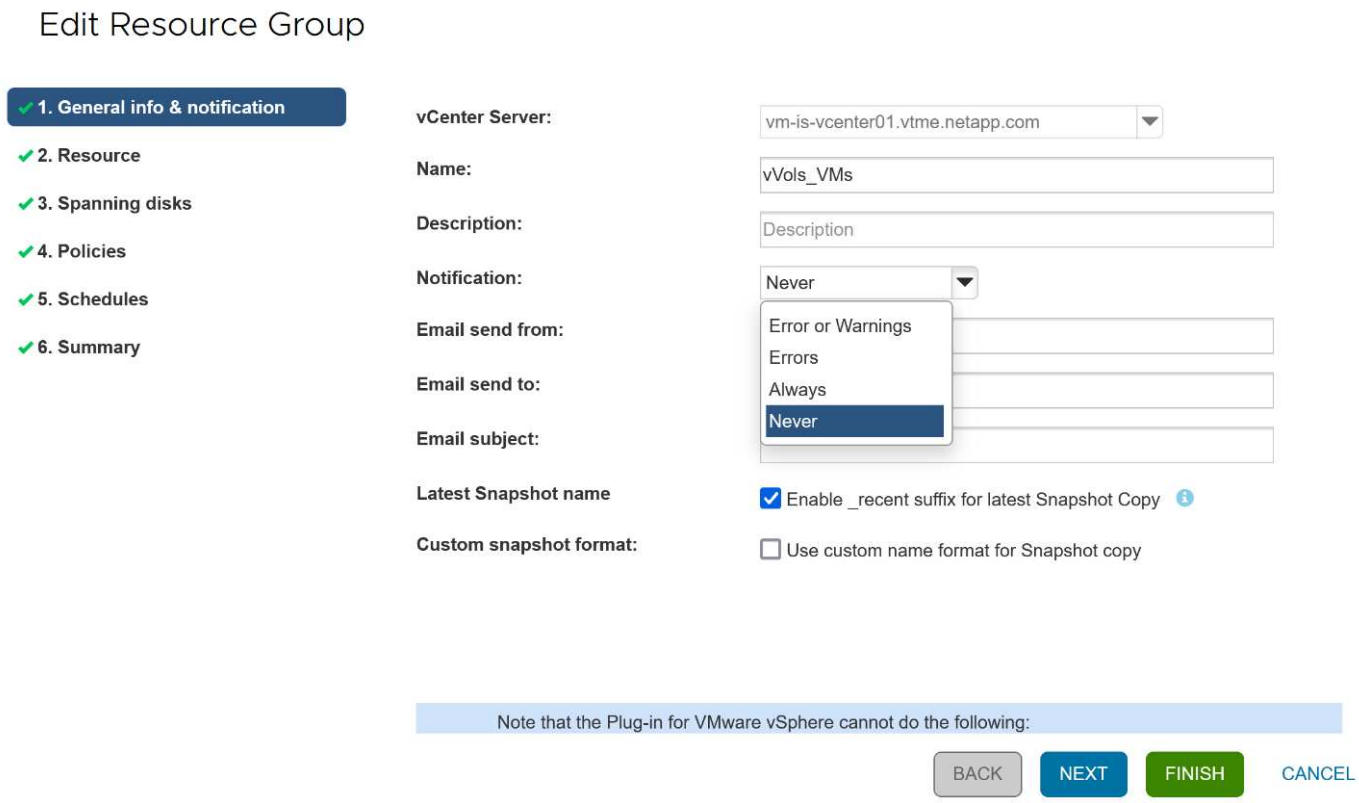
Para obter informações sobre o plug-in do SnapCenter para APIs REST do VMware vSphere, consulte "Plug-in do SnapCenter para APIs REST do VMware vSphere"

Práticas recomendadas

As práticas recomendadas a seguir podem ajudá-lo a aproveitar ao máximo sua implantação do SnapCenter.

- O SCV oferece suporte ao vCenter Server RBAC e ao ONTAP RBAC e inclui funções do vCenter predefinidas que são criadas automaticamente para você quando o plug-in é registrado. Você pode ler mais sobre os tipos compatíveis de RBAC "aqui."
  - Use a IU do vCenter para atribuir acesso a contas com menos privilégios usando as funções predefinidas descritas "aqui".
  - Se você usar o SCV com o servidor SnapCenter, deverá atribuir a função *SnapCenterAdmin*.
  - ONTAP RBAC refere-se à conta de usuário usada para adicionar e gerenciar os sistemas de storage usados pela SCV. O ONTAP RBAC não se aplica a backups baseados em vVols. Leia mais sobre ONTAP RBAC e SCV "aqui".
- Replique seus conjuntos de dados de backup para um segundo sistema usando o SnapMirror para réplicas completas de volumes de origem. Como mencionado anteriormente, você também pode usar políticas de espelhamento de cofre para retenção de dados de backup a longo prazo, independentemente das configurações de retenção de snapshot do volume de origem. Ambos os mecanismos são suportados com vVols.
- Como o SCV também requer ferramentas do ONTAP para a funcionalidade vVols do VMware vSphere, verifique sempre a ferramenta de Matriz de interoperabilidade (IMT) do NetApp para obter compatibilidade de versões específicas
- Se você estiver usando a replicação do vVols com o VMware SRM, lembre-se de sua política de RPO e agendamento de backup
- Crie suas políticas de backup com configurações de retenção que atendem aos objetivos do ponto de restauração (RPOs) definidos pela organização
- Configure as configurações de notificação em seus grupos de recursos para ser notificado sobre o status quando os backups são executados (veja a figura 10 abaixo)

Opções de notificação do grupo de recursos



Comece a usar a SCV usando esses documentos

"Saiba mais sobre o plug-in do SnapCenter para VMware vSphere"

"Implante o plug-in do SnapCenter para VMware vSphere"

Solução de problemas

Existem vários recursos de solução de problemas disponíveis com informações adicionais.

Site de suporte da NetApp

Além de uma variedade de artigos da base de conhecimento para produtos de virtualização NetApp, o site de suporte da NetApp também oferece uma página de destino conveniente para o "Ferramentas do ONTAP para VMware vSphere" produto. Este portal fornece links para artigos, downloads, relatórios técnicos e discussões sobre soluções VMware na Comunidade NetApp. Está disponível em:

"*Site de suporte da NetApp*"

A documentação adicional da solução está disponível aqui:

"*Soluções NetApp para virtualização com VMware da Broadcom*"

Solução de problemas do produto

Os vários componentes das ferramentas do ONTAP, como o plug-in do vCenter, o provedor VASA e o adaptador de replicação de armazenamento, estão todos documentados juntos no repositório de documentos do NetApp. No entanto, cada um tem uma subseção separada da base de dados de Conhecimento e pode ter

procedimentos específicos de solução de problemas. Estes abordam os problemas mais comuns que podem ser encontrados com o Fornecedor VASA.

Problemas de UI do provedor VASA

Ocasionalmente, o Cliente Web do vCenter vSphere encontra problemas com os componentes do Serenity, fazendo com que os itens do menu Fornecedor VASA para ONTAP não sejam exibidos. Consulte Resolução de problemas de Registro do provedor VASA no Guia de implantação ou nesta base de conhecimento "artigo".

Falha no provisionamento do armazenamento de dados do vVols

Ocasionalmente, os serviços do vCenter podem ter tempo limite ao criar o armazenamento de dados do vVols. Para corrigi-lo, reinicie o serviço vmware-sps e reinstale o datastore vVols usando os menus do vCenter (Storage > New datastore). Isso é coberto em falhas de provisionamento de armazenamento de dados do vVols com o vCenter Server 6,5 no Guia de administração.

A atualização do Unified Appliance falha ao montar o ISO

Devido a um bug no vCenter, o ISO usado para atualizar o dispositivo unificado de uma versão para a próxima pode não ser montado. Se o ISO puder ser anexado ao dispositivo no vCenter, siga o processo nesta base de conhecimento "artigo" para resolver.

VMware Site Recovery Manager com ONTAP

Recuperação do site ao vivo da VMware com o ONTAP

O ONTAP tem sido uma solução de armazenamento líder para o VMware vSphere e, mais recentemente, para o Cloud Foundation, desde que o ESX foi introduzido em datacenters modernos há mais de duas décadas. A NetApp continua a introduzir sistemas inovadores, como a última geração da série ASA A, juntamente com recursos como a sincronização ativa SnapMirror . Esses avanços simplificam o gerenciamento, aumentam a resiliência e reduzem o custo total de propriedade (TCO) da sua infraestrutura de TI.

Este documento apresenta a solução ONTAP para VMware Live Site Recovery (VLSR), anteriormente conhecido como Site Recovery Manager (SRM), o software de recuperação de desastres (DR) líder do setor da VMware, incluindo as informações mais recentes sobre o produto e as melhores práticas para otimizar a implantação, reduzir riscos e simplificar o gerenciamento contínuo.

Esta documentação substitui o relatório técnico publicado anteriormente *TR-4900: VMware Site Recovery Manager com ONTAP*

As práticas recomendadas complementam outros documentos, como guias e ferramentas de compatibilidade. Eles são desenvolvidos com base em testes de laboratório e extensa experiência de campo por engenheiros e clientes da NetApp. Em alguns casos, as melhores práticas recomendadas podem não ser a opção certa para o seu ambiente; no entanto, geralmente são as soluções mais simples que atendem às necessidades da maioria dos clientes.

Este documento se concentra nos recursos das versões recentes do ONTAP 9 quando usado em conjunto com as ferramentas do ONTAP para VMware vSphere 10,4 (que inclui o adaptador de replicação de armazenamento NetApp [SRA] e o provedor VASA [VP]), bem como o VMware Live Site Recovery 9.

Por que usar o ONTAP com VLSR ou SRM?

As plataformas de gerenciamento de dados da NetApp com tecnologia ONTAP são algumas das soluções de armazenamento mais amplamente adotadas para VLSR. Os motivos são muitos: uma plataforma de gerenciamento de dados segura, de alto desempenho e com protocolo unificado (NAS e SAN juntos) que fornece eficiência de armazenamento que define o setor, multilocação, controles de qualidade de serviço, proteção de dados com instantâneos com eficiência de espaço e replicação com SnapMirror. Tudo isso aproveitando a integração nativa de multi-nuvem híbrida para a proteção de cargas de trabalho do VMware e uma infinidade de ferramentas de automação e orquestração ao seu alcance.

Ao usar o SnapMirror para replicação baseada em array, você aproveita uma das tecnologias mais comprovadas e maduras do ONTAP. O SnapMirror oferece a vantagem de transferências de dados seguras e altamente eficientes, copiando apenas blocos alterados do sistema de arquivos, não VMs ou armazenamentos de dados inteiros. Mesmo esses blocos aproveitam a economia de espaço, como desduplicação, compactação e compactação. Os sistemas ONTAP modernos agora usam o SnapMirror independente de versão, permitindo flexibilidade na seleção de seus clusters de origem e destino. O SnapMirror realmente se tornou uma das ferramentas mais poderosas disponíveis para recuperação de desastres.

Não importa se você usa armazenamentos de dados tradicionais NFS, iSCSI ou Fibre Channel (agora com suporte para armazenamentos de dados vVols), o VLSR fornece uma oferta primária robusta que aproveita o melhor dos recursos do ONTAP para recuperação de desastres ou planejamento e orquestração de migração de datacenter.

Como o VLSR utiliza o ONTAP 9

O VLSR aproveita as tecnologias avançadas de gerenciamento de dados dos sistemas ONTAP integrando-se às ferramentas do ONTAP para VMware vSphere, um dispositivo virtual que inclui três componentes principais:

- O plug-in do ONTAP Tools vCenter, anteriormente conhecido como VSC (Virtual Storage Console), simplifica o gerenciamento de storage e os recursos de eficiência, aprimora a disponibilidade e reduz os custos de storage e a sobrecarga operacional, não importa se você está usando SAN ou nas. Ele usa as práticas recomendadas para provisionar armazenamentos de dados e otimiza as configurações de host ESXi para ambientes de storage de bloco e NFS. Para todos esses benefícios, a NetApp recomenda esse plug-in ao usar o vSphere com sistemas que executam o ONTAP.
- O provedor VASA (ONTAP Tools) oferece suporte à estrutura VMware vStorage APIs for Storage Awareness (VASA). O provedor VASA coneta o vCenter Server com o ONTAP para auxiliar no provisionamento e monitoramento do armazenamento de VM. Isso permitiu o suporte ao VMware Virtual volumes (vVols), o gerenciamento de políticas de storage de VM e o desempenho individual do VM vVols. Ele também fornece alarmes para monitorar a capacidade e conformidade com os perfis.
- O SRA é usado em conjunto com o VLSR para gerenciar a replicação de dados de VM entre locais de produção e recuperação de desastres para armazenamentos de dados VMFS e NFS tradicionais e também para testes sem interrupções de réplicas de DR. Ele ajuda a automatizar as tarefas de descoberta, recuperação e reproteção. Ele inclui um dispositivo de servidor SRA e adaptadores SRA para o servidor Windows SRM e o dispositivo VLSR.

Depois de instalar e configurar os adaptadores SRA no servidor VLSR para proteger armazenamentos de dados não vVols, você pode começar a tarefa de configurar seu ambiente vSphere para recuperação de desastres.

O SRA oferece uma interface de comando e controle para o servidor VLSR gerenciar os volumes ONTAP FlexVol que contêm suas máquinas virtuais (VMs) da VMware, bem como a replicação do SnapMirror que os protege.

A VLSR pode testar seu plano de DR sem interrupções usando a tecnologia FlexClone proprietária da NetApp para fazer clones quase instantâneos de seus armazenamentos de dados protegidos em seu site de DR. O VLSR cria um sandbox para testes seguros, para que sua organização e seus clientes estejam protegidos em caso de um desastre real, dando a você confiança na capacidade de sua organização de executar um failover durante um desastre.

No caso de um verdadeiro desastre ou mesmo de uma migração planejada, o VLSR permite que você envie quaisquer alterações de última hora para o conjunto de dados por meio de uma atualização final do SnapMirror (se você optar por fazê-lo). Em seguida, ele quebra o espelho e monta o datastore em seus hosts de DR. Nesse ponto, suas VMs podem ser automaticamente ativadas em qualquer ordem de acordo com sua estratégia pré-planejada.

Embora os sistemas ONTAP permitam emparelhar SVMs no mesmo cluster para replicação do SnapMirror, esse cenário não é testado e certificado com o VLSR. Portanto, é recomendável usar apenas SVMs de diferentes clusters ao usar o VLSR.

VLSR com ONTAP e outros casos de uso: Nuvem híbrida e migração

A integração da sua implantação de VLSR com os recursos avançados de gerenciamento de dados do ONTAP permite escala e desempenho significativamente melhores quando comparado com opções de armazenamento local. Mas mais do que isso, ele traz a flexibilidade da nuvem híbrida. A nuvem híbrida permite que você economize dinheiro ao hierarquizar blocos de dados não utilizados do seu array de alto desempenho para o seu hiperescalador preferido usando o FabricPool, que pode ser um armazenamento S3 local, como o NetApp StorageGRID. Você também pode usar o SnapMirror para sistemas baseados em borda com ONTAP Select definido por software ou DR baseado em nuvem usando "Armazenamento NetApp no Equinix Metal", ou outros serviços ONTAP hospedados.

Depois, você pode executar failover de teste no data center de um fornecedor de serviços de nuvem com espaço físico de storage quase zero graças ao FlexClone. Proteger sua organização agora pode custar menos do que nunca.

O VLSR também pode ser usado para executar migrações planejadas utilizando o SnapMirror para transferir eficientemente suas VMs de um data center para outro ou até mesmo dentro do mesmo data center, seja seu, ou por meio de qualquer número de provedores de serviços parceiros da NetApp.

Práticas recomendadas de implantação

As seções a seguir descrevem as práticas recomendadas de implantação com o ONTAP e o VMware SRM.

Use a versão mais recente das ferramentas do ONTAP 10

O ONTAP Tools 10 fornece melhorias significativas em relação às versões anteriores, incluindo o seguinte:

- failover de teste 8xx mais rápido*
- limpeza e reproteção 2xx mais rápidas*
- failover 32% mais rápido*
- Maior escala
- Suporte nativo para layouts de site compartilhados

*Essas melhorias são baseadas em testes internos e podem variar de acordo com o seu ambiente.

Layout e segmentação do SVM para SMT

Com o ONTAP, o conceito de máquina virtual de storage (SVM) fornece segmentação rigorosa em ambientes multitenant seguros. Os usuários do SVM em um SVM não podem acessar ou gerenciar recursos de outro. Dessa forma, você pode utilizar a tecnologia ONTAP criando SVMs separadas para diferentes unidades de negócios que gerenciam seus próprios fluxos de trabalho SRM no mesmo cluster para maior eficiência geral de storage.

Considere o gerenciamento do ONTAP usando contas com escopo SVM e LIFs de gerenciamento de SVM para aprimorar não apenas os controles de segurança, mas também a performance. O desempenho é inerentemente maior ao usar conexões com escopo SVM, pois o SRA não é necessário para processar todos os recursos em um cluster inteiro, incluindo recursos físicos. Em vez disso, ele só precisa entender os ativos lógicos que são abstraídos para o SVM específico.

Práticas recomendadas para gerenciamento de sistemas ONTAP 9

Como mencionado anteriormente, você pode gerenciar clusters do ONTAP usando credenciais de escopo do cluster ou SVM e LIFs de gerenciamento. Para um desempenho ideal, você pode considerar o uso de credenciais com escopo SVM sempre que não estiver usando vVols. No entanto, ao fazer isso, você deve estar ciente de alguns requisitos, e que você perde alguma funcionalidade.

- A conta padrão do vsadmin SVM não tem o nível de acesso necessário para executar tarefas de ferramentas do ONTAP. Portanto, você precisa criar uma nova conta SVM. "Configurar as funções de usuário do ONTAP e o Privileges" Usando o arquivo JSON incluído. Isso pode ser usado para contas com escopo de SVM ou cluster.
- Como o plug-in da IU do vCenter, o provedor VASA e o servidor SRA são todos microsserviços totalmente integrados, você deve adicionar armazenamento ao adaptador SRA no SRM da mesma forma que você adiciona armazenamento na IU do vCenter para ferramentas do ONTAP. Caso contrário, o servidor SRA pode não reconhecer as solicitações enviadas do SRM através do adaptador SRA.
- A verificação de caminho NFS não é realizada ao usar credenciais com escopo SVM, a menos que você primeiro "clusters integrados" no Gerenciador de ferramentas do ONTAP e associe-as a vCenters. Isso ocorre porque a localização física é logicamente abstraída do SVM. No entanto, isso não é motivo de preocupação, já que os sistemas ONTAP modernos não sofrem mais nenhum declínio de desempenho percetível ao usar caminhos indiretos.
- Economias de espaço agregado devido à eficiência de storage podem não ser relatadas.
- Quando suportado, os espelhos de partilha de carga não podem ser atualizados.
- O log do EMS pode não ser realizado em sistemas ONTAP gerenciados com credenciais de escopo da SVM.

Práticas recomendadas operacionais

As seções a seguir descrevem as práticas recomendadas operacionais para o storage VMware SRM e ONTAP.

Armazenamentos de dados e protocolos

- Se possível, sempre use ferramentas do ONTAP para provisionar armazenamentos de dados e volumes. Isso garante que volumes, caminhos de junção, LUNs, grupos, políticas de exportação e outras configurações sejam configurados de maneira compatível.
- O SRM dá suporte a iSCSI, Fibre Channel e NFS versão 3 com ONTAP 9 ao usar replicação baseada em array por meio do SRA. O SRM não dá suporte à replicação baseada em array para NFS versão 4,1 com

datastores tradicionais ou vVols.

- Para confirmar a conectividade, verifique sempre se é possível montar e desmontar um novo datastore de teste no local de DR do cluster do ONTAP de destino. Teste cada protocolo que você pretende usar para a conetividade do datastore. Uma prática recomendada é usar as ferramentas do ONTAP para criar seu datastore de teste, já que ele está fazendo toda a automação do datastore, conforme indicado pelo SRM.
- Os protocolos SAN devem ser homogêneos para cada local. Você pode misturar NFS e SAN, mas os protocolos SAN não devem ser misturados em um local. Por exemplo, você pode usar FCP no local A e iSCSI no local B. você não deve usar FCP e iSCSI no local A.
- Guias anteriores aconselharam a criação de LIF para localidade de dados. Ou seja, monte sempre um datastore usando um LIF localizado no nó que possui fisicamente o volume. Embora essa ainda seja a melhor prática, não é mais um requisito nas versões modernas do ONTAP 9. Sempre que possível, e se forem dadas credenciais com escopo de cluster, as ferramentas do ONTAP ainda escolherão o balanceamento de carga entre LIFs locais para os dados, mas não será um requisito de alta disponibilidade ou desempenho.
- O ONTAP 9 pode ser configurado para remover automaticamente snapshots para preservar o tempo de atividade em caso de uma condição fora do espaço quando o dimensionamento automático não é capaz de fornecer capacidade de emergência suficiente. A configuração padrão para esse recurso não exclui automaticamente os snapshots criados pelo SnapMirror. Se os snapshots do SnapMirror forem excluídos, o NetApp SRA não poderá reverter e ressincronizar a replicação para o volume afetado. Para evitar que o ONTAP elimine instantâneos do SnapMirror, configure a capacidade de instantâneos para "tentar".

```
snap autodelete modify -volume -commitment try
```

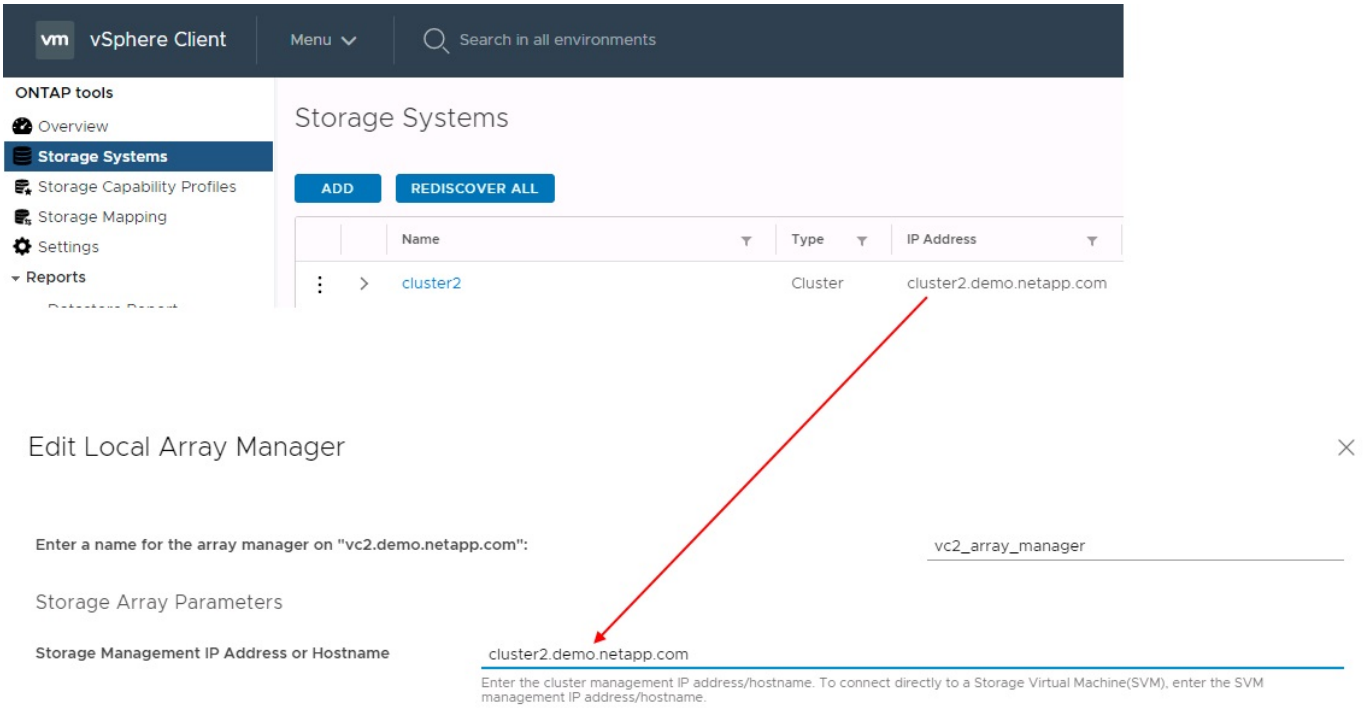
- O dimensionamento automático de volume deve ser definido como `grow` para volumes que contêm armazenamentos de dados SAN e `grow_shrink` para armazenamentos de dados NFS. Saiba mais sobre este tópico em "Configure volumes para aumentar e diminuir automaticamente o tamanho".
- O SRM tem melhor desempenho quando o número de datastores e, portanto, os grupos de proteção são minimizados em seus planos de recuperação. Portanto, você deve considerar a otimização para a densidade da VM em ambientes protegidos pelo SRM, onde o rto é de importância fundamental.
- Use o DRS (Distributed Resource Scheduler) para ajudar a equilibrar a carga nos clusters ESXi protegidos e de recuperação. Lembre-se de que, se você planeja fazer o failback, ao executar uma reproteção, os clusters anteriormente protegidos se tornarão os novos clusters de recuperação. O DRS ajudará a equilibrar a colocação em ambas as direções.
- Sempre que possível, evite usar a personalização de IP com o SRM, pois isso pode aumentar seu rto.

Sobre os pares de array

Um gerenciador de array é criado para cada par de array. Com as ferramentas SRM e ONTAP, cada emparelhamento de array é feito com o escopo de uma SVM, mesmo que você esteja usando credenciais de cluster. Isso permite segmentar fluxos de trabalho de DR entre locatários com base em quais SVMs eles foram atribuídos a gerenciar. Você pode criar vários gerenciadores de array para um determinado cluster, e eles podem ser assimétricos. Você pode fazer fan-out ou fan-out entre diferentes clusters do ONTAP 9. Por exemplo, você pode fazer a replicação do SVM-A e do SVM-B no Cluster-1 para SVM-C no Cluster-2, SVM-D no Cluster-3 ou vice-versa.

Ao configurar pares de matrizes no SRM, deve sempre adicioná-los no SRM da mesma forma que os adicionou às Ferramentas do ONTAP, ou seja, devem utilizar o mesmo nome de utilizador, palavra-passe e LIF de gestão. Esse requisito garante que o SRA se comunique adequadamente com o array. A captura de tela a seguir ilustra como um cluster pode aparecer nas Ferramentas do ONTAP e como ele pode ser

adicionado a um gerenciador de array.



Sobre os grupos de replicação

Os grupos de replicação contêm coleções lógicas de máquinas virtuais que são recuperadas juntas. Como a replicação do ONTAP SnapMirror ocorre no nível do volume, todas as VMs em um volume estão no mesmo grupo de replicação.

Há vários fatores a serem considerados nos grupos de replicação e como você distribui VMs pelos volumes do FlexVol. Agrupar VMs semelhantes no mesmo volume pode aumentar a eficiência de storage com sistemas ONTAP mais antigos que não possuem deduplicação em nível de agregado, mas o agrupamento aumenta o tamanho do volume e reduz a simultaneidade de e/S do volume. O melhor equilíbrio entre performance e eficiência de storage pode ser obtido em sistemas ONTAP modernos, distribuindo máquinas virtuais por volumes FlexVol no mesmo agregado, aproveitando a deduplicação em nível de agregado e obtendo maior paralelização de e/S em vários volumes. Você pode recuperar VMs nos volumes juntos porque um grupo de proteção (discutido abaixo) pode conter vários grupos de replicação. A desvantagem desse layout é que os blocos podem ser transmitidos por cabo várias vezes, porque o SnapMirror não leva em conta a deduplicação agregada.

Uma consideração final para grupos de replicação é que cada um é, por sua natureza, um grupo de consistência lógica (não deve ser confundido com grupos de consistência SRM). Isso ocorre porque todas as VMs no volume são transferidas juntas usando o mesmo snapshot. Portanto, se você tiver VMs que precisam ser consistentes umas com as outras, considere armazená-las no mesmo FlexVol.

Sobre grupos de proteção

Os grupos de proteção definem VMs e datastores em grupos que são recuperados juntos do site protegido. O local protegido é onde as VMs configuradas em um grupo de proteção existem durante operações normais de estado estacionário. É importante notar que, embora o SRM possa exibir vários gerenciadores de matriz para um grupo de proteção, um grupo de proteção não pode abranger vários gerenciadores de matriz. Por esse motivo, você não deve estender arquivos de VM entre armazenamentos de dados em diferentes SVMs.

Sobre planos de recuperação

Os planos de recuperação definem quais grupos de proteção são recuperados no mesmo processo. Vários grupos de proteção podem ser configurados no mesmo plano de recuperação. Além disso, para permitir mais opções para a execução de planos de recuperação, um único grupo de proteção pode ser incluído em vários planos de recuperação.

Os planos de recuperação permitem que os administradores do SRM definam fluxos de trabalho de recuperação atribuindo VMs a um grupo de prioridades de 1 (mais alto) a 5 (mais baixo), sendo 3 (médio) o padrão. Dentro de um grupo de prioridade, as VMs podem ser configuradas para dependências.

Por exemplo, sua empresa pode ter um aplicativo essencial para negócios de nível 1 que depende de um servidor Microsoft SQL para seu banco de dados. Então, você decide colocar suas VMs no grupo de prioridades 1. No grupo de prioridade 1, você começa a Planejar o pedido para abrir serviços. Você provavelmente quer que o controlador de domínio do Microsoft Windows seja inicializado antes do servidor Microsoft SQL, que precisaria estar online antes do servidor de aplicativos, e assim por diante. Você adicionaria todas essas VMs ao grupo de prioridade e, em seguida, definiria as dependências porque as dependências se aplicam somente a um determinado grupo de prioridade.

A NetApp recomenda fortemente que você trabalhe com suas equipes de aplicações para entender a ordem das operações necessárias em um cenário de failover e para construir seus planos de recuperação adequadamente.

Failover de teste

Como prática recomendada, sempre execute um failover de teste sempre que for feita uma alteração na configuração do storage de VM protegido. Isso garante que, no caso de um desastre, você possa confiar que o Site Recovery Manager pode restaurar serviços dentro do destino de rto esperado.

O NetApp também recomenda confirmar ocasionalmente a funcionalidade do aplicativo in-Guest, especialmente depois de reconfigurar o armazenamento de VM.

Quando uma operação de recuperação de teste é executada, uma rede privada de bolhas de teste é criada no host ESXi para as VMs. No entanto, essa rede não é conetada automaticamente a nenhum adaptador de rede físico e, portanto, não fornece conetividade entre os hosts ESXi. Para permitir a comunicação entre VMs que estão sendo executadas em diferentes hosts ESXi durante o teste de DR, uma rede privada física é criada entre os hosts ESXi no local de DR. Para verificar se a rede de teste é privada, a rede de bolhas de teste pode ser separada fisicamente ou usando VLANs ou marcação de VLAN. Essa rede deve ser segregada da rede de produção porque, à medida que as VMs são recuperadas, elas não podem ser colocadas na rede de produção com endereços IP que podem entrar em conflito com os sistemas de produção reais. Quando um plano de recuperação é criado no SRM, a rede de teste criada pode ser selecionada como a rede privada para conetar as VMs durante o teste.

Depois que o teste tiver sido validado e não for mais necessário, execute uma operação de limpeza. A limpeza em execução retorna as VMs protegidas ao seu estado inicial e redefine o plano de recuperação para o estado Pronto.

Considerações sobre failover

Há várias outras considerações quando se trata de falhar em um local, além da ordem de operações mencionada neste guia.

Um problema que você pode ter que lidar com as diferenças de rede entre sites. Alguns ambientes podem ser capazes de usar os mesmos endereços IP de rede no local principal e no local de DR. Essa capacidade é referida como uma LAN virtual (VLAN) estendida ou configuração de rede estendida. Outros ambientes

podem ter um requisito para usar endereços IP de rede diferentes (por exemplo, em VLANs diferentes) no local principal em relação ao local de DR.

A VMware oferece várias maneiras de resolver esse problema. Por um lado, tecnologias de virtualização de rede como o VMware NSX-T Data Center abstraem toda a pilha de rede das camadas 2 a 7 do ambiente operacional, permitindo soluções mais portáteis. Saiba mais "Opções NSX-T com SRM"sobre o .

O SRM também lhe dá a capacidade de alterar a configuração de rede de uma VM à medida que ela é recuperada. Essa reconfiguração inclui configurações como endereços IP, endereços de gateway e configurações de servidor DNS. Diferentes configurações de rede, que são aplicadas a VMs individuais à medida que são recuperadas, podem ser especificadas nas configurações da propriedade de uma VM no plano de recuperação.

Para configurar o SRM para aplicar diferentes configurações de rede a várias VMs sem ter que editar as propriedades de cada uma no plano de recuperação, a VMware fornece uma ferramenta chamada DR-ip-Customizer. Saiba como usar este utilitário, "Documentação da VMware"consulte .

Reproteger

Após uma recuperação, o local de recuperação se torna o novo local de produção. Como a operação de recuperação quebrou a replicação do SnapMirror, o novo local de produção não fica protegido de nenhum desastre futuro. Uma prática recomendada é proteger o novo local de produção para outro local imediatamente após uma recuperação. Se o local de produção original estiver operacional, o administrador da VMware poderá usar o local de produção original como um novo local de recuperação para proteger o novo local de produção, invertendo efetivamente o sentido de proteção. A reproteção está disponível apenas em falhas não catastróficas. Portanto, os vCenter Servers originais, os servidores ESXi, os servidores SRM e os bancos de dados correspondentes devem ser eventualmente recuperáveis. Se eles não estiverem disponíveis, um novo grupo de proteção e um novo plano de recuperação devem ser criados.

Failback

Uma operação de failback é fundamentalmente um failover em uma direção diferente do anterior. Como prática recomendada, você verifica se o site original está de volta aos níveis aceitáveis de funcionalidade antes de tentar failback ou, em outras palavras, failover para o site original. Se o local original ainda estiver comprometido, você deve atrasar o failback até que a falha seja suficientemente remediada.

Outra prática recomendada de failback é sempre executar um failover de teste após concluir a reproteção e antes de fazer seu failback final. Isso verifica se os sistemas no local original podem concluir a operação.

Reproteger o site original

Após o failback, você deve confirmar com todas as partes interessadas que seus serviços foram devolvidos ao normal antes de executar o reprotect novamente,

A execução do reprotect After failback coloca essencialmente o ambiente de volta ao estado em que estava no início, com a replicação do SnapMirror sendo executada novamente do local de produção para o local de recuperação.

Topologias de replicação

No ONTAP 9, os componentes físicos de um cluster são visíveis para os administradores de cluster, mas não são visíveis diretamente para os aplicativos e hosts que usam o cluster. Os componentes físicos fornecem um pool de recursos compartilhados a partir do qual os recursos lógicos do cluster são construídos. As aplicações e os hosts

acessam dados somente por meio de SVMs que contêm volumes e LIFs.

Cada NetApp SVM é tratado como uma matriz exclusiva no Site Recovery Manager. O VLSR oferece suporte a determinados layouts de replicação de matriz para matriz (ou SVM para SVM).

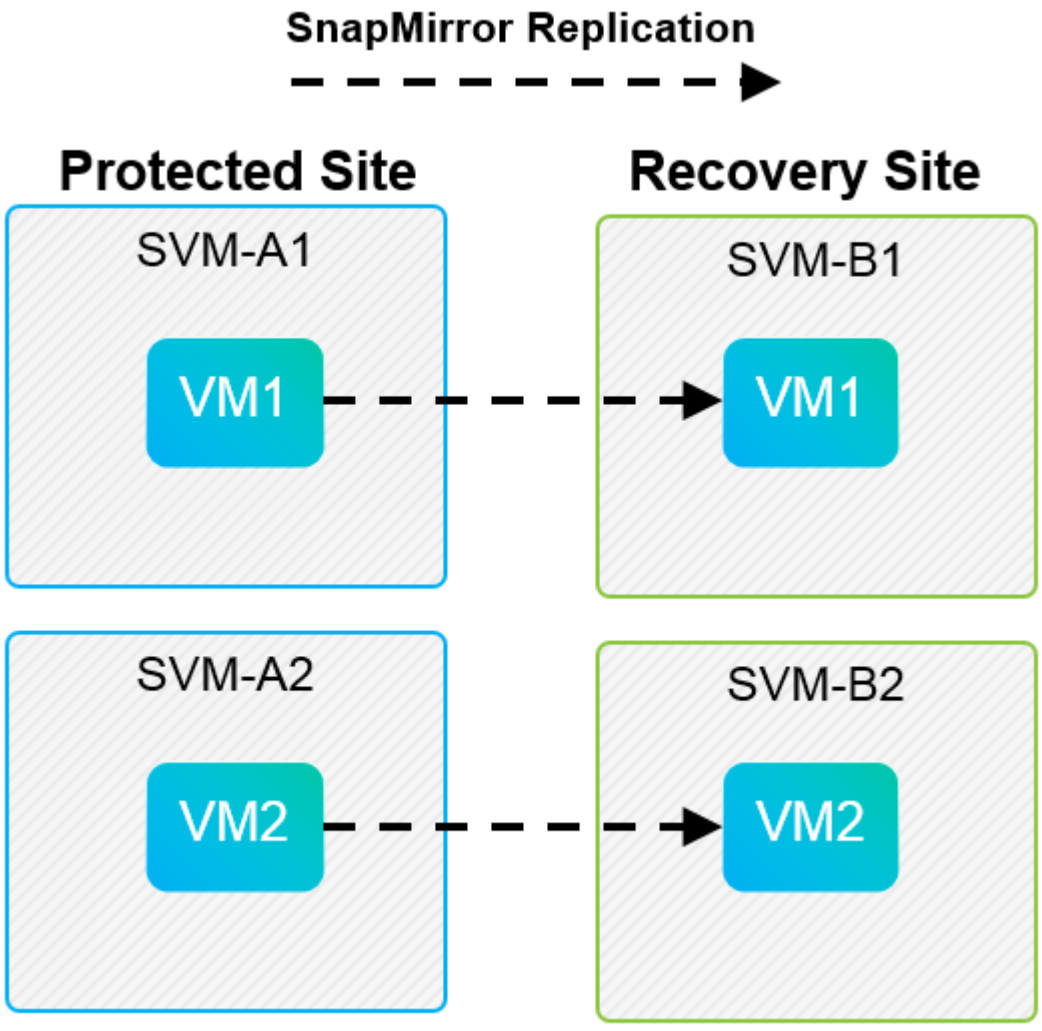
Uma única VM não pode possuir dados – Virtual Machine Disk (VMDK) ou RDM – em mais de um array VLSR pelos seguintes motivos:

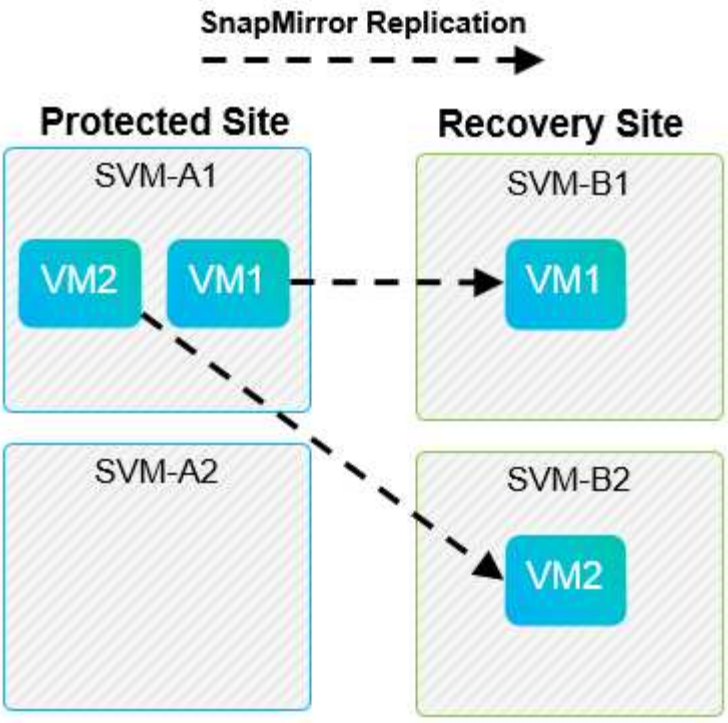
- O VLSR vê apenas o SVM, e não um controlador físico individual.
- Um SVM pode controlar LUNs e volumes que abrangem vários nós em um cluster.

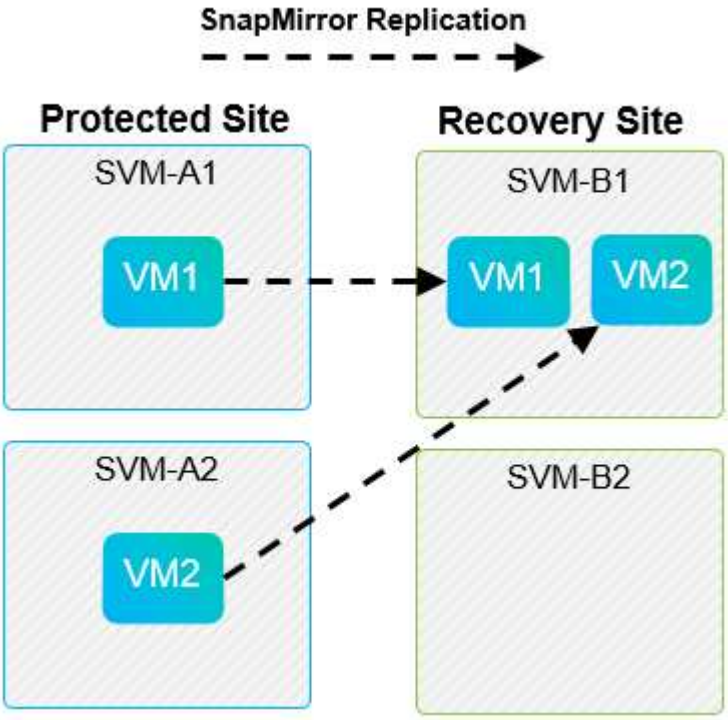
Prática recomendada
Para determinar a capacidade de suporte, tenha em mente esta regra: Para proteger uma VM usando o VLSR e o NetApp SRA, todas as partes da VM devem existir em apenas uma SVM. Esta regra aplica-se tanto no local protegido como no local de recuperação.

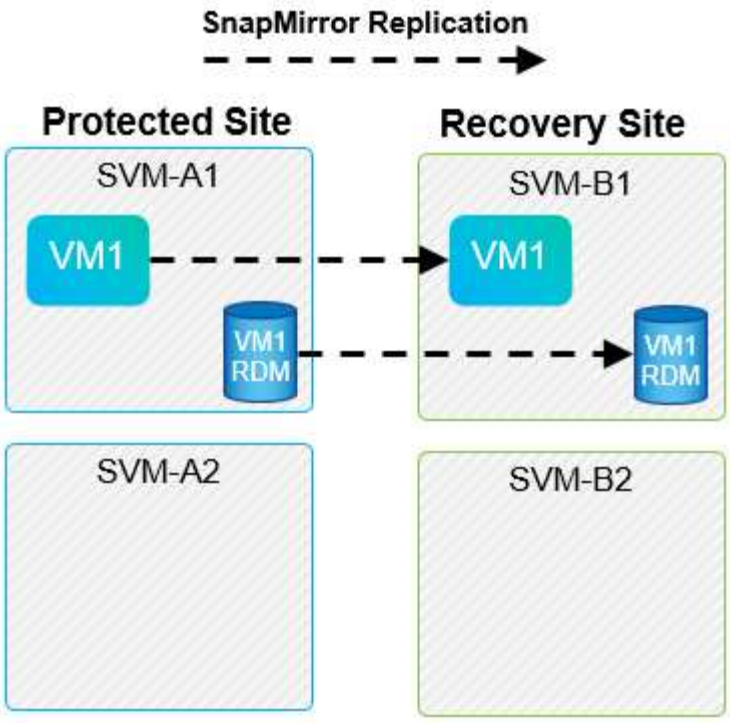
Layouts SnapMirror suportados

As figuras a seguir mostram os cenários de layout de relacionamento do SnapMirror que o VLSR e o SRA suportam. Cada VM nos volumes replicados possui dados em apenas um array VLSR (SVM) em cada local.




SnapMirror Replication
Protected Site
Recovery Site
SVM-A1
SVM-B1
VM2
VM1
VM1
SVM-A2
SVM-B2
VM2


SnapMirror Replication
Protected Site
Recovery Site
SVM-A1
SVM-B1
VM1
VM1
VM2
SVM-A2
SVM-B2
VM2



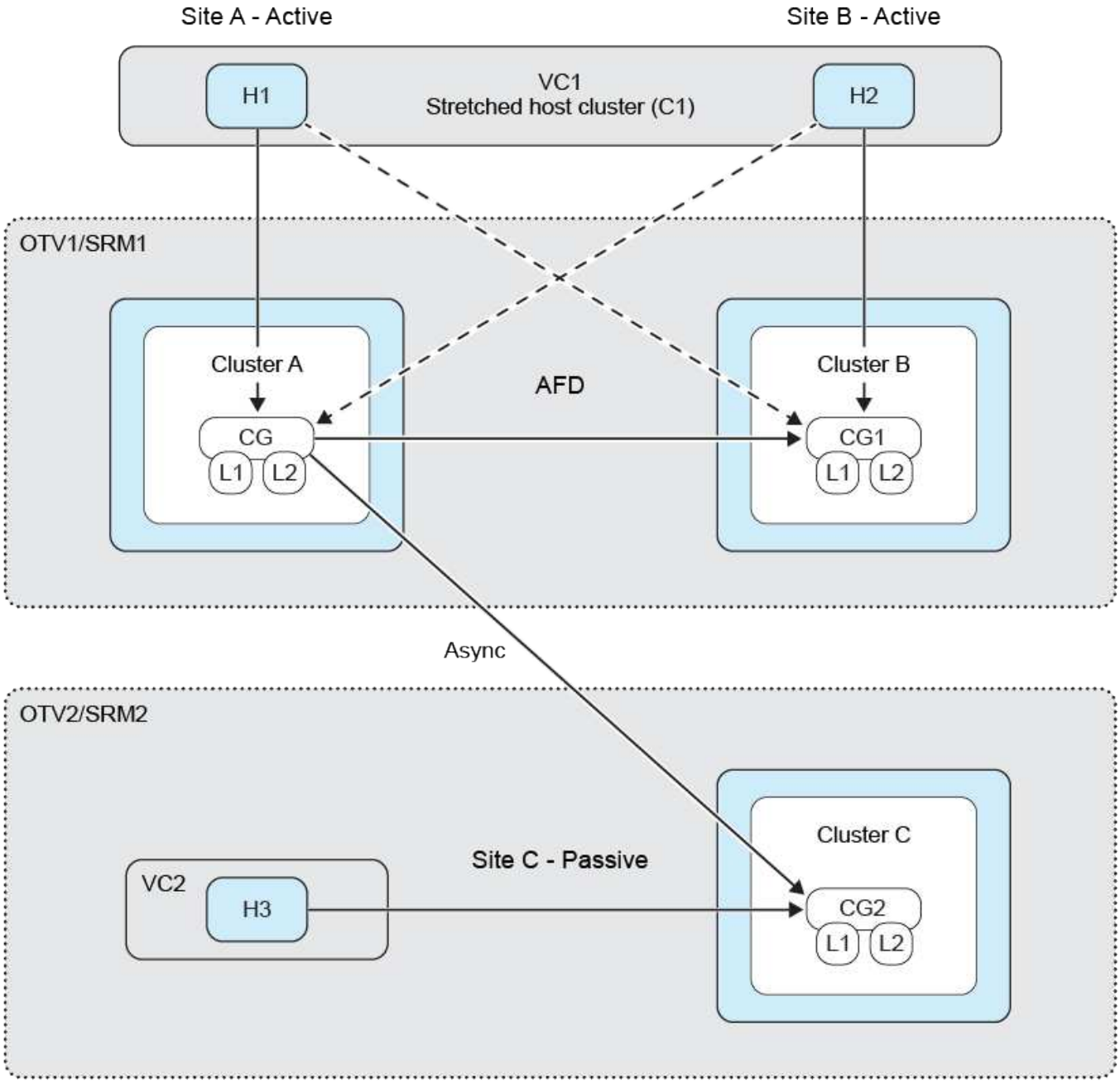
Suporte VMFS com sincronização ativa SnapMirror

As ferramentas ONTAP 10.3 e posteriores também oferecem suporte à proteção de seus armazenamentos de dados VMFS com sincronização ativa do SnapMirror (SMas). Isso permite failover transparente para continuidade de negócios entre dois datacenters (chamados de domínios de falha) que estão relativamente próximos. A recuperação de desastres de longa distância pode então ser orquestrada usando o SnapMirror de forma assíncrona por meio das ferramentas ONTAP SRA com VLSR.

"Saiba mais sobre a sincronização ativa do ONTAP SnapMirror"

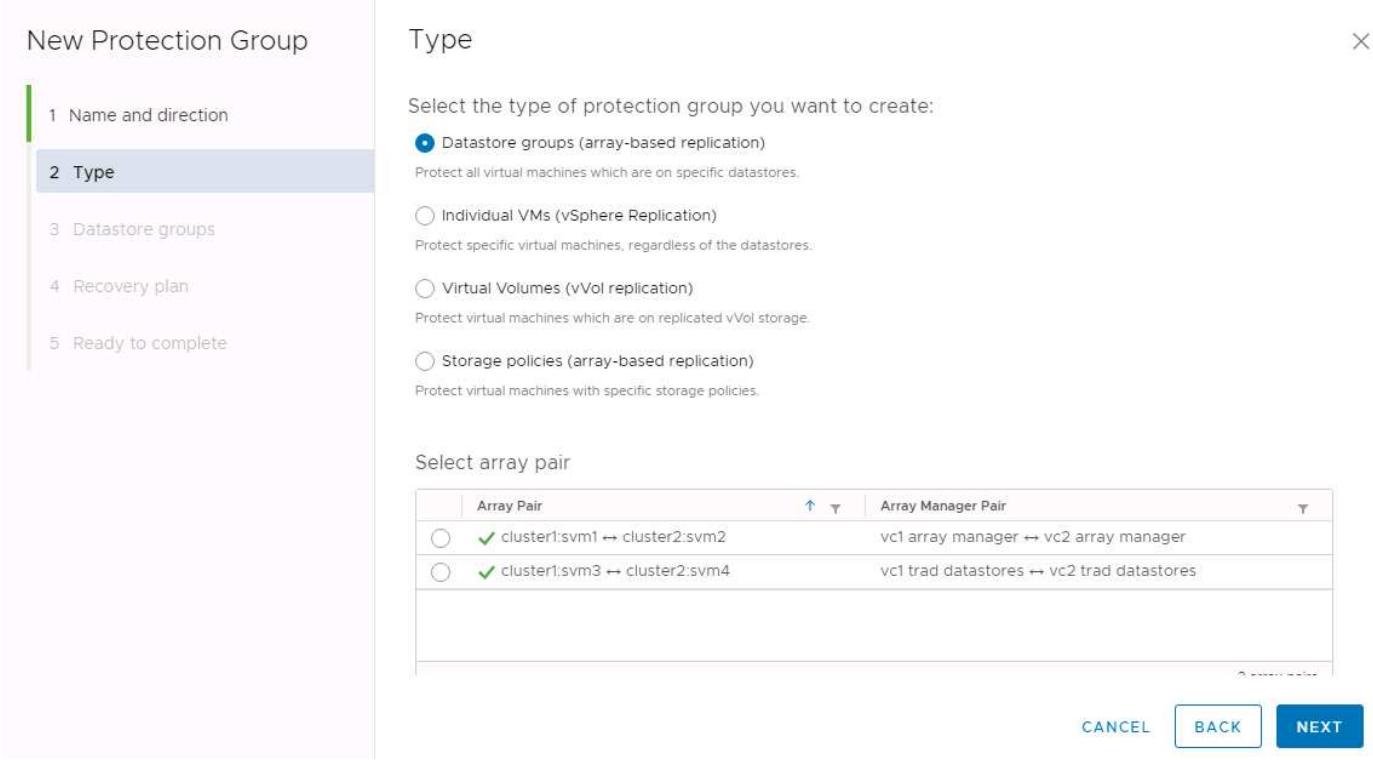
Os armazenamentos de dados são reunidos em um grupo de consistência (CG), e as VMs em todos os armazenamentos de dados permanecerão consistentes na ordem de gravação como membros do mesmo CG.

Alguns exemplos podem ser ter sites em Berlim e Hamburgo protegidos por SMas e uma terceira réplica de site usando SnapMirror assíncrono e protegido por VLSR. Outro exemplo pode ser proteger locais em Nova York e Nova Jersey usando SMas, com um terceiro local em Chicago.



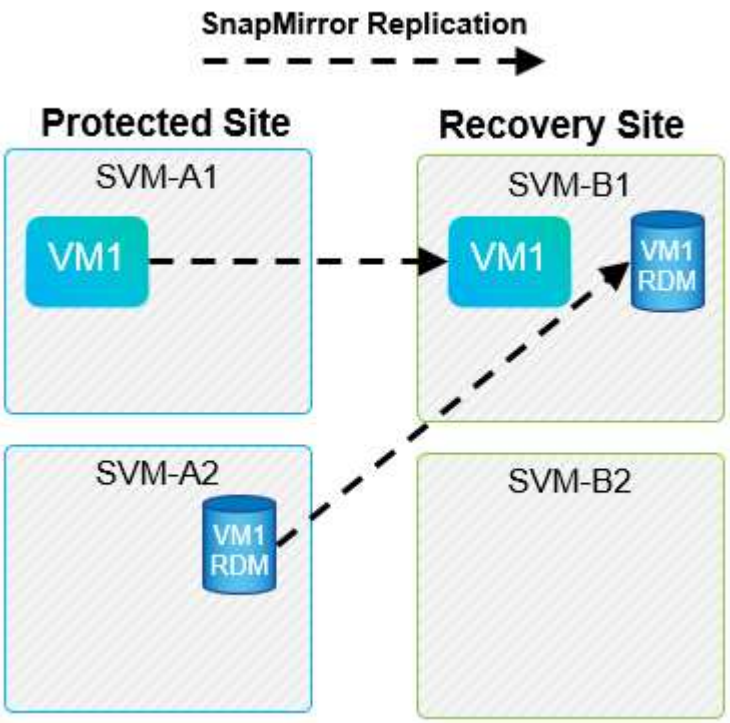
Layouts do Array Manager compatíveis

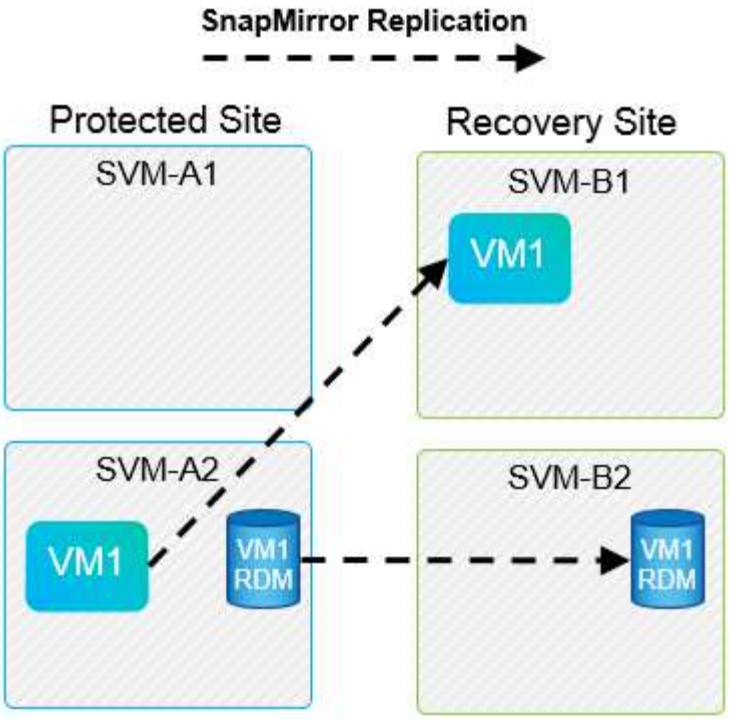
Quando você usa a replicação baseada em array (ABR) no VLSR, os grupos de proteção são isolados a um único par de array, como mostrado na captura de tela a seguir. Neste cenário, `SVM1` e `SVM2` são percorridos com `SVM3` e `SVM4` no local de recuperação. No entanto, você pode selecionar apenas um dos dois pares de matrizes ao criar um grupo de proteção.



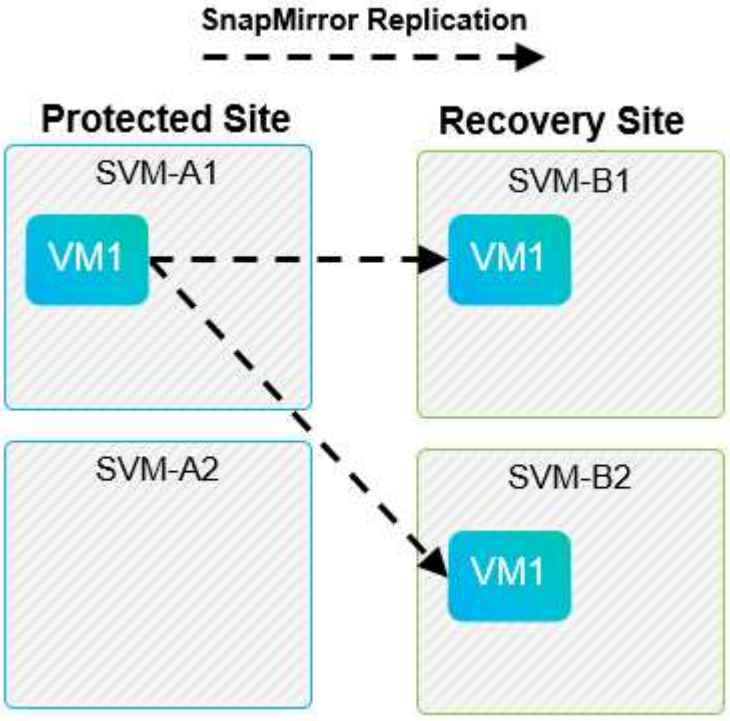
Esquemas não suportados

Configurações não suportadas têm dados (VMDK ou RDM) em vários SVMs que são de propriedade de uma VM individual. Nos exemplos mostrados nas figuras a seguir, `VM1` não pode ser configurado para proteção com VLSR `VM1` porque tem dados em dois SVMs.





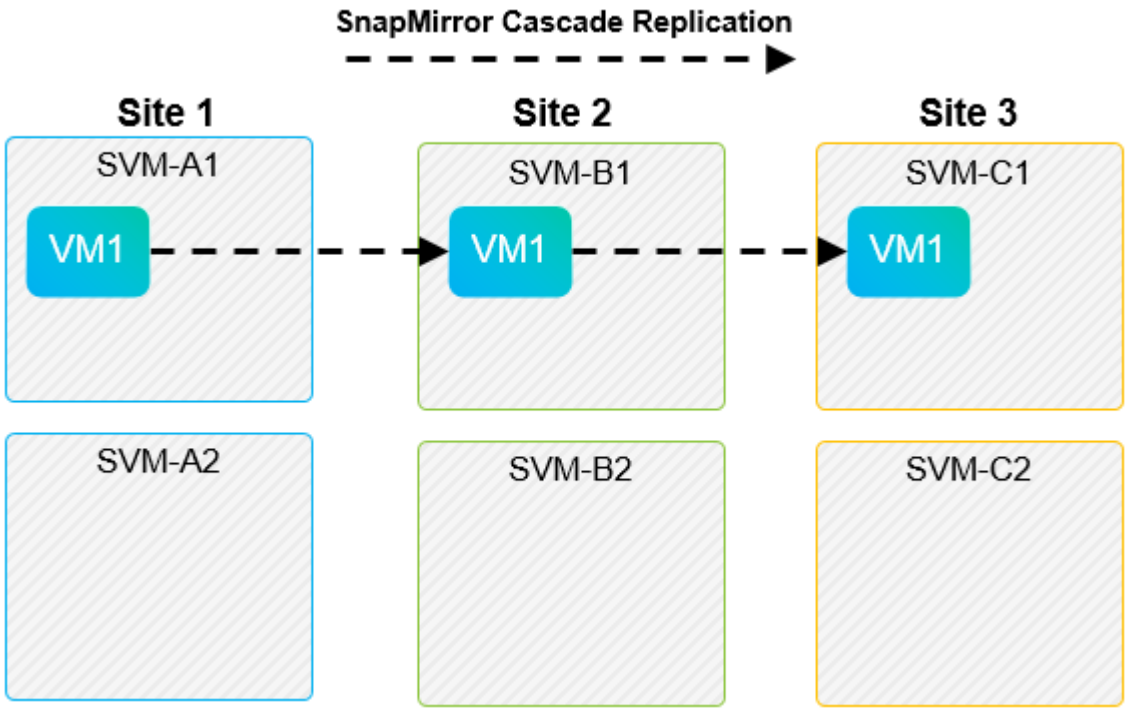
Qualquer relação de replicação na qual um volume de NetApp individual é replicado de uma SVM de origem para vários destinos no mesmo SVM ou em SVMs diferentes é chamada de fan-out do SnapMirror. Fan-out não é suportado com VLSR. No exemplo mostrado na figura a seguir, `VM1` não pode ser configurado para proteção no VLSR porque ele é replicado com o SnapMirror para dois locais diferentes.



Cascata de SnapMirror

O VLSR não oferece suporte a cascata de relacionamentos SnapMirror, nas quais um volume de origem é replicado para um volume de destino e esse volume de destino também é replicado com o SnapMirror para outro volume de destino. No cenário mostrado na figura a seguir, o VLSR não pode ser usado para failover

entre sites.



SnapMirror e SnapVault

O software NetApp SnapVault permite o backup baseado em disco de dados empresariais entre sistemas de storage NetApp. O SnapVault e o SnapMirror podem coexistir no mesmo ambiente; no entanto, o VLSR suporta o failover apenas das relações SnapMirror.

O NetApp SRA suporta o `mirror-vault` tipo de política.

SnapVault foi reconstruído a partir do zero para ONTAP 8,2. Embora antigos usuários do Data ONTAP 7-Mode devam encontrar semelhanças, grandes melhorias foram feitas nesta versão do SnapVault. Um grande avanço é a capacidade de preservar eficiências de storage de dados primários durante transferências SnapVault.

Uma mudança arquitetônica importante é que o in ONTAP 9 replica no nível de volume em vez de no nível de qtree, como é o caso do SnapVault 7-Mode SnapVault. Essa configuração significa que a origem de um relacionamento do SnapVault deve ser um volume e esse volume deve ser replicado para seu próprio volume no sistema secundário do SnapVault.

Em um ambiente em que o SnapVault é usado, os snapshots nomeados especificamente são criados no sistema de storage primário. Dependendo da configuração implementada, os instantâneos nomeados podem ser criados no sistema principal por um agendamento do SnapVault ou por um aplicativo como o NetApp Active IQ Unified Manager. Os instantâneos nomeados que são criados no sistema primário são replicados para o destino SnapMirror e, a partir daí, são abobadados para o destino SnapVault.

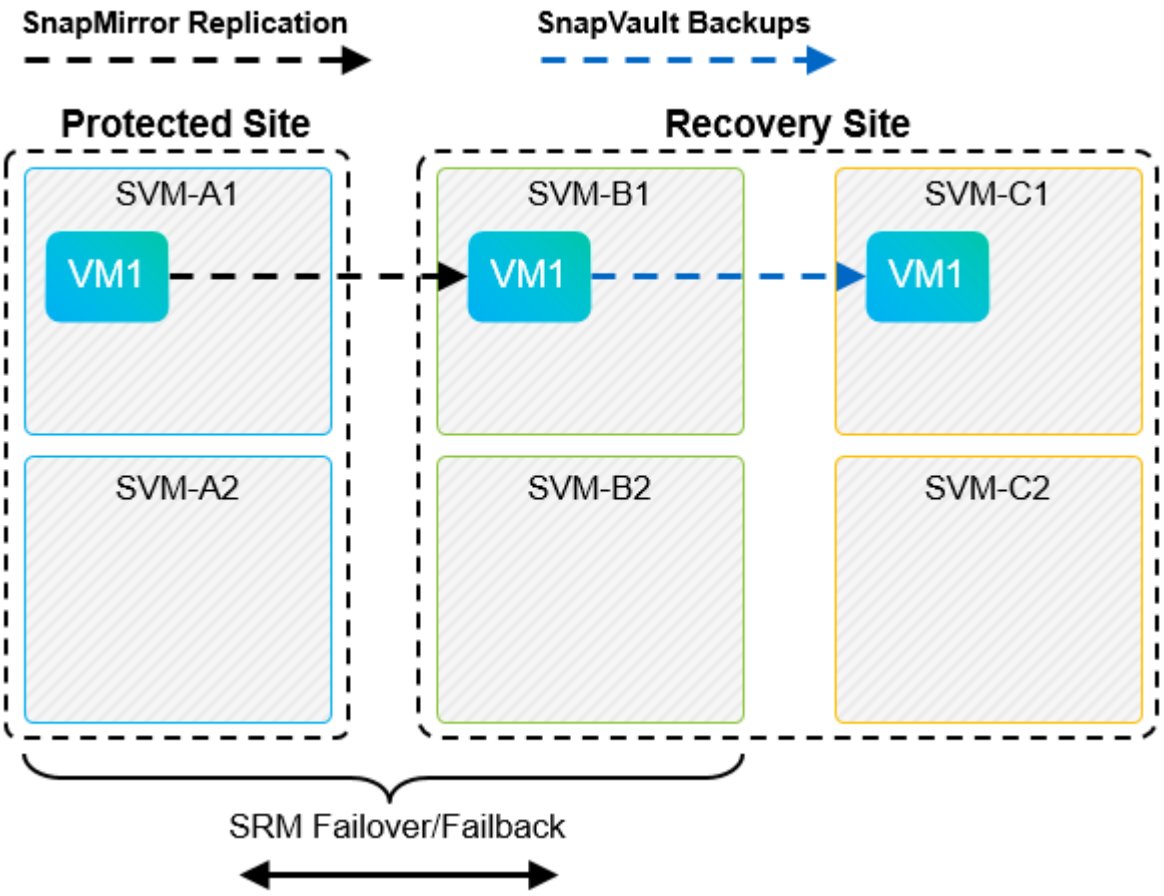
Um volume de origem pode ser criado em uma configuração em cascata na qual um volume é replicado para um destino SnapMirror no local de DR e, a partir daí, é abobadado para um destino SnapVault. Um volume de origem também pode ser criado em uma relação de fan-out em que um destino é um destino SnapMirror e o outro destino é um destino SnapVault. No entanto, o SRA não reconfigura automaticamente a relação do SnapVault para usar o volume de destino do SnapMirror como a origem do Vault quando ocorre failover ou reversão de replicação do VLSR.

Para obter as informações mais recentes sobre o SnapMirror e o SnapVault para ONTAP 9, consulte "TR-4015 Guia de práticas recomendadas de configuração do SnapMirror para ONTAP 9."

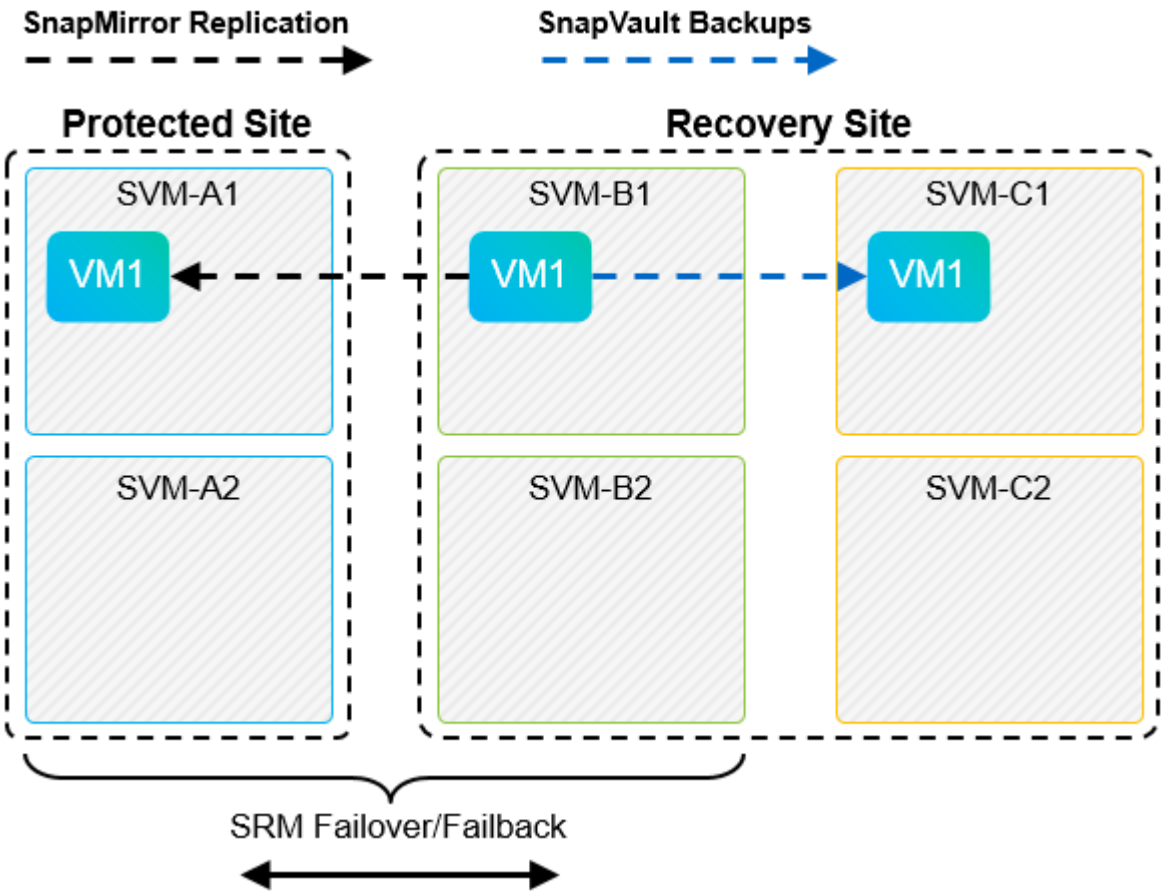
Prática recomendada
Se o SnapVault e o VLSR forem usados no mesmo ambiente, a NetApp recomenda o uso de uma configuração em cascata SnapMirror to SnapVault na qual os backups do SnapVault normalmente são executados a partir do destino do SnapMirror no local de DR. Em caso de desastre, essa configuração torna o site primário inacessível. Manter o destino do SnapVault no local de recuperação permite que os backups do SnapVault sejam reconfigurados após o failover para que os backups do SnapVault possam continuar operando no local de recuperação.

Em um ambiente VMware, cada datastore tem um identificador exclusivo universal (UUID) e cada VM tem um ID de objeto gerenciado exclusivo (MOID). Essas IDs não são mantidas pelo VLSR durante o failover ou failback. Como os UUIDs do datastore e os MOIDs de VM não são mantidos durante o failover pelo VLSR, todos os aplicativos que dependem desses IDs devem ser reconfigurados após o failover do VLSR. Um aplicativo de exemplo é o NetApp Active IQ Unified Manager, que coordena a replicação do SnapVault com o ambiente vSphere.

A figura a seguir mostra uma configuração em cascata SnapMirror to SnapVault. Se o destino do SnapVault estiver no local de DR ou em um local terciário que não seja afetado por uma interrupção no local primário, o ambiente poderá ser reconfigurado para permitir que os backups continuem após o failover.



A figura a seguir mostra a configuração depois que o VLSR foi usado para reverter a replicação do SnapMirror de volta para o local principal. O ambiente também foi reconfigurado de modo que os backups do SnapVault estão ocorrendo a partir do que é agora a fonte SnapMirror. Esta configuração é uma configuração de fan-out do SnapMirror SnapVault.



Depois que o vsrm executa o failback e uma segunda reversão das relações do SnapMirror, os dados de produção estão de volta ao local principal. Agora, esses dados estão protegidos da mesma maneira que antes do failover para o local de recuperação de desastres, por meio de backups SnapMirror e SnapVault.

Uso de Qtrees em ambientes do Site Recovery Manager

Qtrees são diretórios especiais que permitem a aplicação de cotas de sistema de arquivos para nas. O ONTAP 9 permite a criação de qtrees, e qtrees podem existir em volumes replicados com o SnapMirror. No entanto, o SnapMirror não permite replicação de qtrees individuais ou replicação em nível de qtree. Toda a replicação do SnapMirror está apenas no nível do volume. Por esta razão, o NetApp não recomenda o uso de qtrees com VLSR.

Ambientes FC e iSCSI mistos

Com os protocolos SAN compatíveis (FC, FCoE e iSCSI), o ONTAP 9 fornece serviços LUN, ou seja, a capacidade de criar e mapear LUNs para hosts conectados. Como o cluster consiste em vários controladores, há vários caminhos lógicos gerenciados pela e/S multipath em qualquer LUN individual. O acesso de unidade lógica assimétrica (ALUA) é usado nos hosts para que o caminho otimizado para um LUN seja selecionado e seja ativado para transferência de dados. Se o caminho otimizado para qualquer LUN mudar (por exemplo, porque o volume que contém é movido), o ONTAP 9 reconhece e ajusta-se automaticamente para essa alteração sem interrupções. Se o caminho otimizado ficar indisponível, o ONTAP poderá alternar para qualquer outro caminho disponível sem interrupções.

O VMware VLSR e o NetApp SRA suportam o uso do protocolo FC em um local e do protocolo iSCSI no outro local. No entanto, ele não dá suporte a uma combinação de armazenamentos de dados anexados a FC e armazenamentos de dados anexados a iSCSI no mesmo host ESXi ou em hosts diferentes no mesmo cluster. Esta configuração não é suportada com o VLSR porque, durante o failover VLSR ou failover de teste, o VLSR

inclui todos os iniciadores FC e iSCSI nos hosts ESXi na solicitação.

Prática recomendada
O VLSR e o SRA oferecem suporte a protocolos FC e iSCSI mistos entre os locais protegidos e de recuperação. No entanto, cada local deve ser configurado com apenas um protocolo, FC ou iSCSI, e não com ambos os protocolos no mesmo local. Se houver um requisito para que os protocolos FC e iSCSI sejam configurados no mesmo local, o NetApp recomenda que alguns hosts usem iSCSI e outros hosts usem FC. O NetApp também recomenda, neste caso, que os mapeamentos de recursos do VLSR sejam configurados para que as VMs sejam configuradas para failover em um grupo de hosts ou outro.

Solução de problemas do VLSRM/SRM ao usar a replicação do vVols

Ao usar as ferramentas do ONTAP 9.13P2, o fluxo de trabalho dentro do VLSR e SRM é significativamente diferente ao usar a replicação vVols do que é usado com o SRA e armazenamentos de dados tradicionais. Por exemplo, não há conceito de gerenciador de array. Como tal, `discoverarrays` e `discoverdevices` comandos nunca são vistos.

Ao solucionar problemas, é benéfico entender os novos fluxos de trabalho, listados abaixo:

1. QueryReplicationPeer: Descobre os acordos de replicação entre dois domínios de falha.
2. QueryFaultDomain: Descobre a hierarquia do domínio de falha.
3. QueryReplicationGroup: Descobre os grupos de replicação presentes nos domínios de origem ou destino.
4. SyncReplicationGroup: Sincroniza os dados entre origem e destino.
5. QueryPointInTimeReplica: Descobre as réplicas de ponto no tempo em um destino.
6. TestFailoverReplicationGroupStart: Inicia o failover de teste.
7. TestFailoverReplicationGroupStop: Termina o failover de teste.
8. PromoteReplicationGroup: Promove um grupo atualmente em teste para produção.
9. PrepareFailoverReplicationGroup: Prepara-se para uma recuperação de desastres.
10. FailoverReplicationGroup: Executa recuperação de desastres.
11. ReverseReplicateGroup: Inicia a replicação reversa.
12. QueryMatchingContainer: Localiza contentores (junto com hosts ou grupos de replicação) que podem satisfazer uma solicitação de provisionamento com uma determinada política.
13. QueryResourceMetadata: Descobre os metadados de todos os recursos do provedor VASA, a utilização de recursos pode ser retornada como uma resposta para a função queryMatchingContainer.

O erro mais comum visto ao configurar a replicação do vVols é uma falha ao descobrir as relações do SnapMirror. Isso ocorre porque os volumes e as relações SnapMirror são criadas fora do escopo das Ferramentas do ONTAP. Portanto, é uma prática recomendada sempre garantir que sua relação com o SnapMirror esteja totalmente inicializada e que você tenha executado uma redescoberta nas Ferramentas do ONTAP em ambos os sites antes de tentar criar um armazenamento de dados vVols replicado.

Informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e/ou sites:

- Ferramentas do ONTAP para recursos do VMware vSphere 10.x. "https://mysupport.netapp.com/site/products/all/details/otv10/docs-tab"
- Ferramentas do ONTAP para recursos do VMware vSphere 9.x. "https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab"
- TR-4597: VMware vSphere for ONTAP "https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vsphere-overview.html"
- TR-4400: VMware vSphere Virtual volumes com ONTAP "https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vvols-overview.html"
- TR-4015 Guia de Melhores Práticas de Configuração do SnapMirror para ONTAP 9 https://www.netapp.com/pdf.html?item=/media/17229-tr-4015-snapmirror-configuration-ontap.pdf
- Documentação do VMware Live Site Recovery "https://techdocs.broadcom.com/us/en/vmware-cis/live-recovery/live-site-recovery/9-0.html"

Consulte o "Ferramenta de Matriz de interoperabilidade (IMT)"no site de suporte da NetApp para validar se as versões exatas de produtos e recursos descritas neste documento são compatíveis com o seu ambiente específico. O NetApp IMT define os componentes e versões do produto que podem ser usados para construir configurações compatíveis com o NetApp. Os resultados específicos dependem da instalação de cada cliente de acordo com as especificações publicadas.

Cluster de armazenamento do vSphere Metro com o ONTAP

Cluster de armazenamento do vSphere Metro com o ONTAP

O hypervisor vSphere líder do setor da VMware pode ser implantado como um cluster estendido chamado vSphere Metro Storage Cluster (vMSC).

As soluções vmsc são suportadas com o NetApp MetroCluster e o SnapMirror ative Sync (anteriormente conhecido como SnapMirror Business Continuity, ou SMBC) e fornecem continuidade de negócios avançada se um ou mais domínios de falha sofrerem uma interrupção total. A resiliência a diferentes modos de falha depende de quais opções de configuração você escolher.

Esta documentação substitui relatórios técnicos publicados anteriormente *TR-4128: VSphere no NetApp MetroCluster*

Soluções de disponibilidade contínua para ambientes vSphere

A arquitetura ONTAP é uma plataforma de armazenamento flexível e escalável que fornece serviços SAN (FCP, iSCSI e NVMe-oF) e NAS (NFS v3 e v4.1) para armazenamentos de dados. Os sistemas de armazenamento NetApp AFF, ASA e FAS usam o sistema operacional ONTAP para oferecer protocolos adicionais para acesso de armazenamento de convidados, como S3 e SMB/CIFS.

A NetApp MetroCluster usa a função de HA (failover de controladora ou CFO) da NetApp para proteger contra falhas de controladora. Ele também inclui tecnologia SyncMirror local, failover de cluster em desastre (failover de cluster em desastre ou CFOD), redundância de hardware e separação geográfica para alcançar altos níveis de disponibilidade. O SyncMirror espelha de forma síncrona os dados entre as duas metades da configuração do MetroCluster gravando dados em dois plexos: O Plex local (na gaveta local) fornecendo dados ativamente e o Plex remoto (na gaveta remota) normalmente não fornecendo dados. A redundância de hardware é implementada para todos os componentes MetroCluster, como controladores, armazenamento, cabos, switches (usados com Fabric MetroCluster) e adaptadores.

A sincronização ativa do NetApp SnapMirror, disponível em sistemas que não sejam MetroCluster e em sistemas ASA R2, oferece proteção granular do armazenamento de dados com protocolos FCP e SAN iSCSI. Ele permite que você proteja todo o vMSC ou proteja seletivamente cargas de trabalho de alta prioridade. Ele oferece acesso ativo-ativo a locais locais e remotos, ao contrário do NetApp MetroCluster, que é uma solução de espera ativa. A partir do ONTAP 9.15.1, o SnapMirror active Sync oferece suporte a uma funcionalidade ativo-ativo simétrica, permitindo operações de e/S de leitura e gravação de ambas as cópias de um LUN protegido com replicação síncrona bidirecional, permitindo que ambas as cópias do LUN atendam às operações de e/S localmente. Antes do ONTAP 9.15.1, a sincronização ativa do SnapMirror suporta apenas configurações ativas/ativas assimétricas, nas quais os dados no local secundário são proxy para a cópia primária de um LUN.

Para criar um cluster VMware HA/DRS em dois locais, os hosts ESXi são usados e gerenciados por um vCenter Server Appliance (VCSA). As redes de gerenciamento vSphere, vMotion e máquinas virtuais são conetadas por meio de uma rede redundante entre os dois sites. O vCenter Server que gerencia o cluster HA/DRS pode se conetar aos hosts ESXi em ambos os sites e deve ser configurado usando o vCenter HA.

```
https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-vcenter-esxi-
management/GUID-F7818000-26E3-4E2A-93D2-FCDCE7114508.html["Como criar e
configurar clusters no vSphere Client"]Consulte para configurar o vCenter
HA.
```

Você também deve se referir "Práticas recomendadas do VMware vSphere Metro Storage Cluster" a .

O que é o vSphere Metro Storage Cluster?

O vSphere Metro Storage Cluster (vMSC) é uma configuração certificada que protege máquinas virtuais (VMs) e contêineres contra falhas. Isso é obtido usando conceitos de armazenamento estendido junto com clusters de hosts ESXi, que são distribuídos em diferentes domínios de falha, como racks, edifícios, campi ou até mesmo cidades. As tecnologias de armazenamento de sincronização ativa NetApp MetroCluster e SnapMirror são usadas para fornecer uma proteção de objetivo de ponto de recuperação zero (RPO=0) aos clusters de host. A configuração do vMSC foi projetada para garantir que os dados estejam sempre disponíveis, mesmo se um "site" físico ou lógico completo falhar. Um dispositivo de armazenamento que faz parte da configuração do vMSC deve ser certificado após passar por um processo de certificação do vMSC bem-sucedido. Todos os dispositivos de armazenamento suportados podem ser encontrados no "Guia de compatibilidade do VMware Storage".

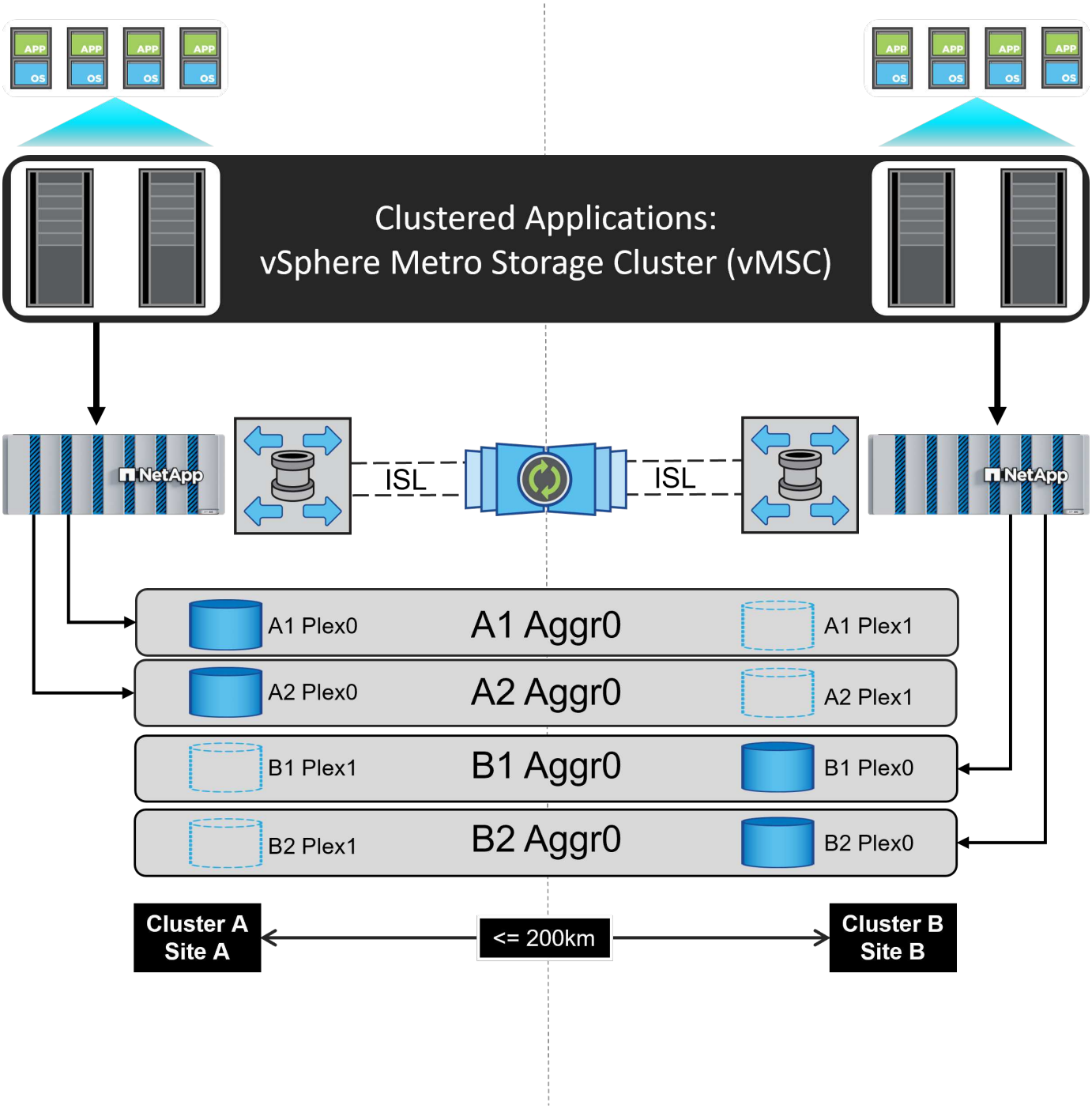
Se você quiser obter mais informações sobre as diretrizes de design do vSphere Metro Storage Cluster, consulte a seguinte documentação:

- "Suporte ao VMware vSphere com o NetApp MetroCluster"
- "Suporte ao VMware vSphere com o NetApp SnapMirror Business Continuity" (Agora conhecido como SnapMirror ative Sync)

O NetApp MetroCluster pode ser implantado em duas configurações diferentes para uso com o vSphere:

- Stretch MetroCluster
- Fabric MetroCluster

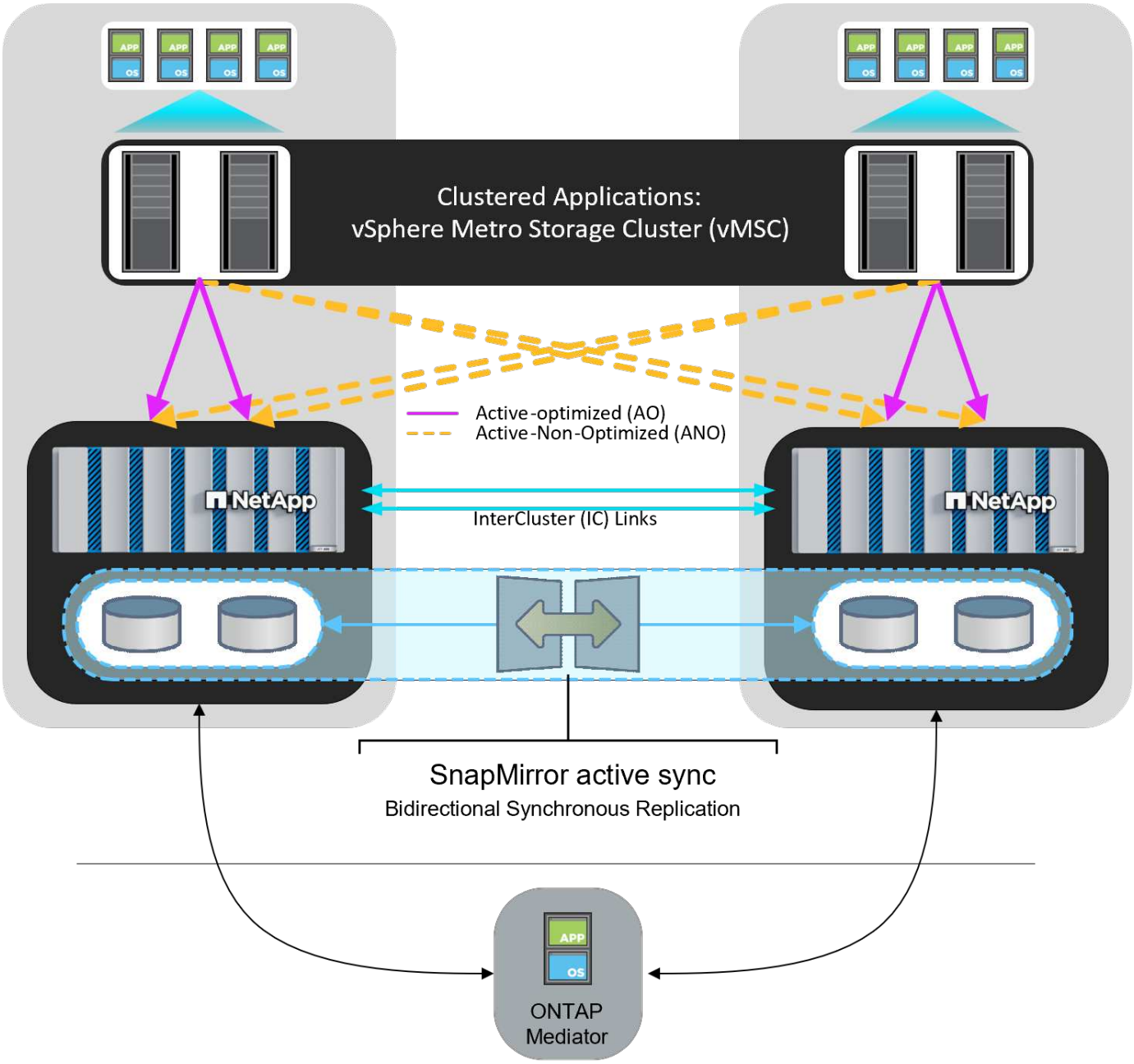
A seguir ilustra um diagrama de topologia de alto nível do Stretch MetroCluster.




```
https://www.netapp.com/support-and-
training/documentation/metrocluster/["Documentação do
MetroCluster"]Consulte para obter informações específicas sobre design e
implantação do MetroCluster.
```

O SnapMirror ative Sync também pode ser implantado de duas maneiras diferentes.

- Assimétrico
- Sincronização ativa simétrica (ONTAP 9.15.1)




```
https://docs.netapp.com/us-en/ontap/smbc/index.html["Documentos do
NetApp"]Consulte para obter informações específicas sobre design e
implementação para sincronização ativa do SnapMirror.
```

Visão geral da solução VMware vSphere

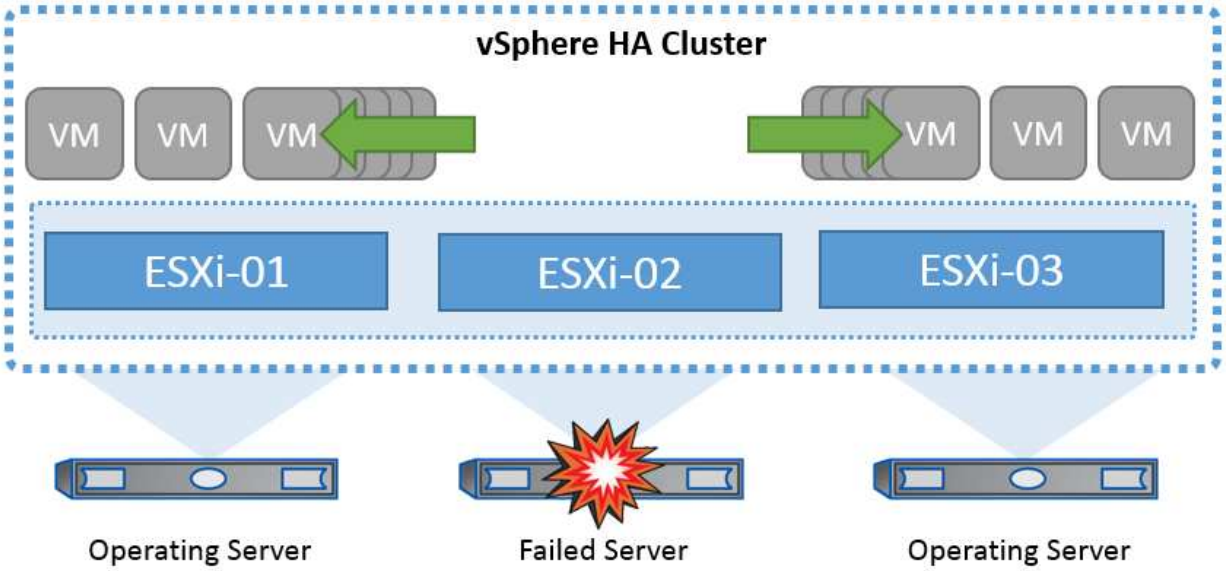
O vCenter Server Appliance (VCSA) é um poderoso sistema de gerenciamento centralizado e um painel de controle único para o vSphere que permite aos administradores operar clusters ESXi de forma eficaz. Ele facilita funções essenciais como provisionamento de máquinas virtuais, operação vMotion, alta disponibilidade (HA), Distributed Resource Scheduler (DRS), VMware vSphere Kubernetes Service (VKS) e muito mais. É um componente essencial em ambientes de nuvem VMware e

deve ser projetado levando em consideração a disponibilidade do serviço.

Alta disponibilidade do vSphere

A tecnologia de cluster da VMware agrupa os servidores ESXi em pools de recursos compartilhados para máquinas virtuais e fornece o vSphere High Availability (HA). O vSphere HA oferece alta disponibilidade e fácil de usar para aplicativos executados em máquinas virtuais. Quando o recurso HA está ativado no cluster, cada servidor ESXi mantém a comunicação com outros hosts para que, se qualquer host ESXi ficar sem resposta ou isolado, o cluster HA possa negociar a recuperação das máquinas virtuais que estavam sendo executadas nesse host ESXi entre os hosts sobreviventes no cluster. No caso de uma falha do sistema operacional convidado, o vSphere HA pode reiniciar a máquina virtual afetada no mesmo servidor físico. O vSphere HA possibilita reduzir o tempo de inatividade planejado, evitar tempo de inatividade não planejado e recuperar rapidamente de interrupções.

Cluster vSphere HA recuperando VMs de um servidor com falha.



É importante entender que o VMware vSphere não tem conhecimento da sincronização ativa do NetApp MetroCluster ou do SnapMirror e vê todos os hosts ESXi no cluster vSphere como hosts qualificados para operações de cluster de HA, dependendo das configurações de afinidade de host e grupo de VM.

Detecção de falha do host

Assim que o cluster HA é criado, todos os hosts do cluster participam da eleição, e um dos hosts se torna o mestre. Cada servidor escravo envia um sinal de pulsação à rede para o servidor mestre, e o servidor mestre, por sua vez, envia um sinal de pulsação a todos os servidores escravos. O host mestre de um cluster vSphere HA é responsável por detectar a falha dos hosts escravos.

Dependendo do tipo de falha detetada, as máquinas virtuais que estão sendo executadas nos hosts podem precisar ser reexecutadas.

Em um cluster do vSphere HA, três tipos de falha de host são detetados:

- Falha - Um host pára de funcionar.
- Isolamento - Um host se torna isolado na rede.
- Partição - Um host perde a conetividade de rede com o host mestre.

O host principal monitora os hosts escravos no cluster. Esta comunicação é feita através da troca de batimentos cardíacos de rede a cada segundo. Quando o host mestre deixa de receber esses batimentos cardíacos de um host escravo, ele verifica a presença de host antes de declarar que o host falhou. A verificação de vivacidade que o host mestre executa é determinar se o host escravo está trocando heartbeats com um dos datastores. Além disso, o host principal verifica se o host responde aos pings ICMP enviados para seus endereços IP de gerenciamento para detetar se ele é meramente isolado de seu nó mestre ou completamente isolado da rede. Ele faz isso fazendo ping no gateway padrão. Um ou mais endereços de isolamento podem ser especificados manualmente para melhorar a confiabilidade da validação de isolamento.

A NetApp recomenda especificar um mínimo de dois endereços de isolamento adicionais e que cada um desses endereços seja local. Isso aumentará a confiabilidade da validação de isolamento.

Resposta de isolamento do host

A Resposta de Isolamento é uma configuração no vSphere HA que determina a ação acionada nas máquinas virtuais quando um host em um cluster vSphere HA perde suas conexões de rede de gerenciamento, mas continua em execução. Existem três opções para esta configuração: "Desativado", "Desligar e reiniciar VMs" e "Desligar e reiniciar VMs".

"Desligar" é melhor do que "Desligar completamente", que não salva as alterações mais recentes no disco nem confirma as transações. Se as máquinas virtuais não forem desligadas em 300 segundos, elas serão desativadas. Para alterar o tempo de espera, use a opção avançada das.isolationshutdowntimeout.

Antes que o HA inicie a resposta de isolamento, ele primeiro verifica se o agente mestre do vSphere HA possui o datastore que contém os arquivos de configuração da VM. Caso contrário, o host não acionará a resposta de isolamento, porque não há mestre para reiniciar as VMs. O host verificará periodicamente o estado do datastore para determinar se ele é reivindicado por um agente do vSphere HA que detém a função mestre.

A NetApp recomenda definir a "resposta de isolamento do host" como Desativado.

Uma condição de split-brain pode ocorrer se um host ficar isolado ou particionado do host master do vSphere HA e o mestre não conseguir se comunicar por meio de datastores de heartbeat ou por ping. O mestre declara o host isolado morto e reinicia as VMs em outros hosts no cluster. Uma condição de split-brain agora existe porque existem duas instâncias da máquina virtual em execução, apenas uma das quais pode ler ou gravar os discos virtuais. As condições de split-brain agora podem ser evitadas configurando a VM Component Protection (VMCP).

Proteção de componentes VM (VMCP)

Um dos aprimoramentos de recursos do vSphere 6, relevantes para o HA, é o VMCP. O VMCP fornece proteção aprimorada contra todas as condições de APD (caminhos para baixo) e PDL (perda permanente de dispositivo) para bloco (FC, iSCSI, FCoE) e armazenamento de arquivos (NFS).

Perda permanente de dispositivo (PDL)

PDL é uma condição que ocorre quando um dispositivo de armazenamento falha permanentemente ou é removido administrativamente e não se espera que retorne. O array de armazenamento NetApp emite um código SCSI Sense para o ESXi, declarando que o dispositivo foi perdido permanentemente. Na seção Condições de Falha e Resposta da VM do vSphere HA, você pode configurar qual deve ser a resposta após a detecção de uma condição PDL.

A NetApp recomenda definir a "Resposta para armazenamento de dados com PDL" como "**Desligar e reiniciar as VMs**". Quando essa condição for detectada, uma máquina virtual será reiniciada instantaneamente em um host íntegro dentro do cluster vSphere HA.

Todos os caminhos para baixo (APD)

APD é uma condição que ocorre quando um dispositivo de armazenamento se torna inacessível ao host e não há caminhos disponíveis para o array. O ESXi considera este um problema temporário com o dispositivo e espera que ele volte a estar disponível em breve.

Quando uma condição APD é detetada, um temporizador é iniciado. Após 140 segundos, a condição APD é oficialmente declarada e o dispositivo é marcado como APD time out. Quando os 140 segundos tiverem passado, o HA começará a contar o número de minutos especificado no atraso para o APD de failover da VM. Quando o tempo especificado tiver passado, o HA reiniciará as máquinas virtuais afetadas. Você pode configurar o VMCP para responder de forma diferente, se desejado (Desativado, Eventos de problemas ou Desligar e reiniciar VMs).

- O NetApp recomenda configurar a "resposta para datastore com APD" para "**Desligar e reiniciar VMs (conservative)**".
- O termo "conservador" refere-se à probabilidade de o HA (alta disponibilidade) conseguir reiniciar as VMs (máquinas virtuais). Quando configurado para o modo Conservador, o HA reiniciará a VM afetada pelo APD somente se souber que outro host pode reiniciá-la. No caso do modo Agressivo, o HA tentará reiniciar a VM mesmo que não conheça o estado dos outros hosts. Isso pode resultar na não reinicialização das VMs caso não haja um host com acesso ao armazenamento de dados onde elas estão localizadas.
- Se o status do APD for resolvido e o acesso ao armazenamento for restaurado antes que o tempo limite tenha passado, o HA não reiniciará desnecessariamente a máquina virtual, a menos que você a configure explicitamente para fazê-lo. Se uma resposta for desejada, mesmo quando o ambiente foi recuperado da condição APD, então Response for APD Recovery After APD Timeout deve ser configurado para Reset VMs.
- O NetApp recomenda configurar a resposta para recuperação do APD após o tempo limite do APD para Desativado.

Implementação do VMware DRS para o NetApp SnapMirror ative Sync

O VMware DRS é um recurso que agrega os recursos de host em um cluster e é usado principalmente para o balanceamento de carga em um cluster em uma infraestrutura virtual. O VMware DRS calcula principalmente os recursos de CPU e memória para realizar o balanceamento de carga em um cluster. Como o vSphere não tem conhecimento do clustering estendido, ele considera todos os hosts em ambos os locais quando o balanceamento de carga.

Implementação do VMware DRS para NetApp MetroCluster

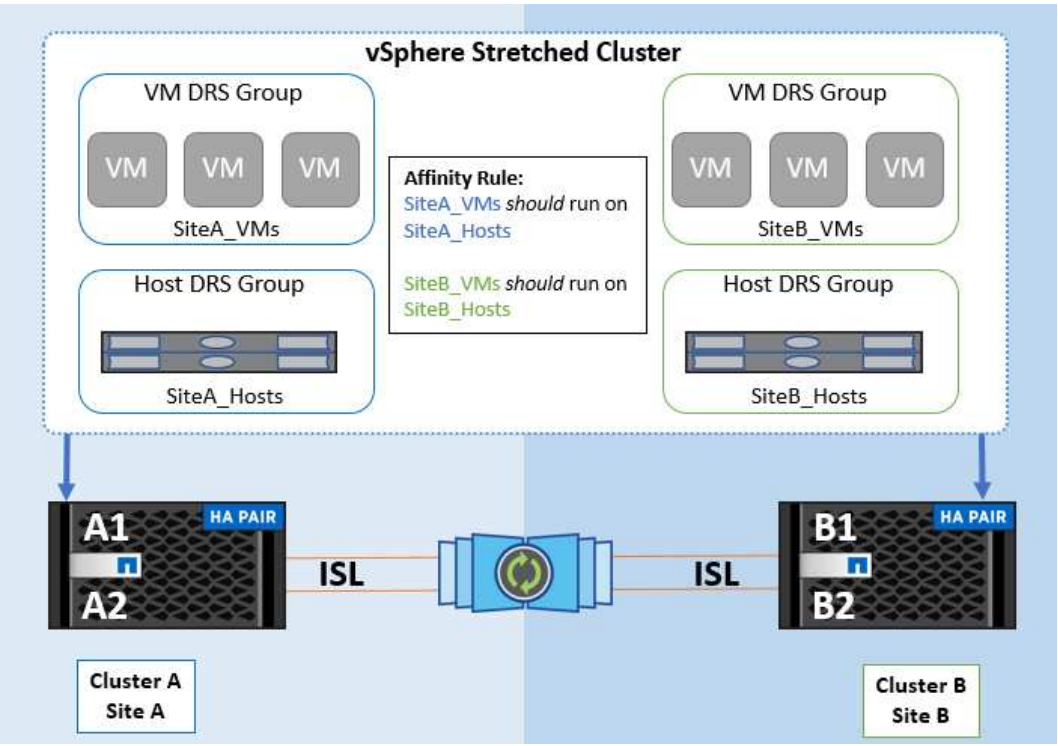
```
 To avoid cross-site traffic, NetApp recommends configuring DRS affinity
rules to manage a logical separation of VMs. This will ensure that, unless
there is a complete site failure, HA and DRS will only use local hosts.
Se você criar uma regra de afinidade DRS para o cluster, poderá
especificar como o vSphere aplica essa regra durante um failover de
máquina virtual.
```

Existem dois tipos de regras que você pode especificar para o comportamento de failover do vSphere HA:

- As regras de anti-afinidade da VM forçam as máquinas virtuais especificadas a permanecerem separadas durante as ações de failover.
- As regras de afinidade de host da VM colocam máquinas virtuais especificadas em um host específico ou em um membro de um grupo definido de hosts durante ações de failover.

Usando regras de afinidade de host de VM no VMware DRS, pode-se ter uma separação lógica entre o local A e o local B para que a VM seja executada no host no mesmo local do array configurado como o controlador de leitura/gravação primário para um determinado datastore. Além disso, as regras de afinidade de host da VM permitem que as máquinas virtuais permaneçam locais para o armazenamento, o que, por sua vez, verifica a conexão da máquina virtual em caso de falhas de rede entre os sites.

A seguir está um exemplo de grupos de hosts de VM e regras de afinidade.



Melhor prática

A NetApp recomenda a implementação de regras "devem" em vez de regras "obrigatórias" porque elas são violadas pelo vSphere HA em caso de falha. O uso de regras "obrigatórias" pode potencialmente levar a interrupções de serviço.

A disponibilidade dos serviços deve sempre prevalecer sobre o desempenho. No cenário em que um data center inteiro falha, as regras "obrigatórias" devem escolher hosts do grupo de afinidade de hosts de VMs e, quando o data center estiver indisponível, as máquinas virtuais não serão reiniciadas.

Implementação do VMware Storage DRS com o NetApp MetroCluster

O recurso VMware Storage DRS permite a agregação de armazenamentos de dados em uma única unidade e equilibra discos de máquina virtual quando os limites de controle de e/S de armazenamento (SIOC) são excedidos.

O controle de e/S de armazenamento é habilitado por padrão nos clusters DRS habilitados para Storage DRS.

O controle de e/S de armazenamento permite que um administrador controle a quantidade de e/S de armazenamento que é alocada a máquinas virtuais durante períodos de congestionamento de e/S, o que permite que máquinas virtuais mais importantes tenham preferência sobre máquinas virtuais menos importantes para alocação de recursos de e/S.

O Storage DRS usa o Storage vMotion para migrar as máquinas virtuais para diferentes datastores dentro de um cluster de datastore. Em um ambiente NetApp MetroCluster, a migração de uma máquina virtual precisa ser controlada nos datastores desse site. Por exemplo, a máquina virtual A, em execução em um host no local A, deve idealmente migrar dentro dos armazenamentos de dados do SVM no local A. se não o fizer, a máquina virtual continuará operando, mas com desempenho degradado, uma vez que a leitura/gravação do disco virtual será do local B através de links entre sites.

*Ao usar o armazenamento ONTAP, é recomendável desativar o DRS de armazenamento.

- O DRS de armazenamento geralmente não é necessário ou recomendado para uso com sistemas de armazenamento ONTAP.
- O ONTAP oferece seus próprios recursos de eficiência de storage, como deduplicação, compressão e compactação, que podem ser afetados pelo Storage DRS.
- Se você estiver usando snapshots do ONTAP , o Storage vMotion deixará para trás a cópia da VM presente no snapshot, o que pode aumentar a utilização do armazenamento e afetar aplicativos de backup como o NetApp SnapCenter, que rastreiam VMs e seus snapshots do ONTAP .

Diretrizes de projeto e implementação do vMSC

Este documento descreve as diretrizes de design e implementação do vMSC com sistemas de storage ONTAP.

Configuração de armazenamento NetApp

As instruções de configuração do NetApp MetroCluster estão disponíveis em "Documentação do MetroCluster". As instruções para a sincronização ativa do SnapMirror (SMA) também estão disponíveis em "Visão geral da continuidade dos negócios da SnapMirror".

Depois de configurar o MetroCluster, administrá-lo é como gerenciar um ambiente ONTAP tradicional. É possível configurar máquinas virtuais de storage (SVMs) usando várias ferramentas, como a interface de linha de comando (CLI), o System Manager ou o Ansible. Uma vez configurados os SVMs, crie interfaces lógicas (LIFs), volumes e números de unidades lógicas (LUNs) no cluster que será usado para operações normais. Esses objetos serão replicados automaticamente para o outro cluster usando a rede de peering de cluster.

Se não estiver usando o MetroCluster ou se você tiver sistemas ONTAP que não sejam compatíveis com o MetroCluster, como sistemas ASA R2, poderá usar o SnapMirror active Sync, que fornece proteção granular do armazenamento de dados e acesso ativo-ativo em vários clusters ONTAP em diferentes domínios de falha. O SMA usa grupos de consistência (CGS) para garantir a consistência da ordem de gravação entre um ou mais datastores e você pode criar vários CGS dependendo dos requisitos do aplicativo e do datastore. Os grupos de consistência são especialmente úteis para aplicativos que exigem sincronização de dados entre vários datastores. Por exemplo, LVMs convidadas distribuídas entre datastores. O SMA também suporta RDMs (Mapeamentos de dispositivo brutos) e armazenamento conetado a convidados com iniciadores iSCSI in-Guest. Você pode aprender mais sobre grupos de consistência em "Visão geral dos grupos de consistência".

Há alguma diferença no gerenciamento de uma configuração vmsc com a sincronização ativa do SnapMirror quando comparada a um MetroCluster. Primeiro, SMA é uma configuração somente SAN, nenhum datastores

NFS pode ser protegido com a sincronização ativa do SnapMirror. Em segundo lugar, você deve mapear ambas as cópias dos LUNs para os hosts ESXi para que eles acessem os datastores replicados em ambos os domínios de falha. Terceiro, você deve criar um ou mais grupos de consistência para os datastores que deseja proteger com a sincronização ativa do SnapMirror. Finalmente, você deve criar uma política do SnapMirror para os grupos de consistência criados. Tudo isso pode ser feito facilmente usando o assistente "proteger cluster" no plug-in do vCenter Tools do ONTAP, ou usando manualmente a CLI do ONTAP ou o Gerenciador do sistema.

Usando o plug-in do vCenter Tools do ONTAP para o SnapMirror ative Sync

O plug-in do ONTAP Tools vCenter oferece uma maneira simples e intuitiva de configurar a sincronização ativa do SnapMirror para vmsc. Você pode usar o plug-in do vCenter Tools do ONTAP para criar e gerenciar relações de sincronização ativa do SnapMirror entre dois clusters do ONTAP. Este plugin fornece uma interface fácil de usar para estabelecer e gerenciar esses relacionamentos de forma eficiente. Você pode saber mais sobre o plugin do vCenter Tools do ONTAP em "Ferramentas do ONTAP para VMware vSphere", ou ir direto para "Proteger usando a proteção do cluster de host"o .

Configuração do VMware vSphere

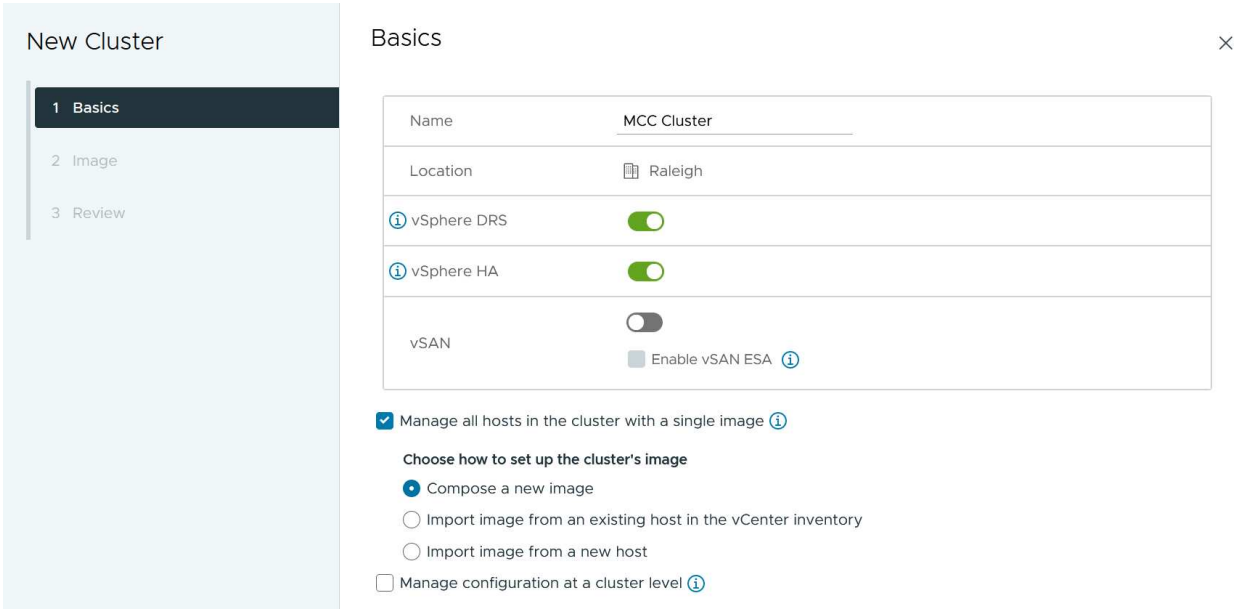
Crie um cluster do vSphere HA

A criação de um cluster do vSphere HA é um processo de várias etapas totalmente documentado em "Como criar e configurar clusters no vSphere Client em docs.vmware.com". Em suma, primeiro você deve criar um cluster vazio e, usando o vCenter, você deve adicionar hosts e especificar o vSphere HA e outras configurações do cluster.

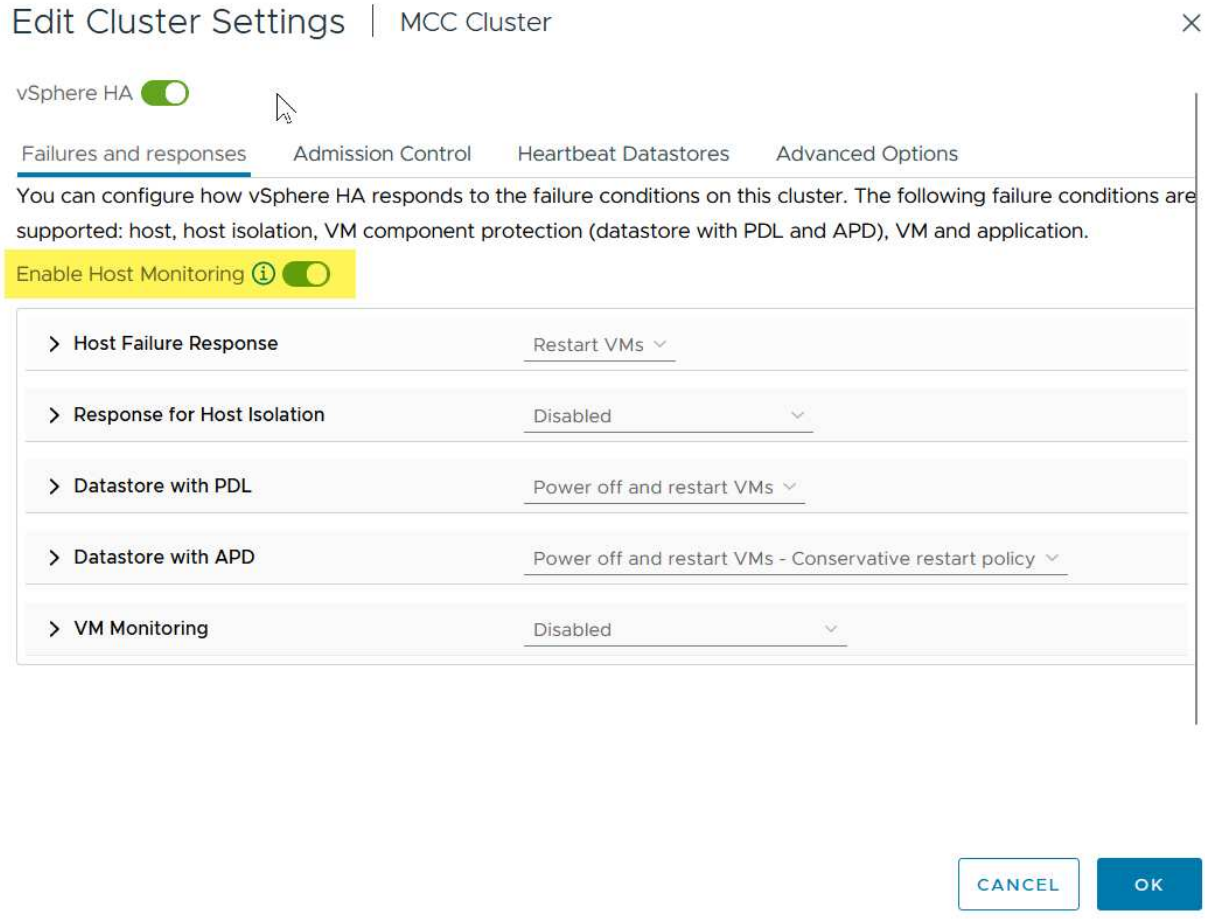
> Nada neste documento substitui "Práticas recomendadas do VMware vSphere Metro Storage Cluster". Este conteúdo é fornecido para fácil referência e não substitui a documentação oficial da VMware.

Para configurar um cluster de HA, execute as seguintes etapas:

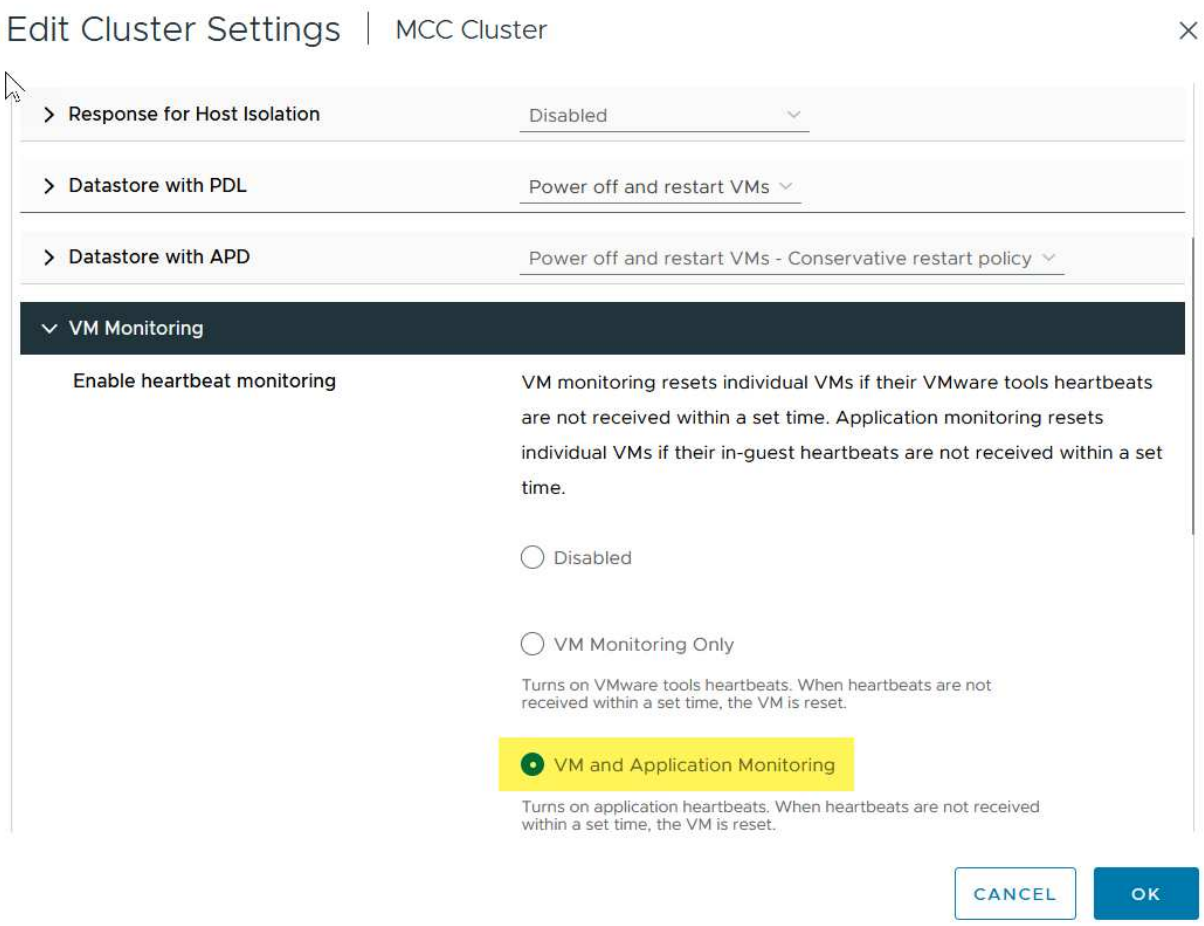
1. Conete-se à IU do vCenter.
2. Em hosts e clusters, navegue até o data center onde você deseja criar seu cluster de HA.
3. Clique com o botão direito do rato no objeto do data center e selecione novo cluster. Em noções básicas, certifique-se de que você ativou o vSphere DRS e o vSphere HA. Conclua o assistente.



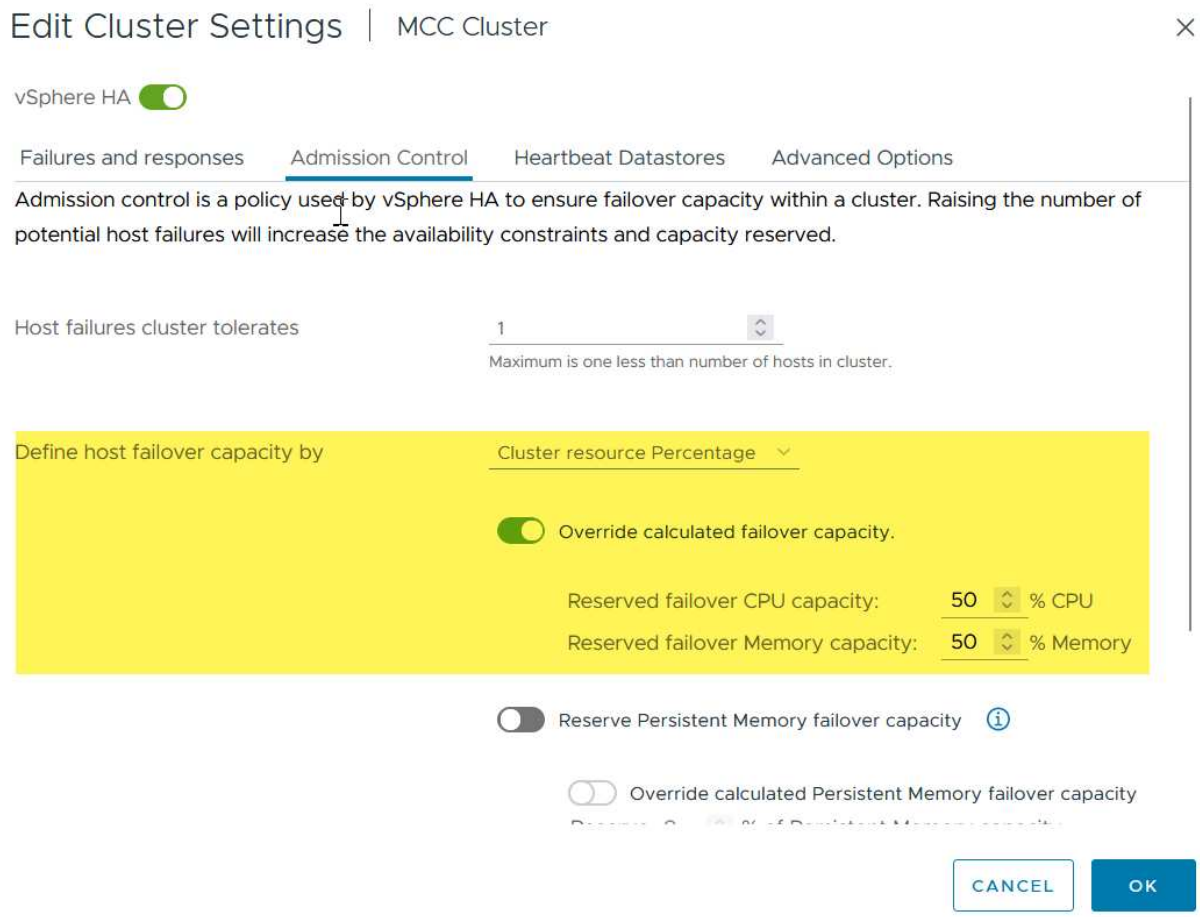
1. Selecione o cluster e vá para a guia configurar. Selecione vSphere HA e clique em Edit.
2. Em Monitoramento de host, selecione a opção Ativar monitoramento de host.



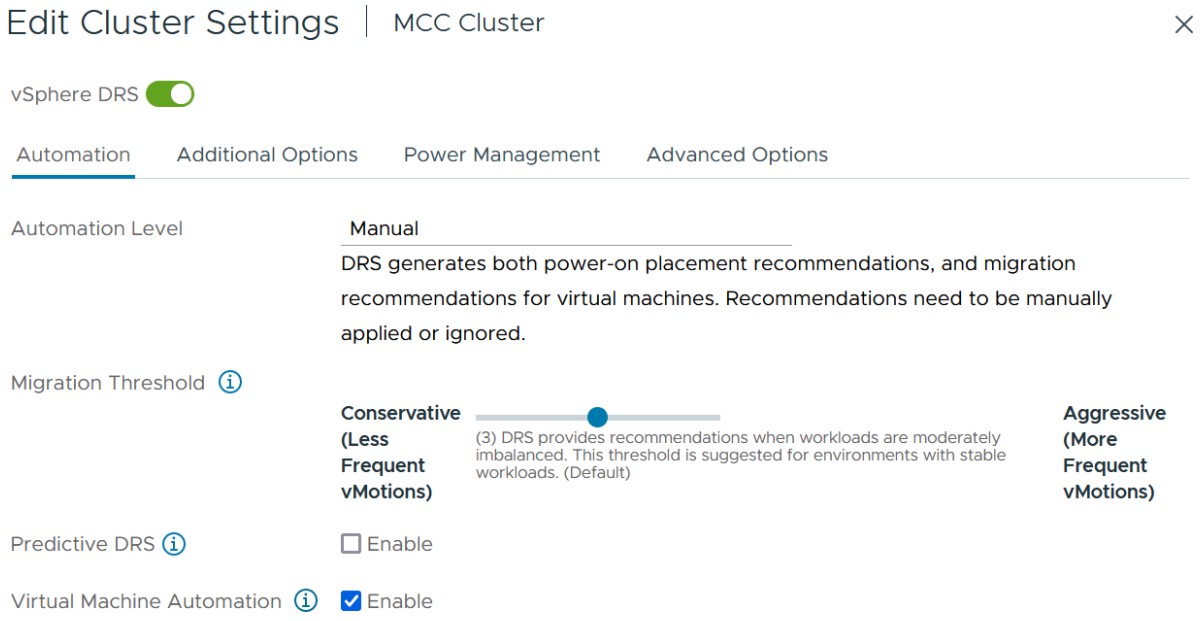
1. Enquanto ainda estiver na guia falhas e respostas, em Monitoramento de VM, selecione a opção somente Monitoramento de VM ou a opção Monitoramento de VM e aplicativo.



1. Em Controle de admissão, defina a opção de controle de admissão HA para reserva de recursos de cluster; use 50% CPU/MEM.



1. Clique em "OK".
2. Selecione DRS e clique EM editar.
3. Defina o nível de automação para manual, a menos que seja necessário pelas suas aplicações.



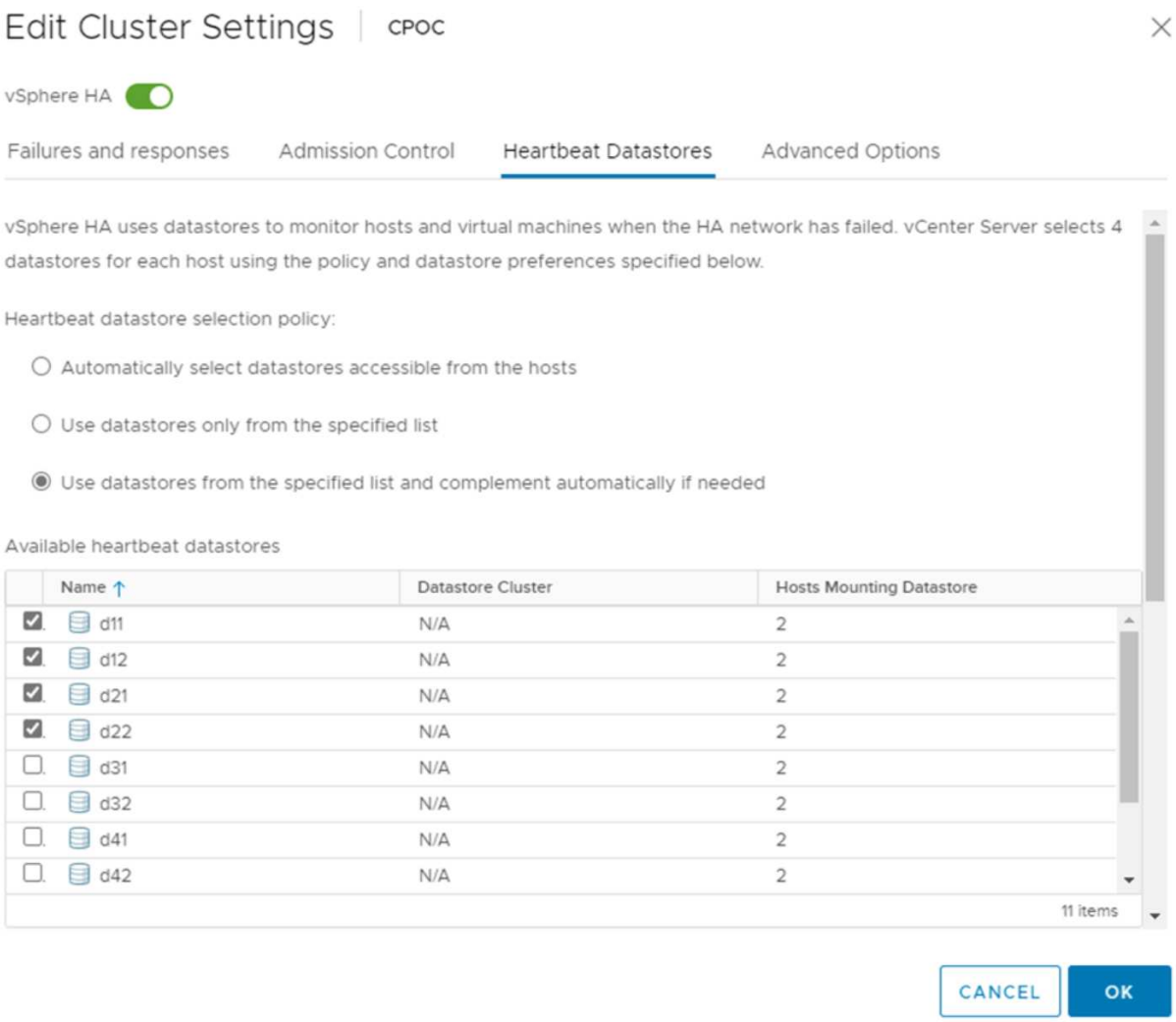
1. Ativar a proteção de componentes VM, "docs.vmware.com" consulte a .
2. As seguintes configurações adicionais do vSphere HA são recomendadas para vMSC com MetroCluster:

Falha	Resposta
Falha do host	Reinicie as VMs
Isolamento de host	Desativado
Armazenamento de dados com perda permanente de dispositivo (PDL)	Desligue e reinicie as VMs
Datastore com todos os caminhos para baixo (APD)	Desligue e reinicie as VMs
Hóspede não é coração batendo	Repor as VMs
Política de reinicialização da VM	Determinado pela importância da VM
Resposta para isolamento do host	Encerre e reinicie as VMs
Resposta para datastore com PDL	Desligue e reinicie as VMs
Resposta para datastore com APD	Desligar e reiniciar as VMs (conservadoras)
Atraso para failover de VM para APD	3 minutos
Resposta para recuperação APD com tempo limite APD	Desativado
Sensibilidade de monitoramento da VM	Predefinição alta

Configurar datastores para Heartbearing

O vSphere HA usa datastores para monitorar hosts e máquinas virtuais quando a rede de gerenciamento falhou. Você pode configurar como o vCenter seleciona armazenamentos de dados Heartbeat. Para configurar armazenamentos de dados para batimentos cardíacos, execute as seguintes etapas:

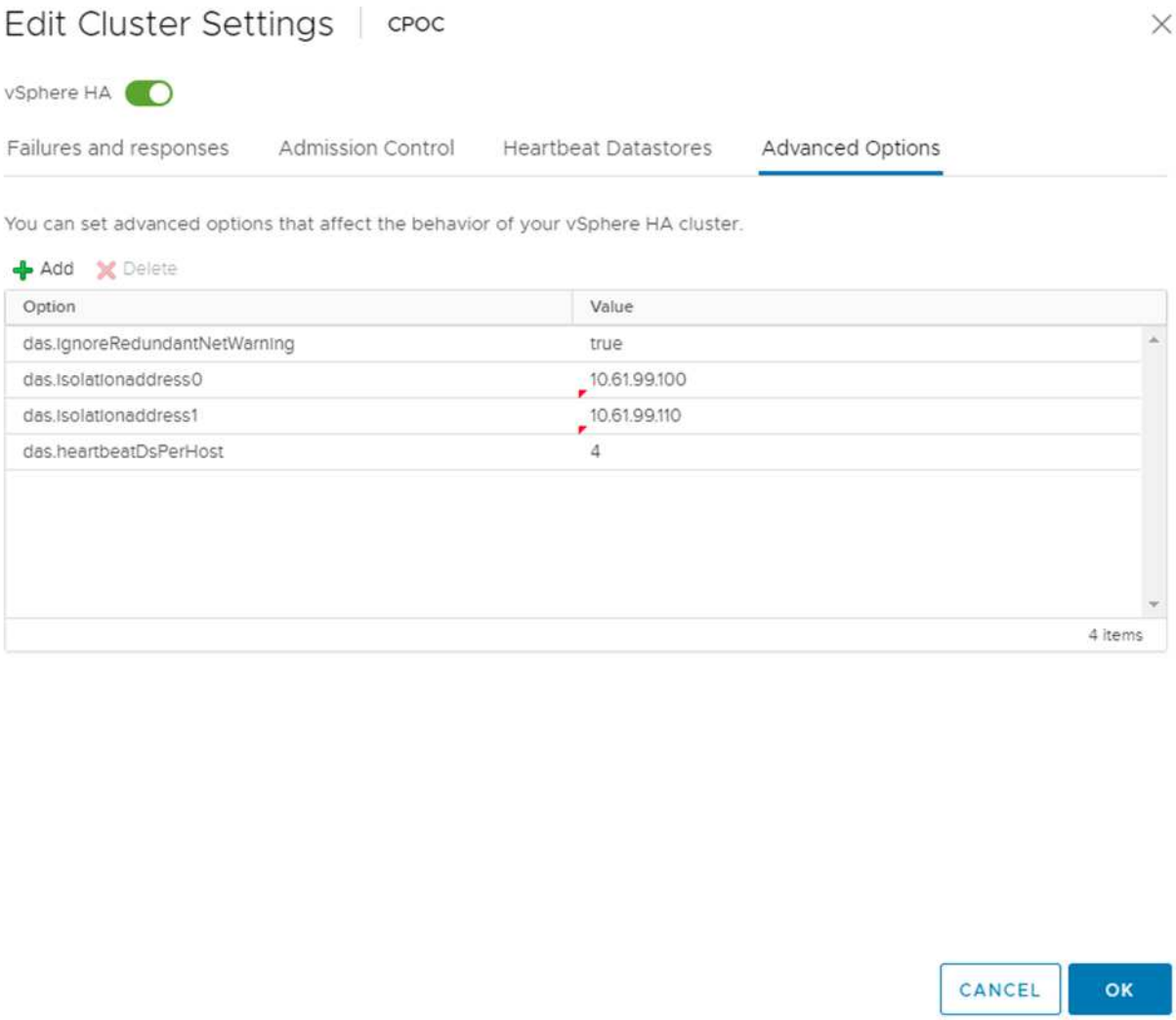
1. Na seção Heartbearing do datastore, selecione usar datastores na Lista especificada e elogiar automaticamente, se necessário.
2. Selecione os datastores que você deseja que o vCenter use em ambos os sites e pressione OK.



Configurar opções avançadas

Os eventos de isolamento ocorrem quando os hosts dentro de um cluster de HA perdem a conetividade com a rede ou com outros hosts no cluster. Por padrão, o vSphere HA usará o gateway padrão para sua rede de gerenciamento como endereço de isolamento padrão. No entanto, você pode especificar endereços de isolamento adicionais para o host fazer ping para determinar se uma resposta de isolamento deve ser acionada. Adicione dois IPs de isolamento que podem fazer ping, um por local. Não utilize o IP do gateway. A configuração avançada do vSphere HA usada é das.isolationaddress. Você pode usar endereços IP do ONTAP ou Mediator para esse fim.

```
https://www.vmware.com/docs/vmw-vmware-vsphere-metro-storage-cluster-
recommended-practices["Práticas recomendadas do VMware vSphere Metro
Storage Cluster"]Consulte para obter mais informações___.__
```



Adicionar uma configuração avançada chamada das.heartbeatDsPerHost pode aumentar o número de datastores de heartbeat. Use quatro datastores de heartbeat (HB DSS) - dois por local. Utilize a opção "Selecionar a partir da lista mas elogio". Isso é necessário porque, se um local falhar, você ainda precisará de dois DSS HB. No entanto, eles não precisam ser protegidos com a sincronização ativa do MetroCluster ou do SnapMirror.

```
https://www.vmware.com/docs/vmw-vmware-vsphere-metro-storage-cluster-
recommended-practices["Práticas recomendadas do VMware vSphere Metro
Storage Cluster"]Consulte para obter mais informações___.__
```

Afinidade do VMware DRS para NetApp MetroCluster

Nesta seção, criamos grupos DRS para VMs e hosts para cada site/cluster no ambiente MetroCluster. Em seguida, configuramos regras VM/Host para alinhar a afinidade do host da VM com os recursos de armazenamento local. Por exemplo, as VMs do Site A pertencem ao grupo VM sitea_vms e os hosts do Site A pertencem ao grupo de hosts sitea_hosts. Em seguida, nas regras VM/Host, declaramos que o sitea_vms deve ser executado em hosts no sitea_hosts.

- O NetApp recomenda altamente a especificação **deve ser executada em hosts no Grupo** em vez da especificação **deve ser executada em hosts no Grupo**. No caso de uma falha de host de um local, as VMs do local A precisam ser reiniciadas em hosts no local B por meio do vSphere HA, mas a última especificação não permite que o HA reinicie VMs no local B porque é uma regra geral. A especificação anterior é uma regra suave e será violada em caso de HA, permitindo assim disponibilidade em vez de desempenho.
- Você pode criar um alarme baseado em eventos que é acionado quando uma máquina virtual viola uma regra de afinidade VM-Host. No vSphere Client, adicione um novo alarme para a máquina virtual e selecione "VM is violing VM-Host Affinity Rule" como gatilho de evento. Para obter mais informações sobre como criar e editar alarmes, "Monitoramento e desempenho do vSphere"consulte a documentação.

Crie grupos de hosts DRS

Para criar grupos de hosts DRS específicos ao local A e local B, execute as seguintes etapas:

1. No cliente da Web vSphere, clique com o botão direito do Mouse no cluster no inventário e selecione Configurações.
2. Clique em VM/Host Groups.
3. Clique em Adicionar.
4. Digite o nome do grupo (por exemplo, sitea_hosts).
5. No menu tipo, selecione Grupo anfitrião.
6. Clique em Adicionar e selecione os hosts desejados no site A e clique em OK.
7. Repita estas etapas para adicionar outro grupo de hosts para o local B.
8. Clique em OK.

Crie grupos de VM DRS

Para criar grupos de VM DRS específicos para o local A e o local B, execute as seguintes etapas:

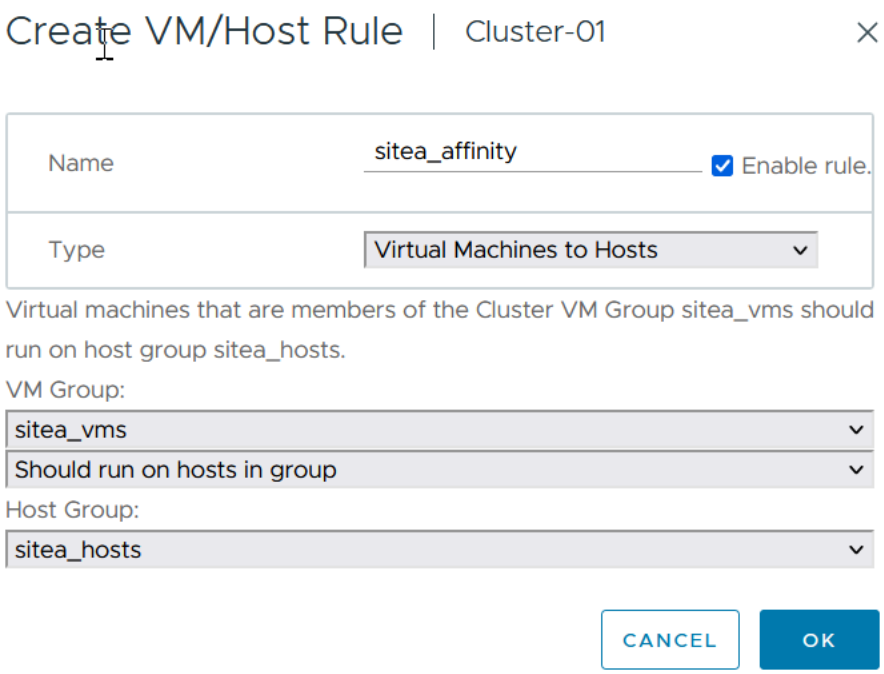
1. No cliente da Web vSphere, clique com o botão direito do Mouse no cluster no inventário e selecione Configurações.
2. Clique em VM/Host Groups.
3. Clique em Adicionar.
4. Digite o nome do grupo (por exemplo, sitea_vms).
5. No menu tipo, selecione Grupo VM.
6. Clique em Adicionar e selecione as VMs desejadas no local A e clique em OK.
7. Repita estas etapas para adicionar outro grupo de hosts para o local B.
8. Clique em OK.

Criar regras de host de VM

Para criar regras de afinidade do DRS específicas ao local A e ao local B, execute as seguintes etapas:

1. No cliente da Web vSphere, clique com o botão direito do Mouse no cluster no inventário e selecione Configurações.
2. Clique em VM/Host Rules.

3. Clique em Adicionar.
4. Digite o nome da regra (por exemplo, sitea_Affinity).
5. Verifique se a opção Ativar regra está marcada.
6. No menu tipo, selecione máquinas virtuais para hosts.
7. Selecione o grupo VM (por exemplo, sitea_vms).
8. Selecione o grupo Host (por exemplo, sitea_hosts).
9. Repita estas etapas para adicionar outra VM/regra de host para o local B.
10. Clique em OK.



Crie clusters de datastore, se necessário

Para configurar um cluster de datastore para cada site, execute as seguintes etapas:

1. Usando o cliente da Web vSphere, navegue até o data center em que o cluster HA reside em Storage.
2. Clique com o botão direito do rato no objeto do data center e selecione armazenamento > novo cluster do datastore.

*Ao usar o armazenamento ONTAP, é recomendável desativar o DRS de armazenamento.

- O DRS de armazenamento geralmente não é necessário ou recomendado para uso com sistemas de armazenamento ONTAP.
- O ONTAP oferece seus próprios recursos de eficiência de storage, como deduplicação, compressão e compactação, que podem ser afetados pelo Storage DRS.
- Se você estiver usando snapshots do ONTAP, o storage vMotion deixaria para trás a cópia da VM no snapshot, aumentando potencialmente a utilização do storage e pode afetar aplicativos de backup, como o NetApp SnapCenter, que rastreiam VMs e seus snapshots do ONTAP.

1. Selecione o cluster HA e clique em Next (seguinte).

1. Selecione os datastores pertencentes ao site A e clique em Avançar.

1. Reveja as opções e clique em concluir.
2. Repita essas etapas para criar o cluster do datastore do site B e verifique se somente os datastores do site B estão selecionados.

Disponibilidade do vCenter Server

Os dispositivos do vCenter Server (VCSAs) devem ser protegidos com o vCenter HA. O vCenter HA permite implantar dois VCSAs em um par de HA ativo-passivo. Um em cada domínio de falha. Você pode ler mais sobre o vCenter HA no "docs.vmware.com".

Resiliência para eventos planejados e não planejados

O NetApp MetroCluster e o SnapMirror ative Sync são ferramentas poderosas que melhoram a alta disponibilidade e as operações ininterruptas do hardware NetApp e do software ONTAP.

Essas ferramentas fornecem proteção em todo o local para todo o ambiente de storage, garantindo que seus dados estejam sempre disponíveis. Quer você esteja usando servidores autônomos, clusters de servidores de alta disponibilidade, contêineres ou servidores virtualizados, a tecnologia NetApp mantém perfeitamente a disponibilidade do storage em caso de uma interrupção total devido à perda de energia, resfriamento ou conectividade de rede, desligamento do storage array ou erro operacional.

O MetroCluster e o SnapMirror ative Sync oferecem três métodos básicos para a continuidade dos dados em caso de eventos planejados ou não planejados:

- Componentes redundantes para proteção contra falha de componente único
- Takeover de HA local para eventos que afetam um único controlador
- Proteção completa do local – retomada rápida do serviço movendo o armazenamento e o acesso do cliente do cluster de origem para o cluster de destino

Isso significa que as operações continuam sem problemas em caso de falha de um único componente e retornam automaticamente à operação redundante quando o componente com falha é substituído.

Todos os clusters do ONTAP, exceto clusters de nó único (normalmente versões definidas por software, como o ONTAP Select, por exemplo), têm recursos de HA incorporados, chamados de takeover e giveback. Cada controlador no cluster é emparelhado com outro controlador, formando um par de HA. Esses pares garantem que cada nó esteja conetado localmente ao storage.

O takeover é um processo automatizado no qual um nó assume o storage do outro para manter os serviços de dados. Giveback é o processo reverso que restaura a operação normal. O takeover pode ser planejado, como ao executar a manutenção de hardware ou atualizações de ONTAP, ou não planejado, resultante de um pânico de nó ou falha de hardware.

Durante uma takeover, LIFs nas nas configurações do MetroCluster fazem failover automático. No entanto, os LIFs SAN não fazem failover; eles continuarão a usar o caminho direto para os LUNs (Logical Unit Numbers).

Para obter mais informações sobre a aquisição de HA e a giveback, consulte o "Visão geral do gerenciamento do par HA". Vale a pena notar que essa funcionalidade não é específica para a sincronização ativa do MetroCluster ou do SnapMirror.

O switchover do local com o MetroCluster ocorre quando um local está off-line ou como uma atividade planejada para manutenção em todo o local. O local restante assume a propriedade dos recursos de storage (discos e agregados) do cluster off-line, e os SVMs no site com falha são colocados on-line e reiniciados no local de desastre, preservando sua identidade completa para acesso ao cliente e ao host.

Com a sincronização ativa do SnapMirror, uma vez que ambas as cópias são usadas ativamente simultaneamente, seus hosts existentes continuarão operando. O Mediador ONTAP é necessário para garantir que o failover do site ocorra corretamente.

Cenários de falha para vMSC com MetroCluster

As seções a seguir descrevem os resultados esperados de vários cenários de falha com sistemas vMSC e NetApp MetroCluster.

Falha de caminho de storage único

Nesse cenário, se componentes como a porta HBA, a porta de rede, a porta do switch de dados front-end ou um cabo FC ou Ethernet falharem, esse caminho específico para o dispositivo de armazenamento será marcado como morto pelo host ESXi. Se vários caminhos forem configurados para o dispositivo de storage fornecendo resiliência na porta HBA/rede/switch, o ESXi executará idealmente um switchover de caminho. Durante esse período, as máquinas virtuais permanecem em execução sem serem afetadas, pois a disponibilidade para o armazenamento é tratada fornecendo vários caminhos para o dispositivo de armazenamento.

Não há nenhuma mudança no comportamento do MetroCluster neste cenário, e todos os datastores continuam intactos de seus respetivos sites.

Melhor prática

Em ambientes em que os volumes NFS/iSCSI são usados, a NetApp recomenda ter pelo menos dois uplinks de rede configurados para a porta NFS vmkernel no vSwitch padrão e o mesmo no grupo de portas em que a interface NFS vmkernel é mapeada para o vSwitch distribuído. O agrupamento de NIC pode ser configurado em ativo-ativo ou ativo-standby.

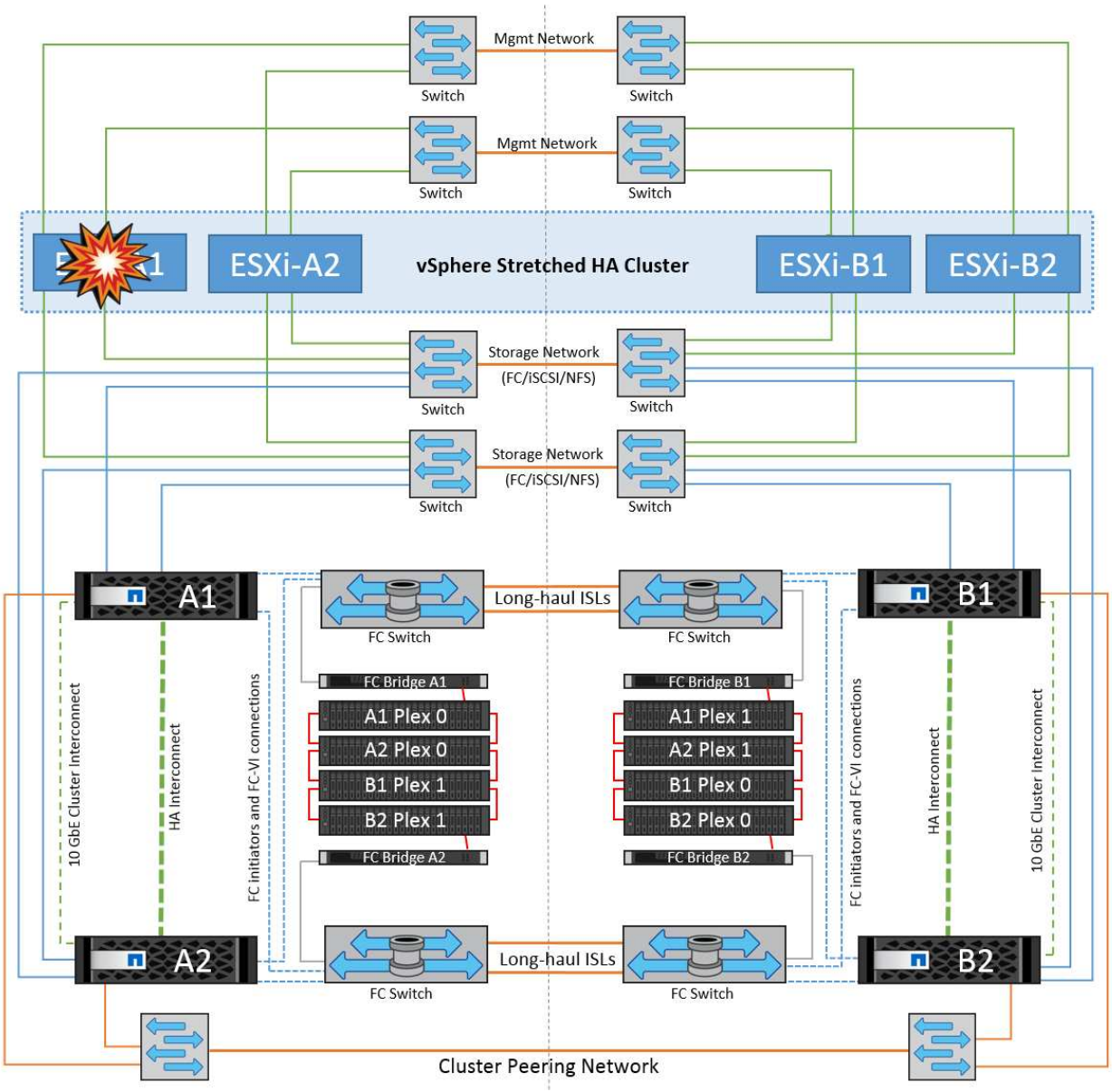
Além disso, para iSCSI LUNs, multipathing deve ser configurado vinculando as interfaces vmkernel aos adaptadores de rede iSCSI. Para obter mais informações, consulte a documentação de armazenamento do vSphere.

Melhor prática

Em ambientes em que LUNs de Fibre Channel são usados, a NetApp recomenda ter pelo menos dois HBAs, o que garante resiliência no nível de HBA/porta. O NetApp também recomenda um iniciador único para o zoneamento de destino único como a melhor prática para configurar o zoneamento.

O VSC (Virtual Storage Console) deve ser usado para definir políticas de multipathing porque define políticas para todos os dispositivos de armazenamento NetApp novos e existentes.

Falha única do host ESXi



Nesse cenário, se houver uma falha do host ESXi, o nó mestre no cluster do VMware HA deteta a falha do host, já que ele não recebe mais batimentos cardíacos da rede. Para determinar se o host está realmente inativo ou apenas uma partição de rede, o nó mestre monitora os batimentos cardíacos do datastore e, se eles estiverem ausentes, ele executa uma verificação final fazendo ping nos endereços IP de gerenciamento do host com falha. Se todas essas verificações forem negativas, o nó principal declara que este host é um host com falha e todas as máquinas virtuais que estavam sendo executadas nesse host com falha são reinicializadas no host sobrevivente no cluster.

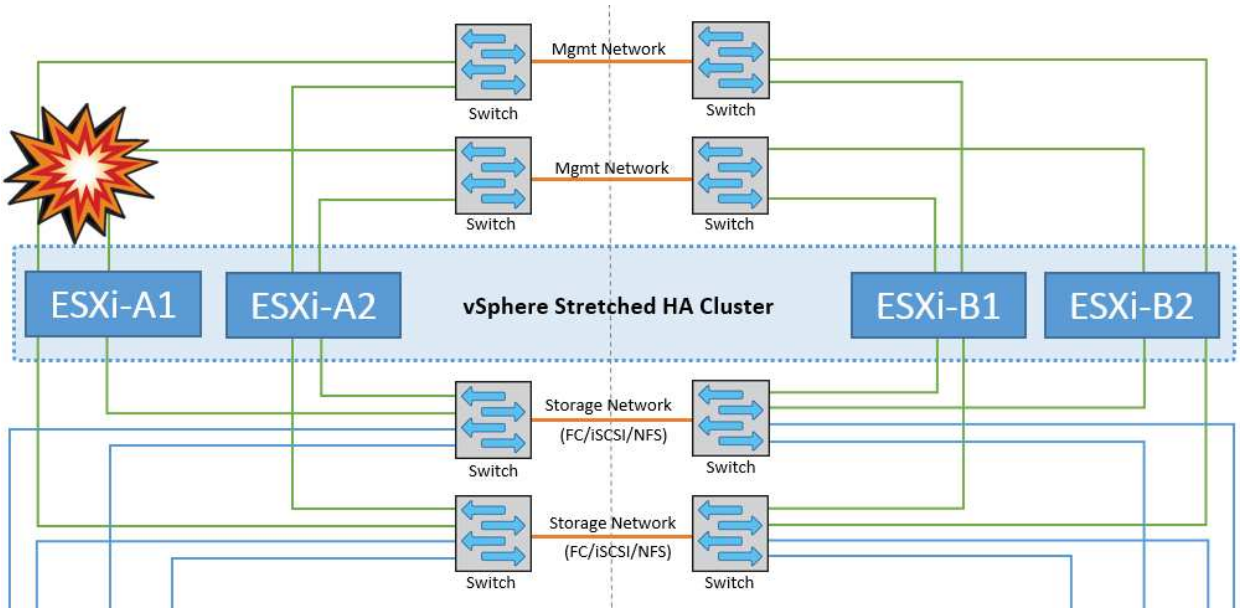
Se as regras de afinidade de host e VM DRS tiverem sido configuradas (as VMs no grupo VM sitea_vms devem executar hosts no grupo host sitea_hosts), o mestre HA primeiro verifica se há recursos disponíveis no local A. se não houver hosts disponíveis no local A, o mestre tentará reiniciar as VMs nos hosts no local B.

É possível que as máquinas virtuais sejam iniciadas nos hosts ESXi no outro site se houver uma restrição de recursos no site local. No entanto, as regras de afinidade de host e VM DRS definidas corrigirão se alguma regra for violada migrando as máquinas virtuais de volta para qualquer host ESXi sobrevivente no site local. Nos casos em que o DRS é definido como manual, o NetApp recomenda chamar o DRS e aplicar as recomendações para corrigir o posicionamento da máquina virtual.

Não há nenhuma mudança no comportamento do MetroCluster neste cenário e todos os datastores continuam

intactos de seus respetivos sites.

Isolamento do host ESXi

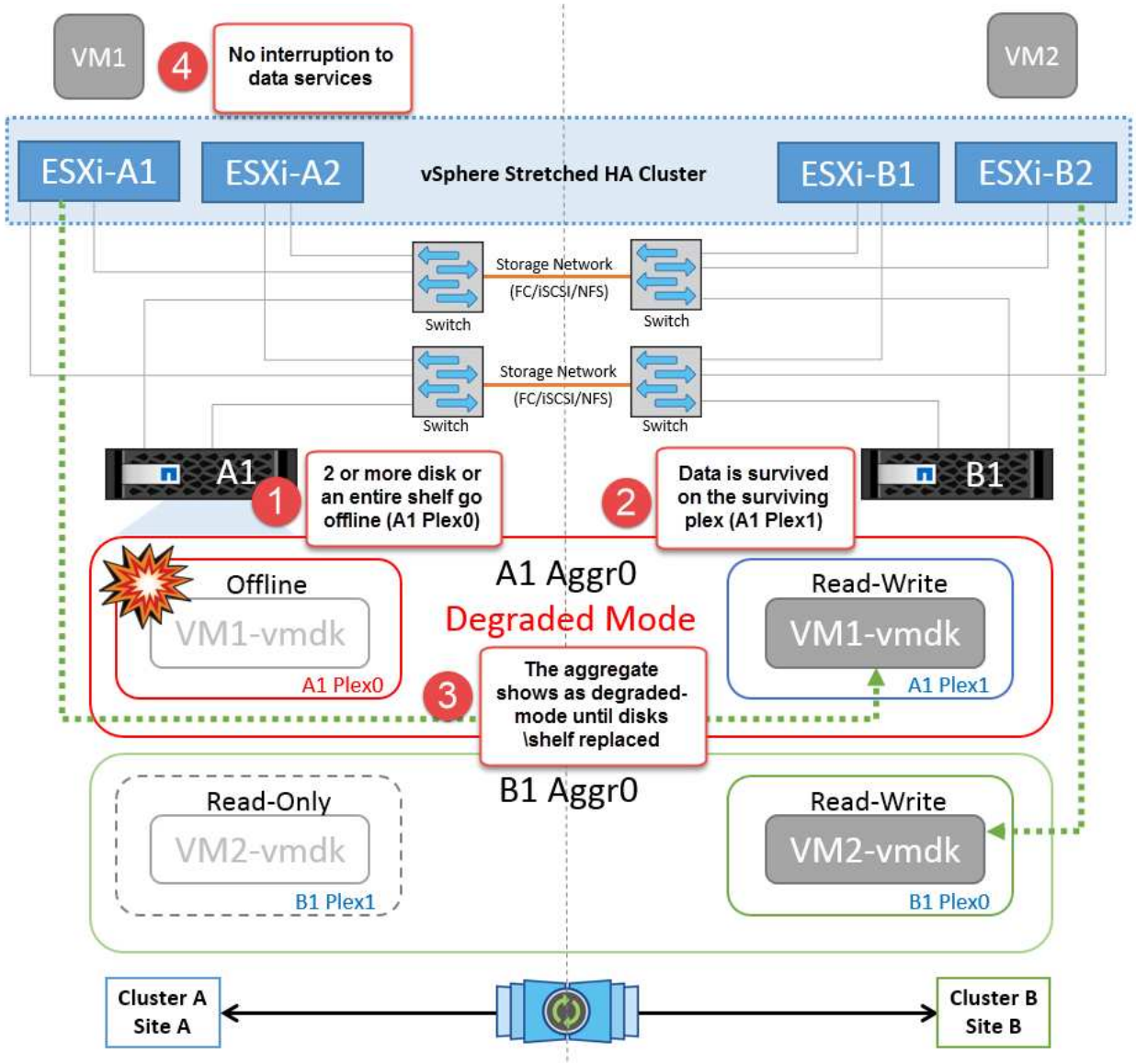


Nesse cenário, se a rede de gerenciamento do host ESXi estiver inativa, o nó mestre no cluster HA não receberá nenhum heartbeats e, portanto, esse host fica isolado na rede. Para determinar se ele falhou ou está isolado apenas, o nó principal começa a monitorar o batimento cardíaco do datastore. Se estiver presente, o host é declarado isolado pelo nó mestre. Dependendo da resposta de isolamento configurada, o host pode optar por desligar, desligar as máquinas virtuais ou até mesmo deixar as máquinas virtuais ligadas. O intervalo padrão para a resposta de isolamento é de 30 segundos.

Não há nenhuma mudança no comportamento do MetroCluster neste cenário e todos os datastores continuam intactos de seus respetivos sites.

Falha no compartimento de disco

Nesse cenário, há uma falha de mais de dois discos ou de uma gaveta inteira. Os dados são fornecidos do Plex sobrevivente sem interrupção para os serviços de dados. A falha do disco pode afetar um Plex local ou remoto. Os agregados serão apresentados como modo degradado porque apenas um Plex está ativo. Depois que os discos com falha forem substituídos, os agregados afetados serão ressincronizados automaticamente para reconstruir os dados. Após a ressincronização, os agregados retornarão automaticamente ao modo espelhado normal. Se mais de dois discos dentro de um único grupo RAID falharem, o Plex terá de ser reconstruído.

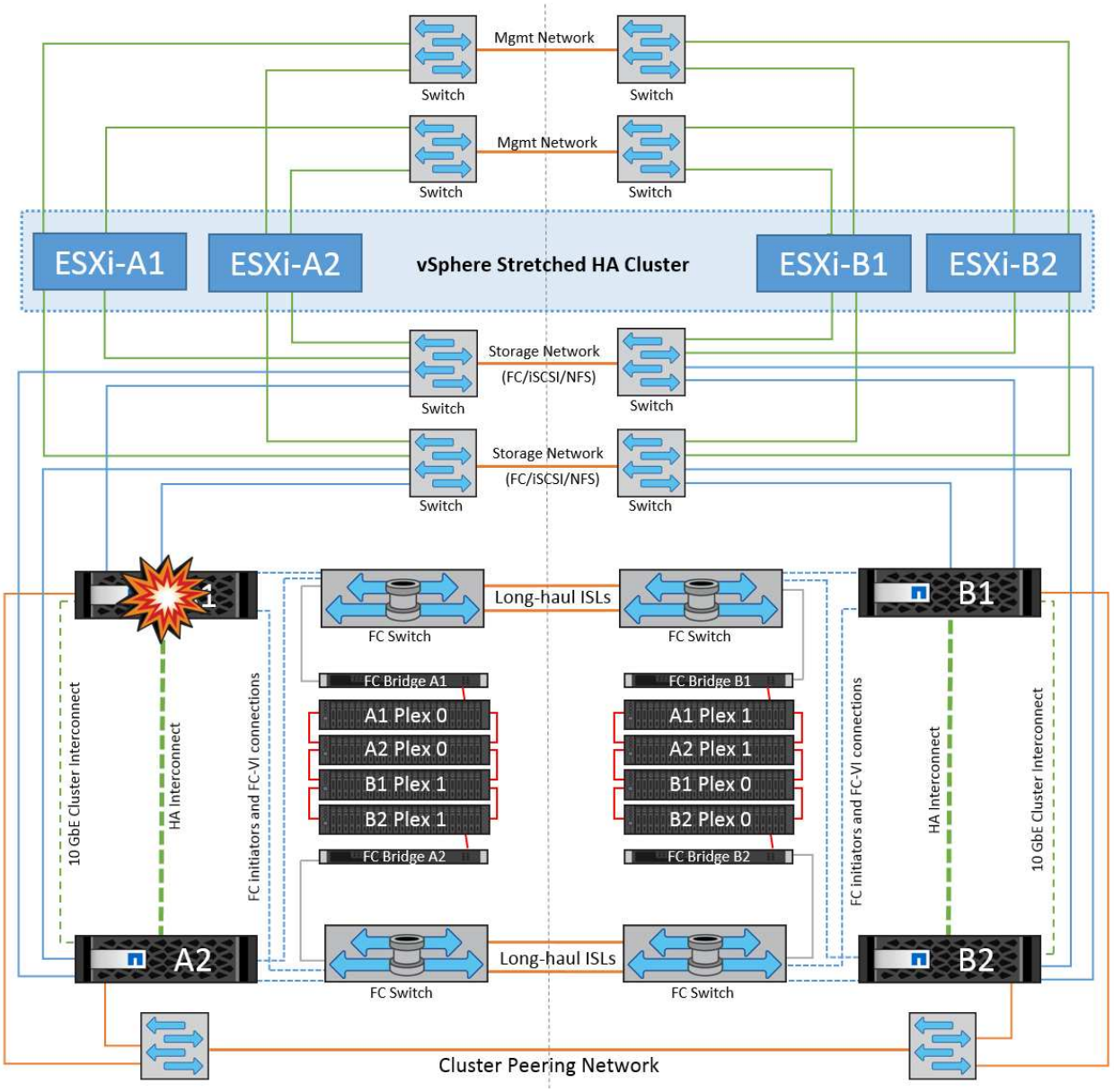


*[NOTA]

- Durante esse período, não há impactos nas operações de e/S da máquina virtual, mas há desempenho degradado porque os dados estão sendo acessados do compartimento de disco remoto por meio de links ISL.

Falha no controlador de storage único

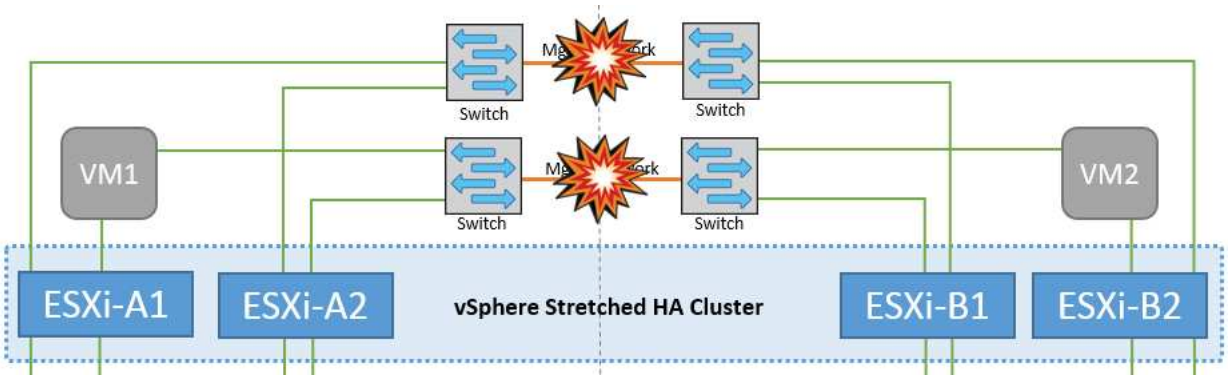
Nesse cenário, um dos dois controladores de storage falha em um local. Como há um par de HA em cada local, uma falha de um nó aciona o failover automaticamente para o outro nó. Por exemplo, se o nó A1 falhar, o storage e os workloads serão transferidos automaticamente para o nó A2. As máquinas virtuais não serão afetadas porque todos os plexos permanecem disponíveis. Os segundo nós do local (B1 e B2) não são afetados. Além disso, o vSphere HA não tomará nenhuma ação porque o nó mestre no cluster ainda estará recebendo os batimentos cardíacos da rede.



Se o failover fizer parte de um desastre contínuo (nó A1 faz failover para A2) e houver uma falha subsequente de A2 ou a falha completa do local A, o switchover após um desastre pode ocorrer no local B.

Avarias na ligação InterSwitch

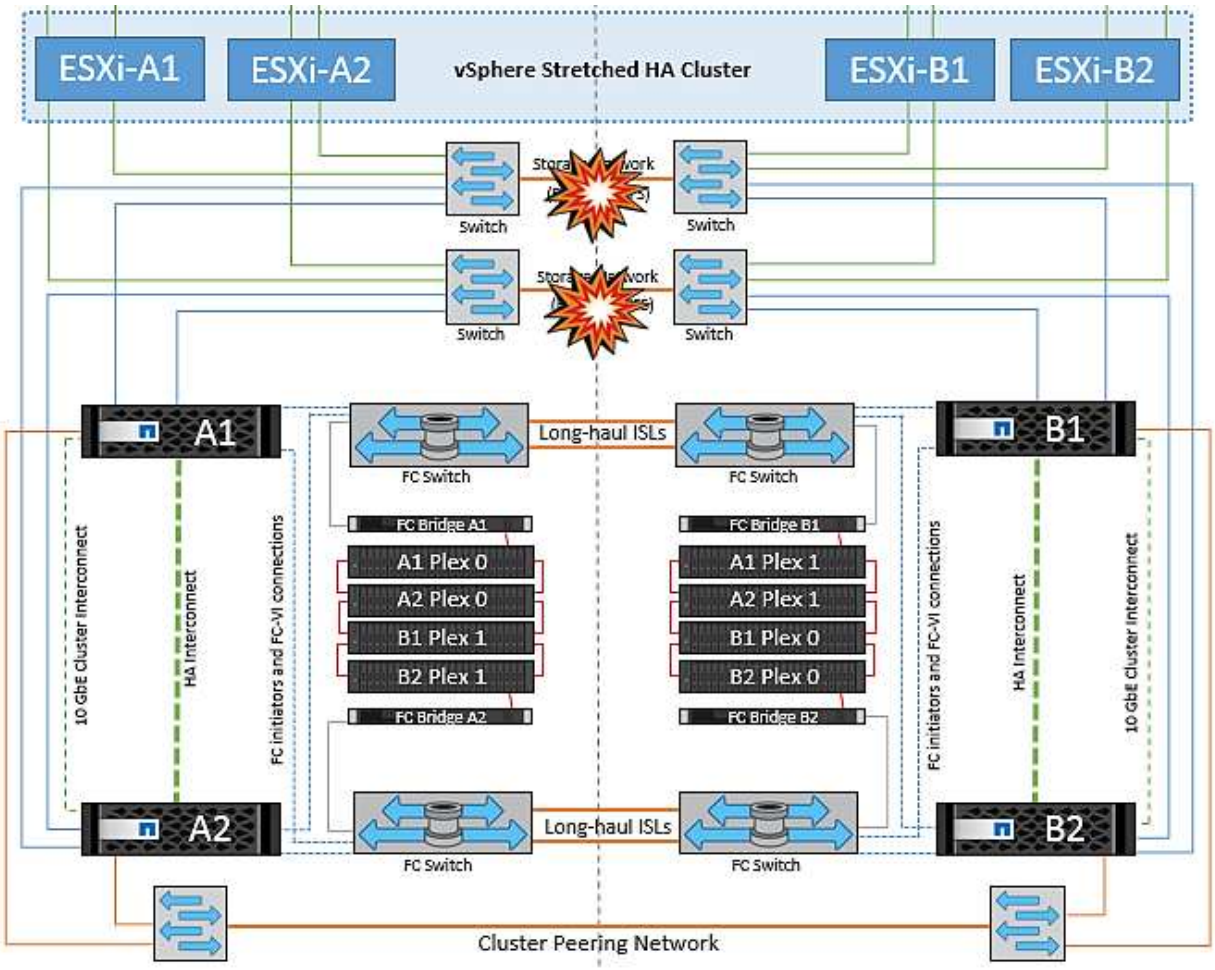
Falha de ligação InterSwitch na rede de gestão



Nesse cenário, se os links ISL na rede de gerenciamento de host front-end falharem, os hosts ESXi no local A não poderão se comunicar com hosts ESXi no local B. isso levará a uma partição de rede porque os hosts ESXi em um determinado local não poderão enviar os batimentos cardíacos da rede para o nó mestre no cluster HA. Como tal, haverá dois segmentos de rede por causa da partição e haverá um nó mestre em cada segmento que protegerá as VMs de falhas de host dentro do site específico.

Durante esse período, as máquinas virtuais permanecem em execução e não há alteração no comportamento do MetroCluster nesse cenário. Todos os armazenamentos de dados continuam intactos de seus respetivos sites.

Falha na ligação InterSwitch na rede de armazenamento

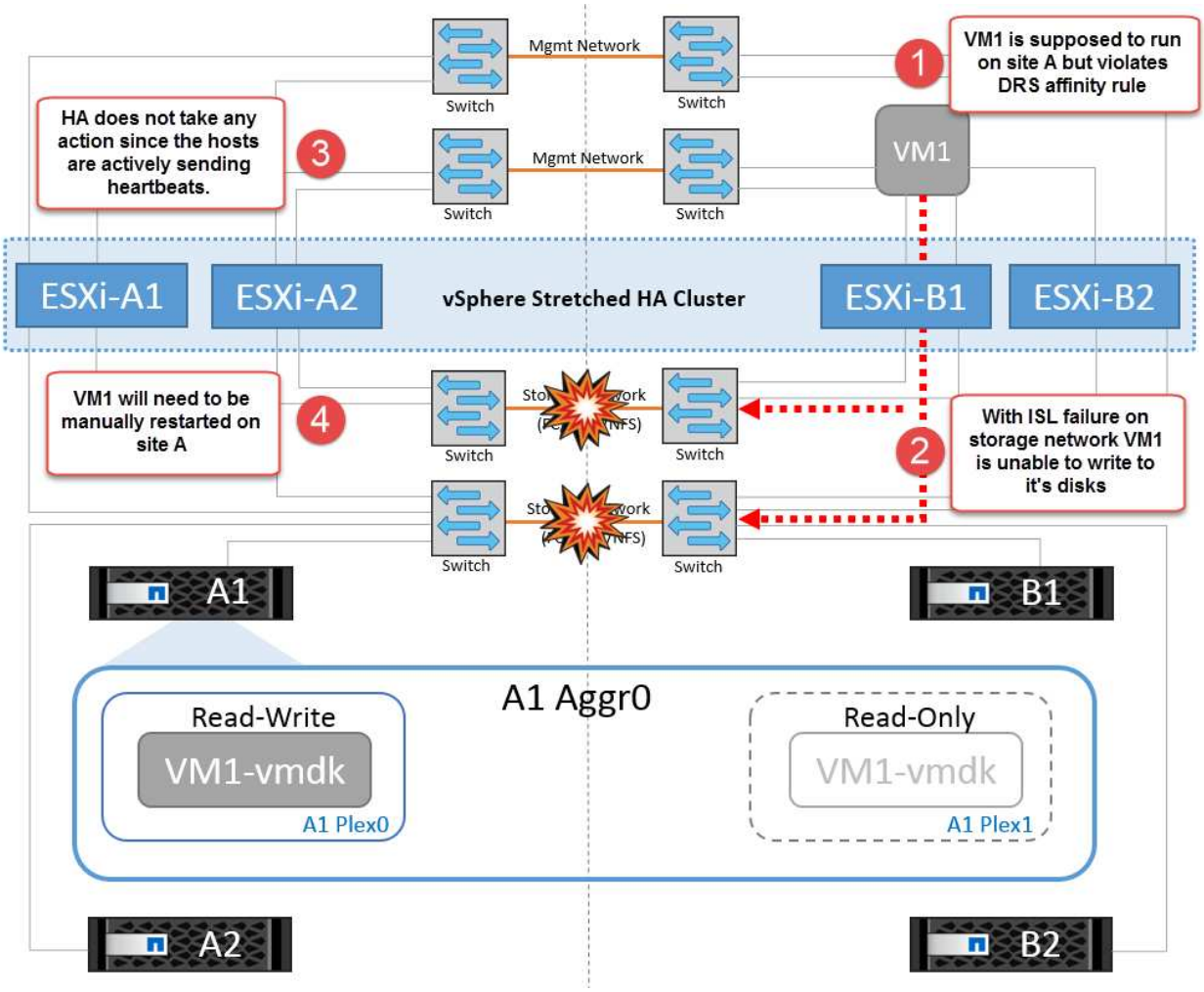


Nesse cenário, se os links ISL na rede de armazenamento de back-end falharem, os hosts no local A perderão acesso aos volumes de armazenamento ou LUNs do cluster B no local B e vice-versa. As regras do VMware DRS são definidas para que a afinidade do local de armazenamento de host facilite a execução das máquinas virtuais sem impactos no local.

Durante esse período, as máquinas virtuais permanecem em execução em seus respetivos sites e não há alteração no comportamento do MetroCluster nesse cenário. Todos os armazenamentos de dados continuam intactos de seus respetivos sites.

Se, por algum motivo, a regra de afinidade foi violada (por exemplo, VM1, que deveria ser executado a partir do site A, onde seus discos residem em nós de cluster local A, está sendo executado em um host no local B), o disco da máquina virtual será acessado remotamente por meio de links ISL. Devido à falha do link ISL, o VM1 em execução no local B não seria capaz de gravar em seus discos porque os caminhos para o volume

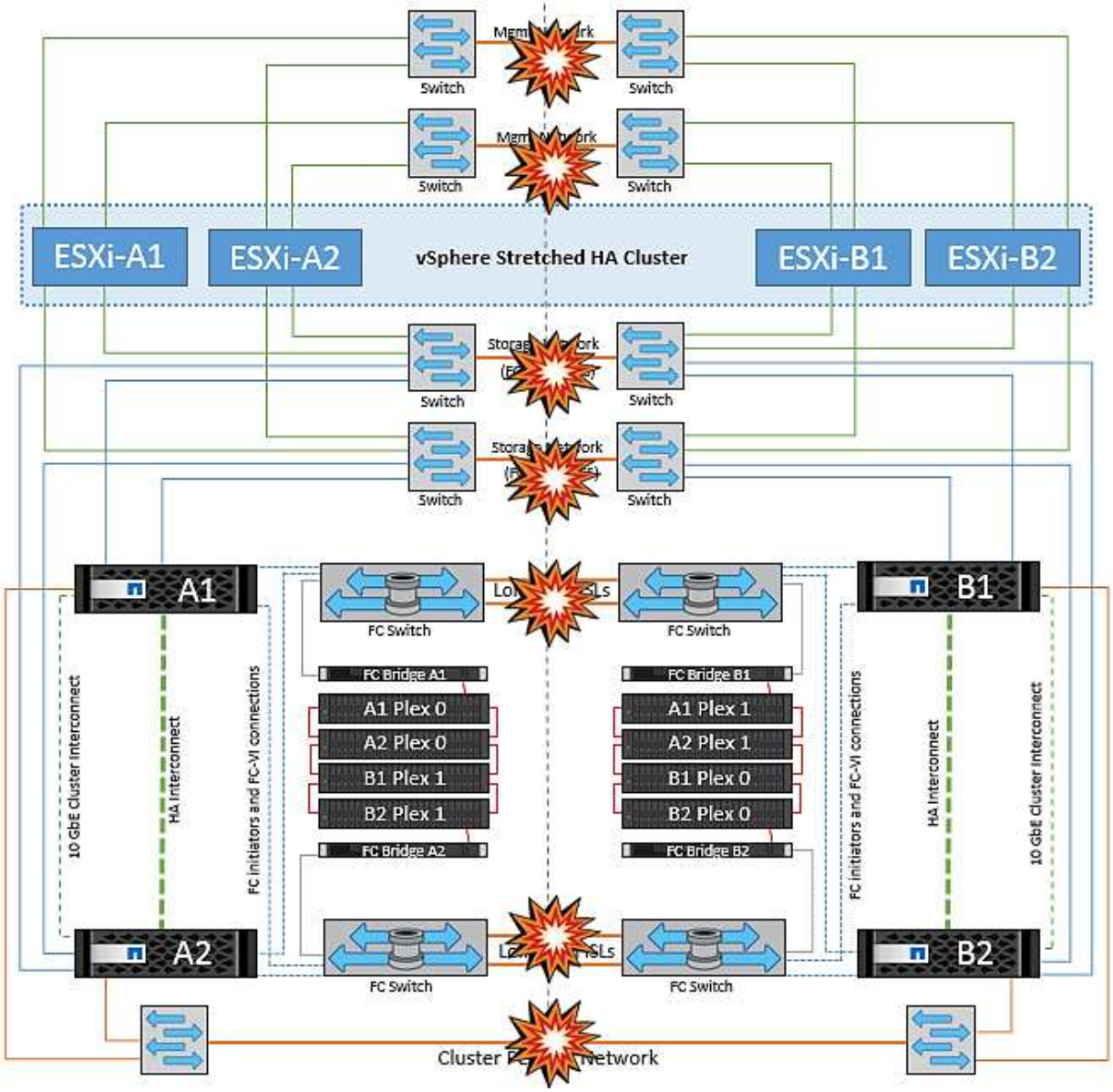
de armazenamento estão inativos e essa máquina virtual específica está inativa. Nessas situações, o VMware HA não toma nenhuma ação, uma vez que os hosts estão enviando batimentos cardíacos ativamente. Essas máquinas virtuais precisam ser manualmente desligadas e ligadas em seus respetivos sites. A figura a seguir ilustra uma VM que viola uma regra de afinidade DRS.



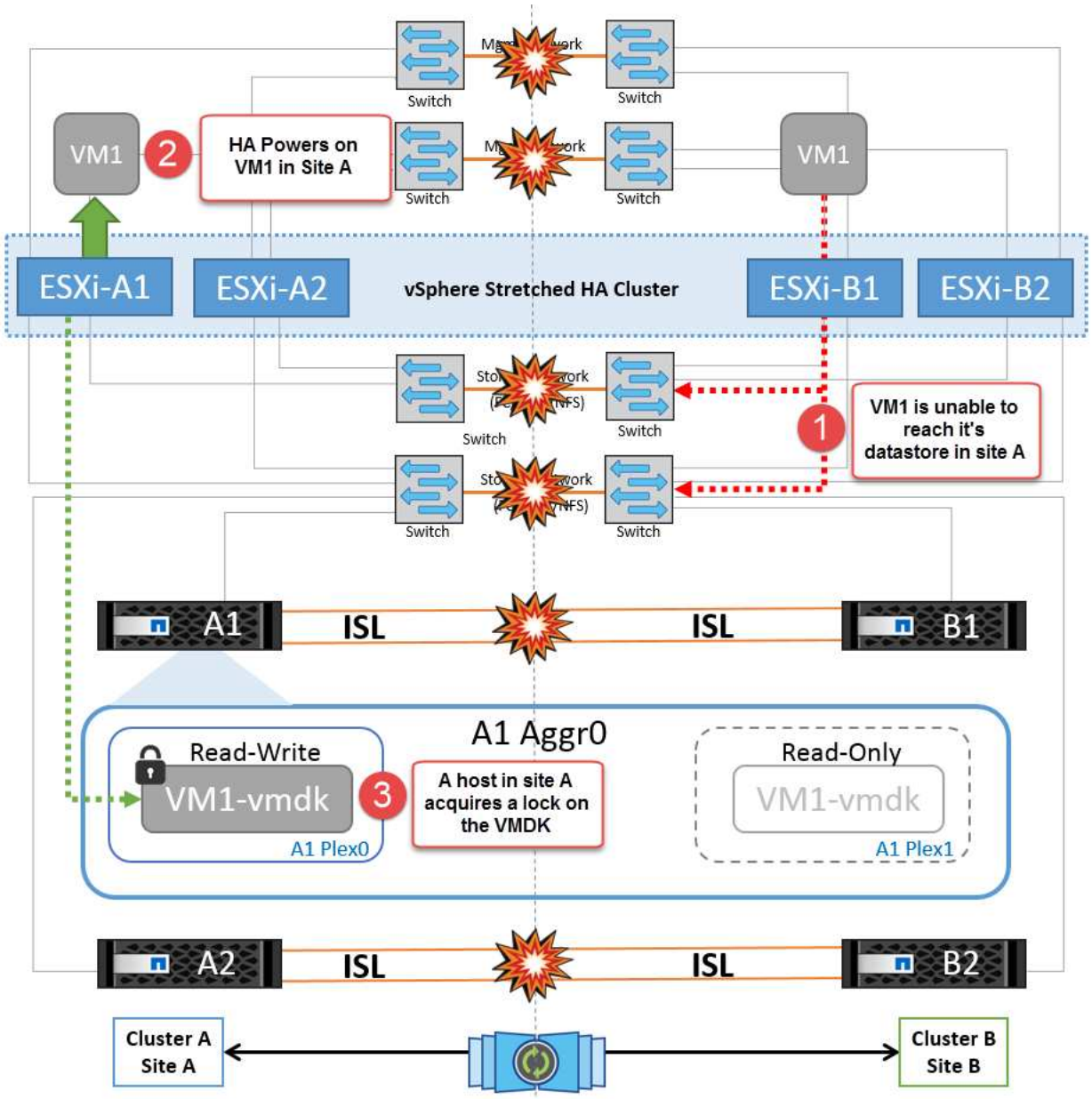
Todas as falhas do InterSwitch ou completa partição do data center

Neste cenário, todos os links ISL entre os sites estão inativos e ambos os sites são isolados uns dos outros. Como discutido em cenários anteriores, como falha de ISL na rede de gerenciamento e na rede de armazenamento, as máquinas virtuais não são afetadas em falha completa de ISL.

Depois que os hosts ESXi forem particionados entre sites, o agente do vSphere HA verificará os batimentos cardíacos do datastore e, em cada site, os hosts ESXi locais poderão atualizar os batimentos cardíacos do datastore para o respetivo volume/LUN de leitura/gravação. Os hosts no local A assumirão que os outros hosts ESXi no local B falharam porque não há heartbeats de rede/datastore. O vSphere HA no local A tentará reiniciar as máquinas virtuais do local B, o que acabará falhará porque os datastores do local B não estarão acessíveis devido a falha do ISL de armazenamento. Uma situação semelhante é repetida no local B..



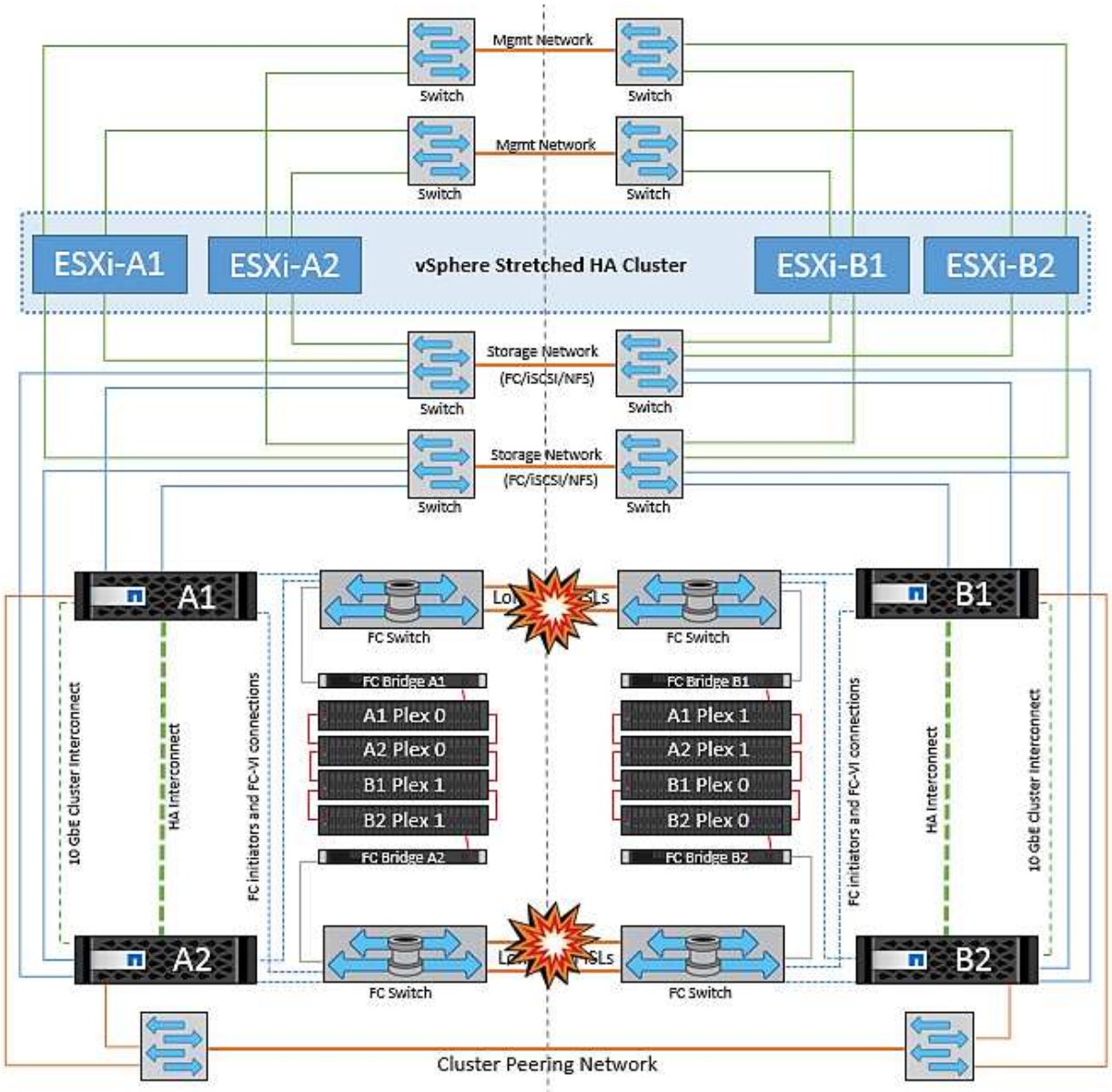
A NetApp recomenda determinar se alguma máquina virtual violou as regras do DRS. Todas as máquinas virtuais executadas a partir de um site remoto ficarão inativas, uma vez que não poderão acessar o datastore, e o vSphere HA reiniciará essa máquina virtual no site local. Depois que os links ISL estiverem novamente online, a máquina virtual que estava sendo executada no local remoto será morta, uma vez que não pode haver duas instâncias de máquinas virtuais executando com os mesmos endereços MAC.



Falha de ligação InterSwitch em ambas as malhas no NetApp MetroCluster

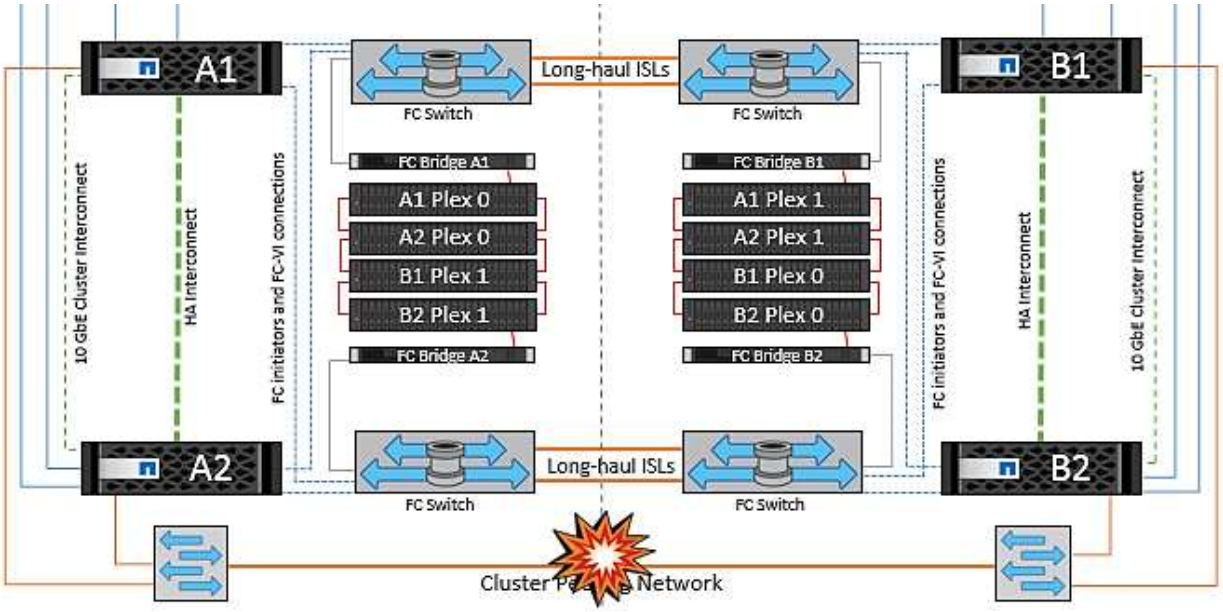
Em um cenário de falha de um ou mais ISLs, o tráfego continua através dos links restantes. Se todos os ISLs em ambas as malhas falharem, de modo que não haja nenhum link entre os locais para armazenamento e replicação do NVRAM, cada controladora continuará fornecendo seus dados locais. Em um mínimo de um ISL é restaurado, a ressincronização de todos os plexos acontecerá automaticamente.

Quaisquer gravações que ocorram depois de todos os ISLs estarem inativos não serão espelhadas para o outro site. Um switchover em caso de desastre, enquanto a configuração estiver nesse estado, incorreria, portanto, na perda dos dados que não haviam sido sincronizados. Neste caso, a intervenção manual é necessária para a recuperação após a mudança. Se for provável que nenhum ISLs esteja disponível por um período prolongado, um administrador pode optar por encerrar todos os serviços de dados para evitar o risco de perda de dados se for necessário um switchover em caso de desastre. A execução dessa ação deve ser ponderada contra a probabilidade de um desastre exigir mudança antes de pelo menos uma ISL ficar disponível. Alternativamente, se os ISLs estiverem falhando em um cenário em cascata, um administrador pode acionar um switchover planejado para um dos sites antes que todos os links tenham falhado.



Falha na ligação do cluster de peered

Em um cenário de falha de enlace de cluster com peered, como os ISLs de malha ainda estão ativos, os serviços de dados (leituras e gravações) continuam em ambos os locais para ambos os plexos. Qualquer alteração na configuração de cluster (por exemplo, adicionar um novo SVM, provisionar um volume ou LUN em um SVM existente) não pode ser propagado para o outro local. Estes são mantidos nos volumes de metadados locais do CRS e propagados automaticamente para o outro cluster após a recuperação do link do cluster peered. Se for necessário um switchover forçado antes que o link do cluster com peering possa ser restaurado, as alterações pendentes na configuração do cluster serão reproduzidas automaticamente da cópia replicada remota dos volumes de metadados no local que sobreviveu como parte do processo de switchover.



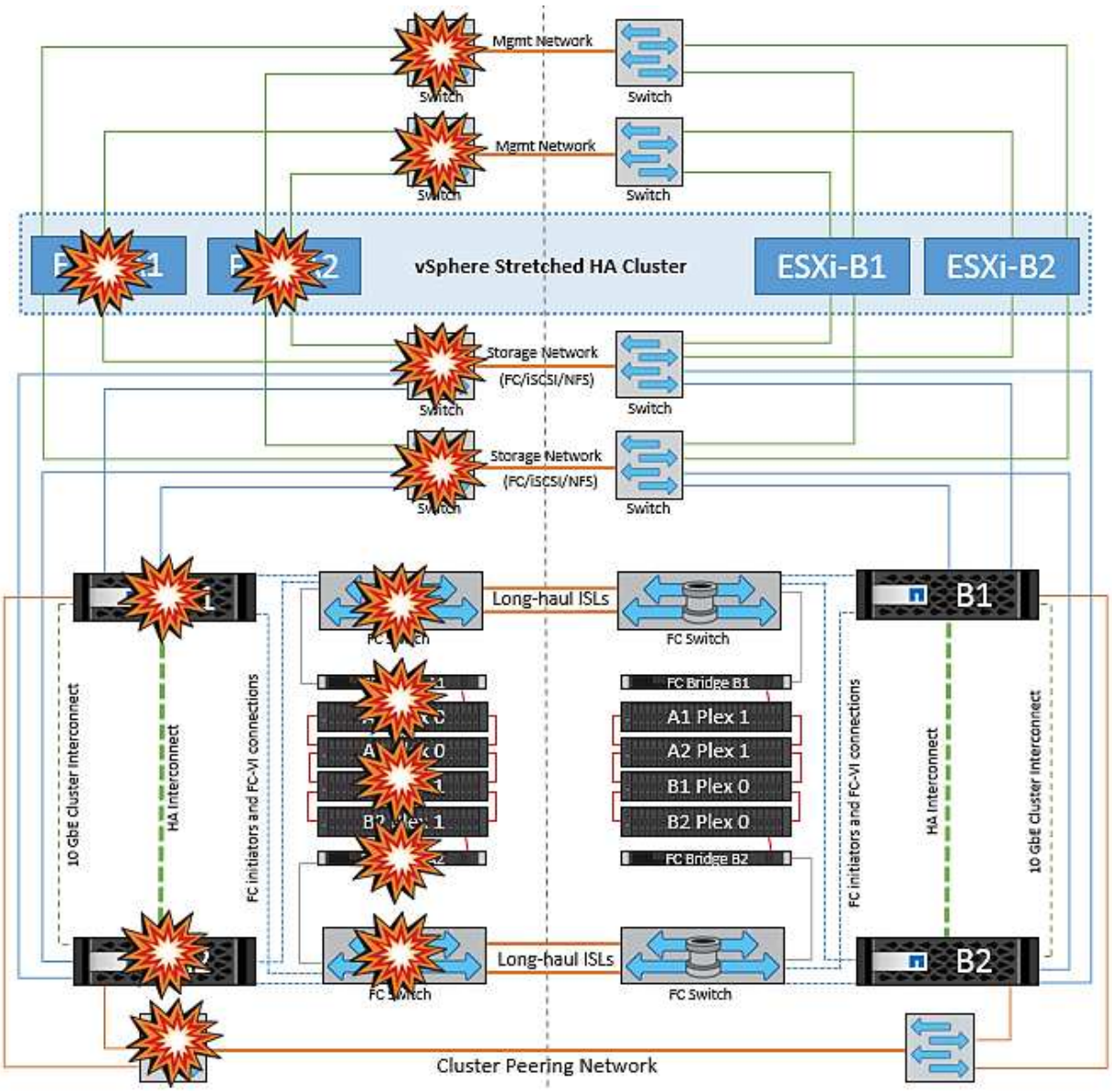
Falha no local completo

Em um local completo Um cenário de falha, os hosts ESXi no local B não receberão o heartbeat da rede dos hosts ESXi no local A porque estão inoperantes. O mestre de HA no local B verificará se os batimentos cardíacos do armazenamento de dados não estão presentes, declarará que os hosts no local A estão com falha e tentará reiniciar o local Uma máquina virtual no local B. durante esse período, o administrador de storage executa um switchover para retomar os serviços dos nós com falha no local sobrevivente, o que restaurará todos os serviços de armazenamento do Local A no local B. após o local A volumes ou LUNs estarem disponíveis no local B, o agente de HA tentará reiniciar o local B.

Se a tentativa do agente mestre do vSphere HA de reiniciar uma VM (que envolve registrá-la e ligá-la) falhar, a reinicialização será novamente tentada após um atraso. O atraso entre reinicializações pode ser configurado até um máximo de 30 minutos. O vSphere HA tenta reiniciar para um número máximo de tentativas (seis tentativas por padrão).

O mestre de HA não inicia as tentativas de reinicialização até que o gerente de colocação encontre um armazenamento adequado, portanto, no caso de uma falha completa no local, isso seria depois que o switchover foi executado.

Se o local A tiver sido substituído, uma falha subsequente de um dos nós do local B sobreviventes pode ser tratada de forma otimizada pelo failover para o nó sobrevivente. Neste caso, o trabalho de quatro nós agora está sendo executado por apenas um nó. A recuperação neste caso consistiria em realizar um giveback para o nó local. Em seguida, quando o local A é restaurado, uma operação de switchback é executada para restaurar a operação de estado estável da configuração.



Segurança do produto

Ferramentas do ONTAP para VMware vSphere

A engenharia de software com as ferramentas ONTAP para VMware vSphere emprega as seguintes atividades de desenvolvimento seguro:

- **Modelagem de ameaças.** O objetivo da modelagem de ameaças é descobrir falhas de segurança em um recurso, componente ou produto no início do ciclo de vida do desenvolvimento de software. Um modelo de ameaça é uma representação estruturada de todas as informações que afetam a segurança de um aplicativo. Em essência, é uma visão da aplicação e do seu ambiente através da lente da segurança.
- **Teste Dinâmico de Segurança de aplicativos (DAST).** Essa tecnologia foi projetada para detetar condições vulneráveis em aplicativos em seu estado de execução. O DAST testa as interfaces HTTP e HTML expostas de aplicações web-enable.
- **Moeda de código de terceiros.** Como parte do desenvolvimento de software com software de código aberto (OSS), você deve resolver vulnerabilidades de segurança que podem estar associadas a qualquer OSS incorporado em seu produto. Este é um esforço contínuo porque uma nova versão do OSS pode ter

uma vulnerabilidade descoberta recentemente relatada a qualquer momento.

- **Verificação de vulnerabilidades.** O objetivo da verificação de vulnerabilidades é detetar vulnerabilidades de segurança comuns e conhecidas nos produtos NetApp antes de serem lançadas aos clientes.
- * Teste de penetração.* O teste de penetração é o processo de avaliação de um sistema, aplicativo da Web ou rede para encontrar vulnerabilidades de segurança que possam ser exploradas por um invasor. Os testes de penetração (testes de caneta) na NetApp são conduzidos por um grupo de empresas terceirizadas aprovadas e confiáveis. Seu escopo de teste inclui o lançamento de ataques contra um aplicativo ou software semelhante a intrusos hostis ou hackers usando métodos ou ferramentas de exploração sofisticados.

Recursos de segurança do produto

As ferramentas do ONTAP para VMware vSphere incluem os seguintes recursos de segurança em cada versão.

- * Login banner.* O SSH é desativado por padrão e só permite logins únicos se ativado a partir do console da VM. O banner de login a seguir é exibido depois que o usuário insere um nome de usuário no prompt de login:

  AVISO: o acesso não autorizado a este sistema é proibido e será processado por lei. Ao acessar este sistema, você concorda que suas ações podem ser monitoradas se houver suspeita de uso não autorizado.

  Depois que o usuário concluir o login através do canal SSH, o seguinte texto é exibido:

```
Linux vsc1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

- **Controle de acesso baseado em função (RBAC).** Dois tipos de controles RBAC estão associados às ferramentas do ONTAP:
  - Privileges nativo do vCenter Server
  - Privileges específico do plug-in do vCenter. Para obter detalhes, "este link" consulte .
- **Canais de comunicação criptografados.** Toda a comunicação externa acontece por HTTPS usando a versão 1,2 do TLS.
- * Exposição mínima do porto.* Apenas as portas necessárias estão abertas no firewall.

  A tabela a seguir descreve os detalhes da porta aberta.

N.o da porta TCP v4/V6	Direção	Função
8143	de entrada	Conexões HTTPS para API REST
8043	de entrada	Conexões HTTPS

N.o da porta TCP v4/V6	Direção	Função
9060	de entrada	Conexões HTTPS usadas para SOAP em conexões https esta porta deve ser aberta para permitir que um cliente se conete ao servidor API de ferramentas ONTAP.
22	de entrada	SSH (Desativado por padrão)
9080	de entrada	Conexões HTTPS - VP e SRA - conexões internas somente de loopback
9083	de entrada	Conexões HTTPS - VP e SRA usados para SOAP em conexões https
1162	de entrada	Pacotes de intercetação SNMP VP
1527	apenas interno	Porta de banco de dados Derby, apenas entre este computador e ele mesmo, conexões externas não aceitas — somente conexões internas
443	bidirecional	Usado para conexões com clusters ONTAP

- **Suporte para certificados assinados pela autoridade de certificação (CA).** As ferramentas do ONTAP para VMware vSphere oferecem suporte a certificados assinados pela CA. Consulte este "artigo da kb" documento para obter mais informações.
- **Registo de auditoria.** Os pacotes de suporte podem ser baixados e são extremamente detalhados. As ferramentas do ONTAP Registram todas as atividades de login e logout do usuário em um arquivo de log separado. As chamadas de API VASA são registradas em um log de auditoria VASA dedicado (local cxf.log).
- **Políticas de senha.** As seguintes políticas de senha são seguidas:
  - As senhas não são registradas em nenhum arquivo de log.
  - As senhas não são comunicadas em texto simples.
  - As senhas são configuradas durante o próprio processo de instalação.
  - O histórico de senhas é um parâmetro configurável.
  - A idade mínima da senha é definida para 24 horas.
  - O preenchimento automático dos campos de senha está desativado.
  - As ferramentas do ONTAP criptografam todas as informações de credenciais armazenadas usando hash SHA256.

Plug-in do SnapCenter VMware vSphere

O plug-in do NetApp SnapCenter para a engenharia de software VMware vSphere usa as seguintes atividades de desenvolvimento seguro:

- **Modelagem de ameaças.** O objetivo da modelagem de ameaças é descobrir falhas de segurança em um recurso, componente ou produto no início do ciclo de vida do desenvolvimento de software. Um modelo de ameaça é uma representação estruturada de todas as informações que afetam a segurança de um aplicativo. Em essência, é uma visão da aplicação e do seu ambiente através da lente da segurança.
- **Teste dinâmico de segurança de aplicativos (DAST).** Tecnologias projetadas para detetar condições vulneráveis em aplicativos em seu estado de execução. O DAST testa as interfaces HTTP e HTML expostas de aplicações web-enable.
- **Moeda de código de terceiros.** Como parte do desenvolvimento de software e do uso de software de código aberto (OSS), é importante abordar vulnerabilidades de segurança que podem estar associadas ao OSS que foi incorporado ao seu produto. Este é um esforço contínuo, uma vez que a versão do componente OSS pode ter uma vulnerabilidade recentemente descoberta relatada a qualquer momento.
- **Verificação de vulnerabilidades.** O objetivo da verificação de vulnerabilidades é detetar vulnerabilidades de segurança comuns e conhecidas nos produtos NetApp antes de serem lançadas aos clientes.
- * Teste de penetração.* O teste de penetração é o processo de avaliação de um sistema, aplicativo da Web ou rede para encontrar vulnerabilidades de segurança que possam ser exploradas por um invasor. Os testes de penetração (testes de caneta) na NetApp são conduzidos por um grupo de empresas terceirizadas aprovadas e confiáveis. Seu escopo de teste inclui o lançamento de ataques contra um aplicativo ou software como intrusos hostis ou hackers usando métodos ou ferramentas de exploração sofisticados.
- **Atividade de resposta a incidentes de Segurança do produto.** Vulnerabilidades de segurança são descobertas interna e externamente para a empresa e podem representar um sério risco para a reputação da NetApp se não forem abordadas em tempo hábil. Para facilitar esse processo, uma equipe de resposta a incidentes de Segurança do produto (PSIRT) relata e rastreia as vulnerabilidades.

Recursos de segurança do produto

O plug-in do NetApp SnapCenter para VMware vSphere inclui os seguintes recursos de segurança em cada versão:

- **Acesso restrito ao shell.** O SSH é desativado por padrão, e logins únicos só são permitidos se estiverem ativados a partir do console da VM.
- **Aviso de acesso no banner de login.** O banner de login a seguir é exibido depois que o usuário insere um nome de usuário no prompt de login:

  AVISO: o acesso não autorizado a este sistema é proibido e será processado por lei. Ao acessar este sistema, você concorda que suas ações podem ser monitoradas se houver suspeita de uso não autorizado.

  Depois que o usuário concluir o login pelo canal SSH, a seguinte saída é exibida:

```
Linux vsc1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

- **Controle de acesso baseado em função (RBAC).** Dois tipos de controles RBAC estão associados às ferramentas do ONTAP:

- Privileges nativo do vCenter Server.
- Privileges específico do plug-in do VMware vCenter. Para obter mais informações, "Controle de acesso baseado em função (RBAC)"consulte .

- **Canais de comunicação criptografados.** Toda a comunicação externa acontece por HTTPS usando TLS.
- * Exposição mínima do porto.* Apenas as portas necessárias estão abertas no firewall.

A tabela a seguir fornece os detalhes da porta aberta.

Número da porta TCP v4/V6	Função
8144	Conexões HTTPS para API REST
8080	Conexões HTTPS para GUI OVA
22	SSH (desativado por padrão)
3306	MySQL (somente conexões internas; conexões externas desativadas por padrão)
443	Nginx (serviços de proteção de dados)

- **Suporte para certificados assinados pela Autoridade de Certificação (CA).** O plug-in do SnapCenter para VMware vSphere oferece suporte ao recurso de certificados assinados pela CA. "Como criar e/ou importar um certificado SSL para o plug-in SnapCenter para VMware vSphere (SCV)"Consulte .
- **Políticas de senha.** As seguintes políticas de senha estão em vigor:
  - As senhas não são registradas em nenhum arquivo de log.
  - As senhas não são comunicadas em texto simples.
  - As senhas são configuradas durante o próprio processo de instalação.
  - Todas as informações de credenciais são armazenadas usando hash SHA256.
- **Imagem base do sistema operacional.** O produto é fornecido com o sistema operacional base Debian para OVA com acesso restrito e acesso shell desativado. Isso reduz a ocupação física do ataque. Todos os sistemas operacionais baseados em versões do SnapCenter são atualizados com os patches de segurança mais recentes disponíveis para cobertura máxima de segurança.

A NetApp desenvolve recursos de software e patches de segurança em relação ao plug-in do SnapCenter para o dispositivo VMware vSphere e, em seguida, os lança aos clientes como uma plataforma de software agrupada. Como esses dispositivos incluem dependências específicas do sistema sub-operacional Linux, bem como nosso software proprietário, a NetApp recomenda que você não faça alterações no sistema sub-operacional porque isso tem um alto potencial para afetar o dispositivo NetApp. Isto pode afetar a capacidade do NetApp de suportar o aparelho. A NetApp recomenda testar e implantar nossa versão de código mais recente para dispositivos porque eles são lançados para corrigir quaisquer problemas relacionados à segurança.

Guia de fortalecimento da segurança para as ferramentas do ONTAP para VMware vSphere

Guia de fortalecimento da segurança para ferramentas do ONTAP para VMware vSphere 9,13

O guia de proteção de segurança para as ferramentas do ONTAP para VMware vSphere fornece um conjunto abrangente de instruções para configurar as configurações mais seguras.

Estes guias aplicam-se aos aplicativos e ao SO convidado do próprio aparelho.

Verificando a integridade das ferramentas do ONTAP para os pacotes de instalação do VMware vSphere 9,13

Existem dois métodos disponíveis para os clientes verificarem a integridade de seus pacotes de instalação de ferramentas ONTAP.

1. Verificando as somas de verificação
2. Verificando a assinatura

As somas de verificação são fornecidas nas páginas de download dos pacotes de instalação do OTV. Os usuários devem verificar as somas de verificação dos pacotes baixados em relação à soma de verificação fornecida na página de download.

Verificando a assinatura das ferramentas ONTAP OVA

O pacote de instalação do vApp é entregue na forma de um tarball. Este tarball contém certificados intermediários e raiz para o dispositivo virtual, juntamente com um arquivo README e um pacote OVA. O arquivo README orienta os usuários sobre como verificar a integridade do pacote vApp OVA.

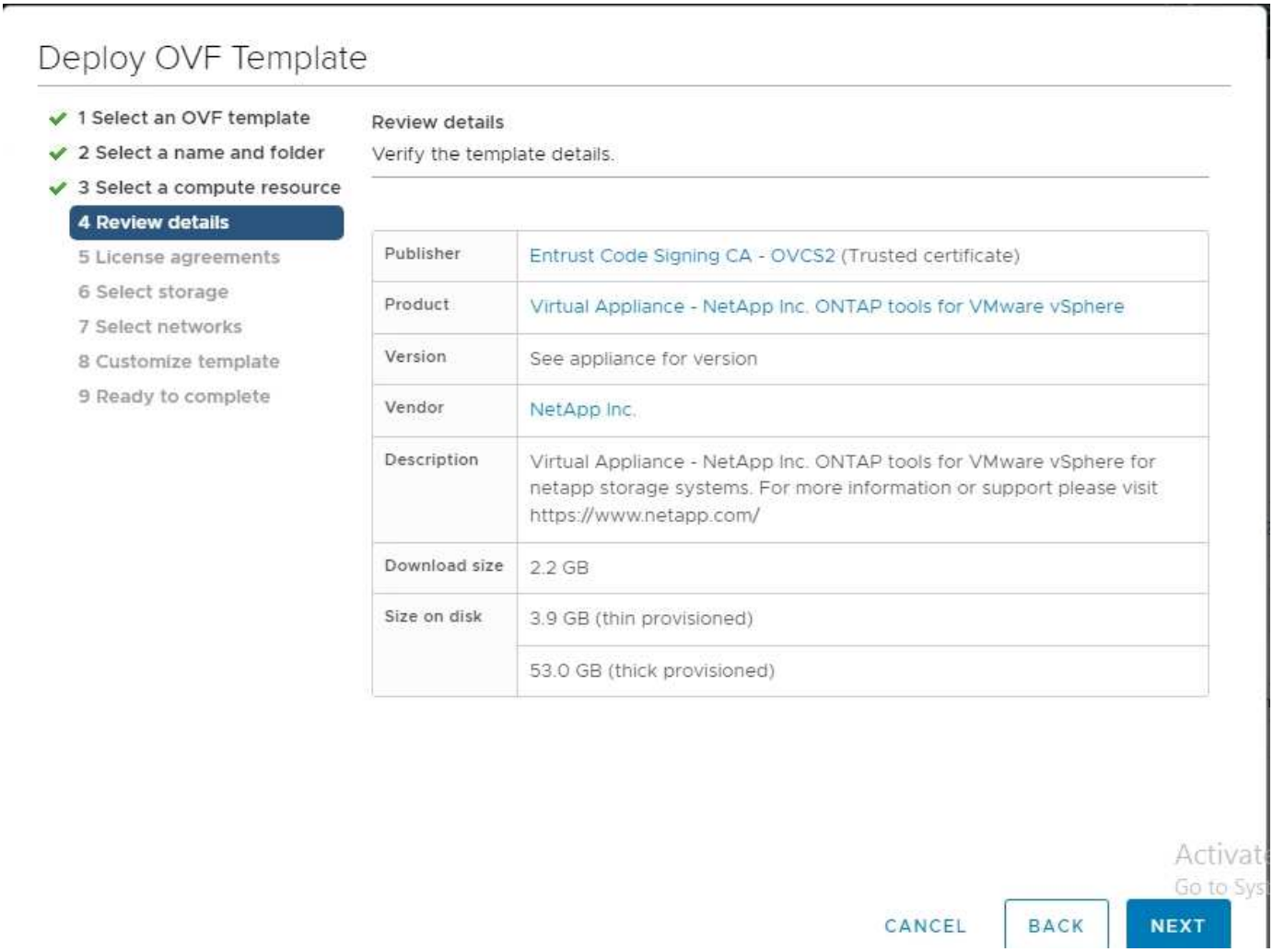
Os clientes também devem fazer o upload do certificado raiz e intermediário fornecido no vCenter versão 7.0U3E e superior. Para versões do vCenter entre 7.0.1 e 7,0.U3E, a funcionalidade de verificação de certificado não é suportada pela VMware. Os clientes não precisam carregar nenhum certificado para o vCenter versões 6.x.

Carregar o certificado raiz confiável para o vCenter

1. Faça login com o VMware vSphere Client no vCenter Server.
2. Especifique o nome de usuário e a senha para o administrador ou outro membro do grupo Administradores de logon único do vCenter. Se você especificou um domínio diferente durante a instalação, faça login como administrador.
3. Navegue até a IU de Gerenciamento de certificados: a. no menu inicial, selecione Administração. b. em certificados, clique em Gerenciamento de certificados.
4. Se o sistema solicitar, insira as credenciais do vCenter Server.
5. Em certificados raiz confiáveis, clique em Adicionar.
6. Clique em Procurar e selecione a localização do ficheiro .pem do certificado (OTV_OVA_INTER_ROOT_CERT_Chain.pem).
7. Clique em Adicionar. O certificado é adicionado à loja.

"Adicione um certificado raiz confiável ao armazenamento de certificados"Consulte para obter mais informações. Ao implantar um vApp (usando o arquivo OVA), a assinatura digital do pacote vApp pode ser verificada na página 'Detalhes de revisão'. Se o pacote vApp baixado for original, a coluna 'Publisher' exibe

'certificado confiável' (como na captura de tela a seguir).



Verificando a assinatura das ferramentas ONTAP ISO e SRA tar.gz

A NetApp compartilha seu certificado de assinatura de código com os clientes na página de download do produto, juntamente com os arquivos zip do produto para OTV-ISO e SRA.tgz.

A partir do certificado de assinatura de código, os usuários podem extrair a chave pública como abaixo:

```
 #> openssl x509 -in <code-sign-cert, pem file> -pubkey -noout > <public-
key name>
Em seguida, a chave pública deve ser usada para verificar a assinatura
para iso e tgz produto zip como abaixo:
```

```
 #> openssl dgst -sha256 -verify <public-key> -signature <signature-file>
<binary-name>
Exemplo:
```

```
#> openssl x509 -in OTV_ISO_CERT.pem -pubkey -noout > OTV_ISO.pub
#> openssl dgst -sha256 -verify OTV_ISO.pub -signature netapp-ontap-tools-
for-vmware-vsphere-9.12-upgrade-iso.sig netapp-ontap-tools-for-vmware-
vsphere-9.12-upgrade.iso
Verified OK  => response
```

Portas e protocolos para ferramentas ONTAP 9,13

Aqui estão listadas as portas e protocolos necessários que permitem a comunicação entre as ferramentas do ONTAP para o servidor VMware vSphere e outras entidades, como sistemas de storage gerenciados, servidores e outros componentes.

Portas de entrada e saída necessárias para o OTV

Observe a tabela abaixo, que lista as portas de entrada e saída necessárias para o funcionamento adequado das ferramentas do ONTAP. É importante garantir que apenas as portas mencionadas na tabela estejam abertas para conexões de máquinas remotas, enquanto todas as outras portas devem ser bloqueadas para conexões de máquinas remotas. Isso ajudará a garantir a segurança e a segurança do seu sistema.

A tabela a seguir descreve os detalhes da porta aberta.

Número da porta TCP v4/V6	Direção	Função
8143	de entrada	Conexões HTTPS para API REST
8043	de entrada	Conexões HTTPS
9060	de entrada	Esta porta deve ser aberta para permitir que um cliente se conete ao servidor de API do ONTAP Tools.
22	de entrada	SSH (Desativado por padrão)
9080	de entrada	Conexões HTTPS - VP e SRA - conexões internas somente de loopback
9083	de entrada	Conexões HTTPS - VP e SRA usados para SOAP em conexões HTTPS
1162	de entrada	Pacotes de intercetação SNMP VP
8443	de entrada	Plug-in remoto
1527	apenas interno	Porta de banco de dados Derby, apenas entre este computador e ele mesmo, conexões externas não aceitas - somente conexões internas
8150	apenas interno	O serviço de integridade de log é executado na porta
443	bidirecional	Usado para conexões com clusters ONTAP

Controlar o acesso remoto ao banco de dados Derby

Os administradores podem acessar o banco de dados derby com os seguintes comandos. Ele pode ser acessado através da VM local das ferramentas do ONTAP, bem como de um servidor remoto com as

seguintes etapas:

```
java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;
connect 'jdbc:derby://<OTV-
IP>:1527//opt/netapp/vpserver/vvoldb;user=<user>;password=<password>';
```

*[.Underline

```
root@UnifiedVSC:~# java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;
ij version 10.15
ij> connect 'jdbc:derby://localhost:1527//opt/netapp/vpserver/vvoldb;user=app;password=[redacted]';
ij> show tables;
TABLE_SCHEM         |TABLE_NAME                    |REMARKS
------------------------------------------------------------------------
SYS                 |SYSALIASES                    |
SYS                 |SYSCHECKS                     |
SYS                 |SYSCOLPERMS                   |
SYS                 |SYSCOLUMNS                    |
SYS                 |SYSCONGLOMERATES              |
SYS                 |SYSCONSTRAINTS                |
SYS                 |SYSDEPENDS                    |
SYS                 |SYSFILES                      |
SYS                 |SYSFOREIGNKEYS                |
SYS                 |SYSKEYS                       |
SYS                 |SYSPERMS                      |
```

Ferramentas do ONTAP para pontos de acesso do VMware vSphere 9,13 (usuários)

A instalação das Ferramentas do ONTAP para VMware vSphere cria e usa três tipos de usuários:

1. Usuário do sistema: A conta de usuário raiz
2. Usuário do aplicativo: O usuário administrador, usuário de manutenção e contas de usuário de banco de dados
3. Usuário de suporte: A conta de usuário diag

1. Utilizador do sistema

O usuário System(root) é criado pela instalação de ferramentas ONTAP no sistema operacional subjacente (Debian).

- Um usuário padrão do sistema "root" é criado no Debian pela instalação de ferramentas do ONTAP. Seu padrão é desabilitado e pode ser habilitado em uma base ad-hoc através do console 'aint'.

2. Utilizador da aplicação

O usuário do aplicativo é nomeado como um usuário local nas ferramentas do ONTAP. Estes são usuários criados no aplicativo de ferramentas do ONTAP. A tabela abaixo lista os tipos de usuários de aplicativos:

Usuário	Descrição
Usuário Administrador	Ele é criado durante a instalação das ferramentas do ONTAP e o usuário fornece as credenciais ao implantar as ferramentas do ONTAP. Os usuários têm a opção de alterar a 'senha' no console 'não'. A senha expirará em 90 dias e espera-se que os usuários alterem a mesma.

Usuário	Descrição
Utilizador de manutenção	Ele é criado durante a instalação das ferramentas do ONTAP e o usuário fornece as credenciais ao implantar as ferramentas do ONTAP. Os usuários têm a opção de alterar a 'senha' no console 'não'. Este é um usuário de manutenção e é criado para executar as operações do console de manutenção.
Utilizador da base de dados	Ele é criado durante a instalação das ferramentas do ONTAP e o usuário fornece as credenciais ao implantar as ferramentas do ONTAP. Os usuários têm a opção de alterar a 'senha' no console 'não'. A senha expirará em 90 dias e espera-se que os usuários alterem a mesma.

3. Usuário do suporte (usuário diag)

Durante a instalação das ferramentas do ONTAP, um usuário de suporte é criado. Esse usuário pode ser usado para acessar as ferramentas do ONTAP em caso de qualquer problema ou falha no servidor e para coletar logs. Por padrão, esse usuário está desativado, mas pode ser habilitado em uma base adhoc através do console 'mint'. É importante notar que este utilizador será automaticamente desativado após um determinado período de tempo.

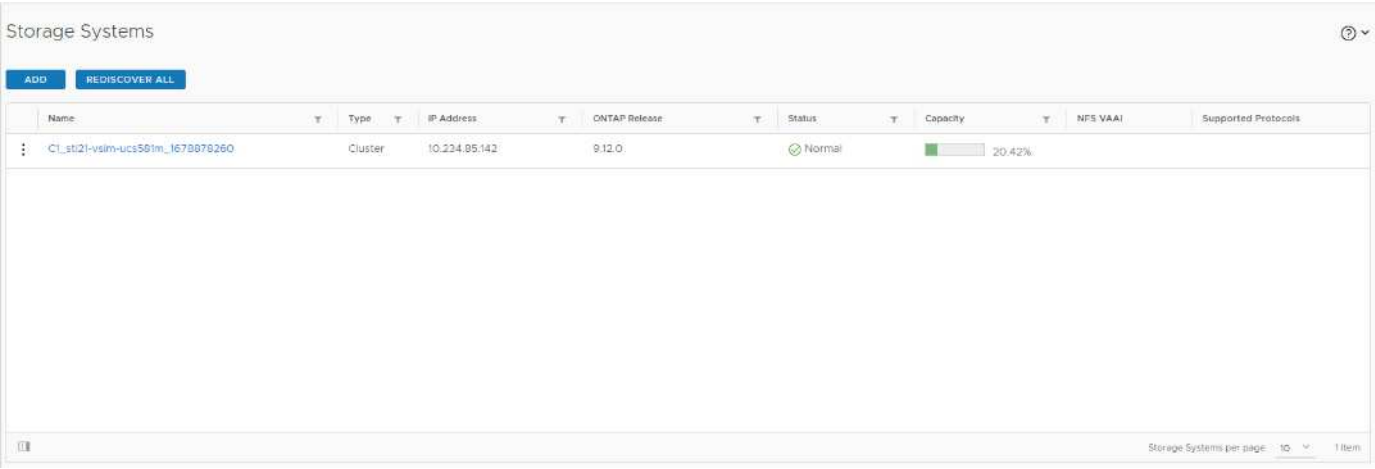
ONTAP Tools 9,13 TLS mútuo (autenticação baseada em certificado)

As versões 9,7 e posteriores do ONTAP suportam comunicação TLS mútua. A partir das Ferramentas do ONTAP para VMware e vSphere 9,12, o TLS mútuo é usado para comunicação com clusters recém-adicionados (dependendo da versão do ONTAP).

ONTAP

Para todos os sistemas de armazenamento adicionados anteriormente: Durante uma atualização, todos os sistemas de armazenamento de dados adicionados serão auto-confiáveis e os mecanismos de autenticação baseados em certificado serão configurados.

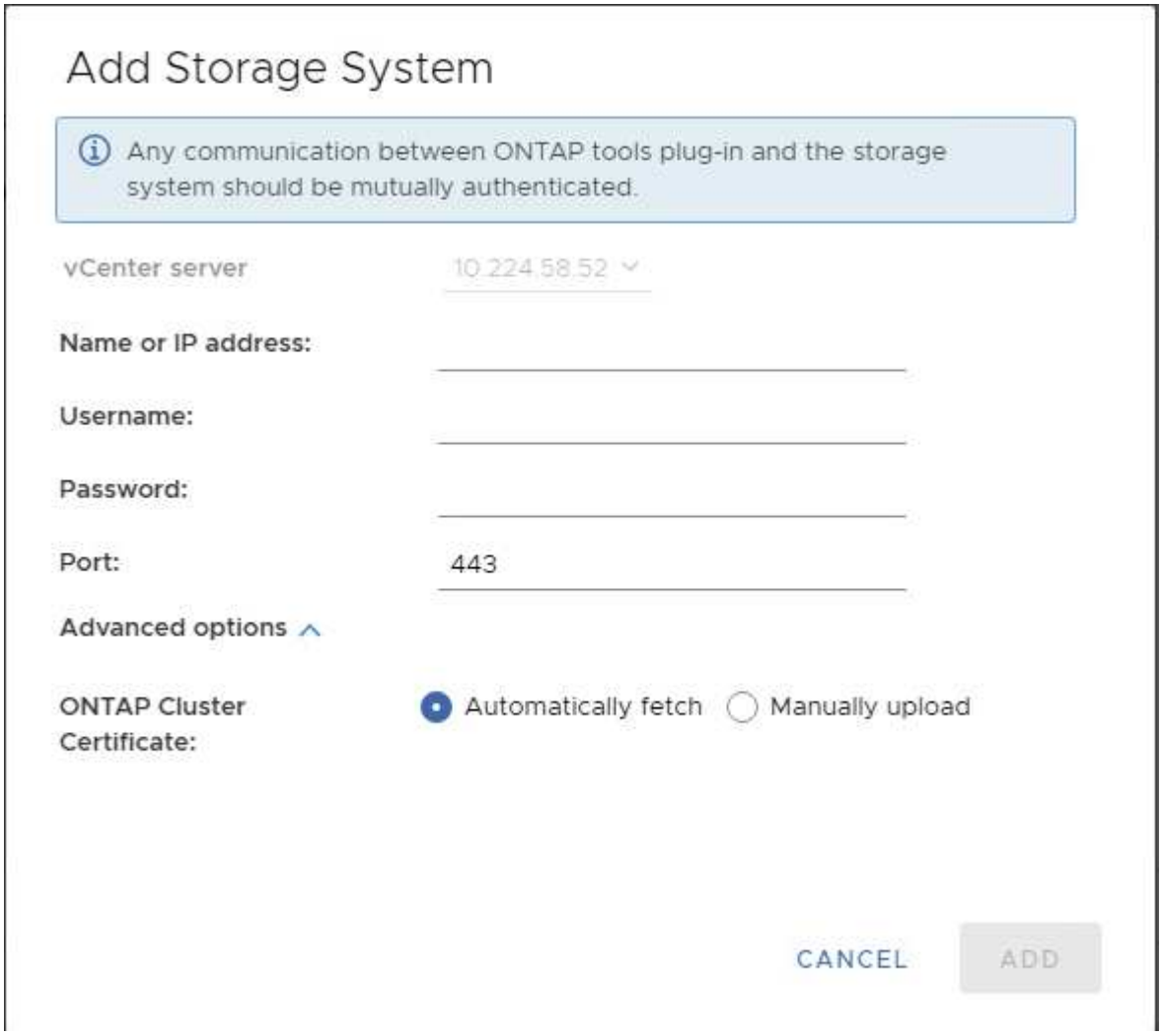
Como na captura de tela abaixo, a página de configuração do cluster mostrará o status de TLS mútuo (autenticação baseada em certificado), configurado para cada cluster.

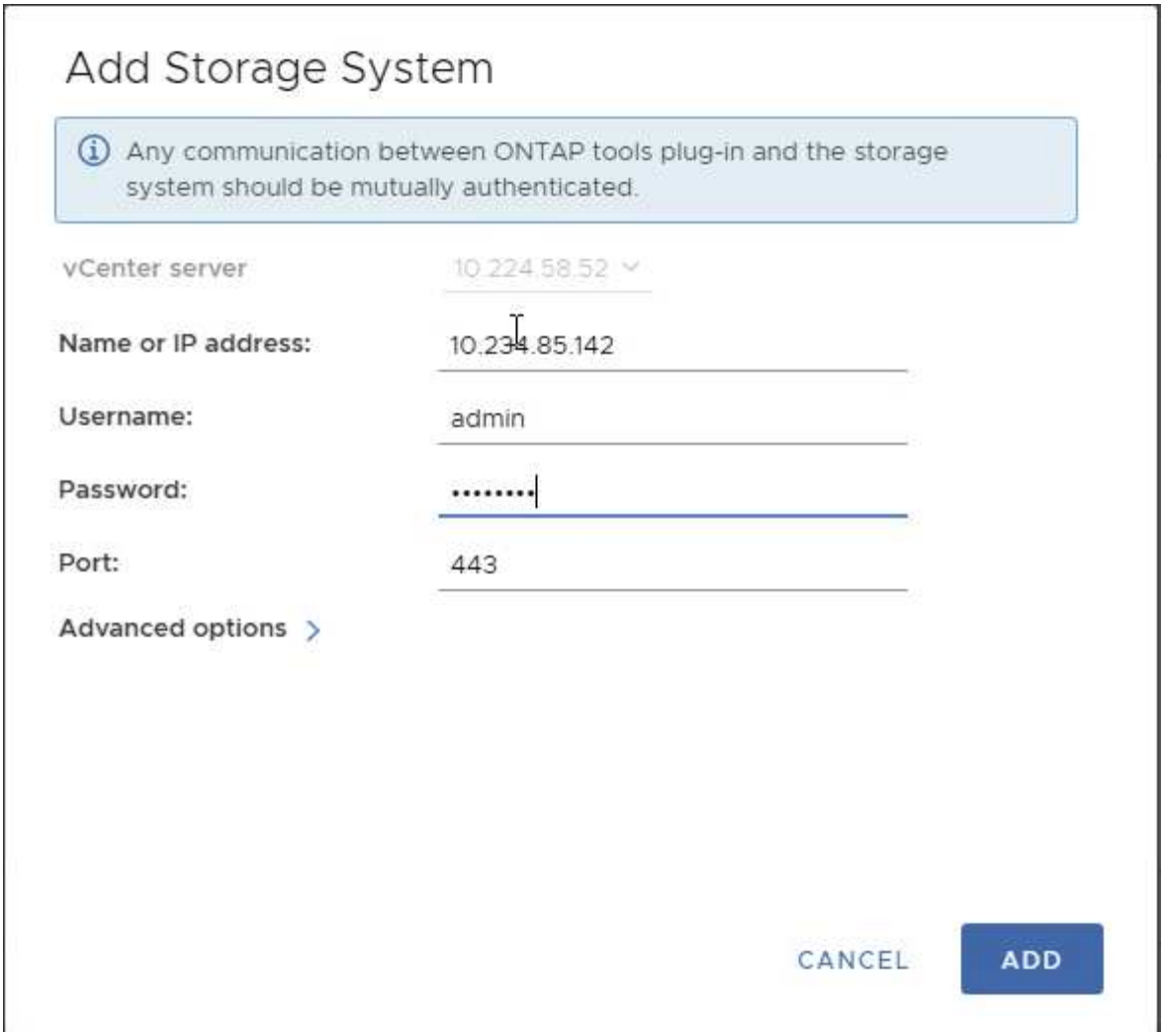


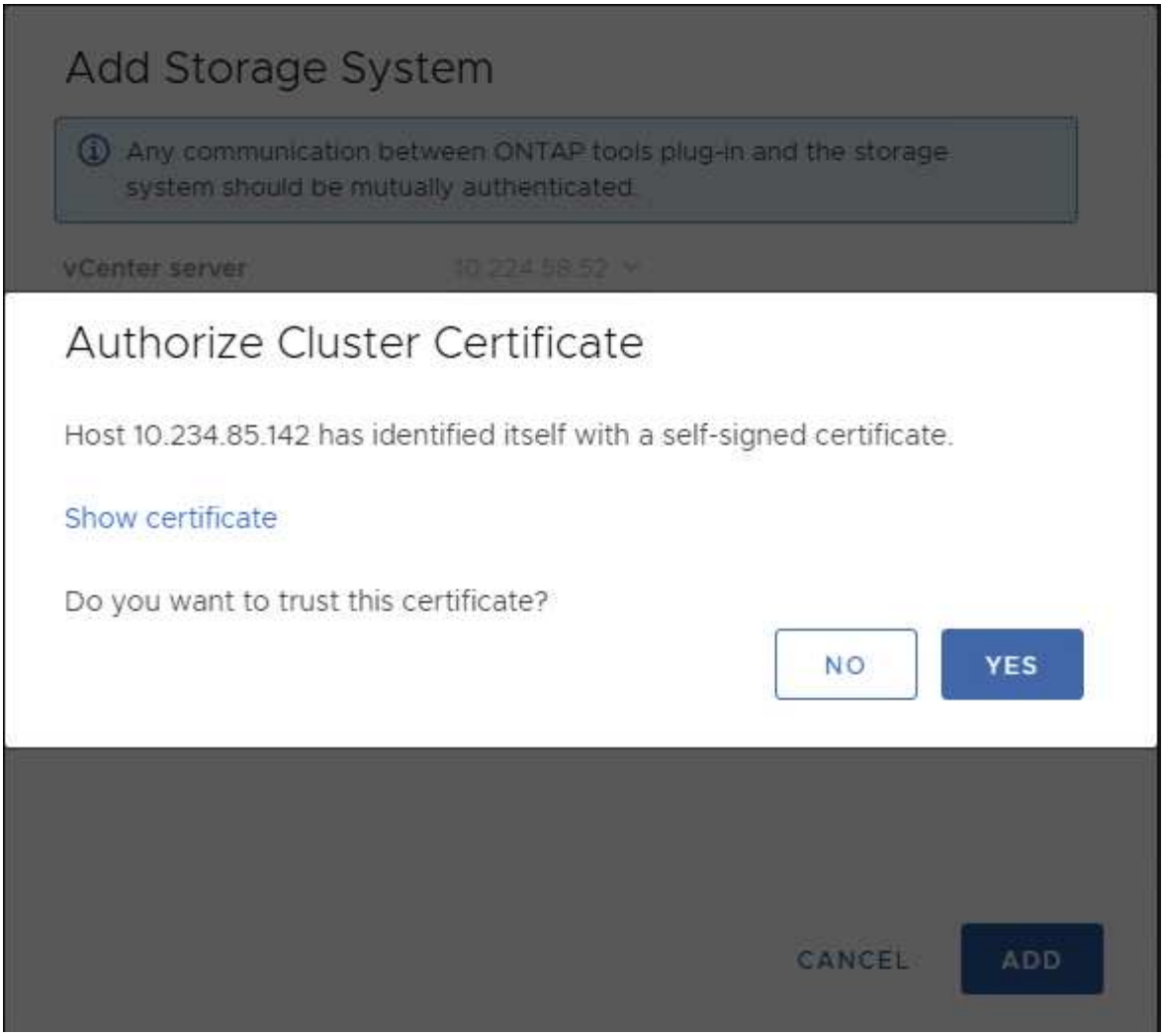
Cluster Add

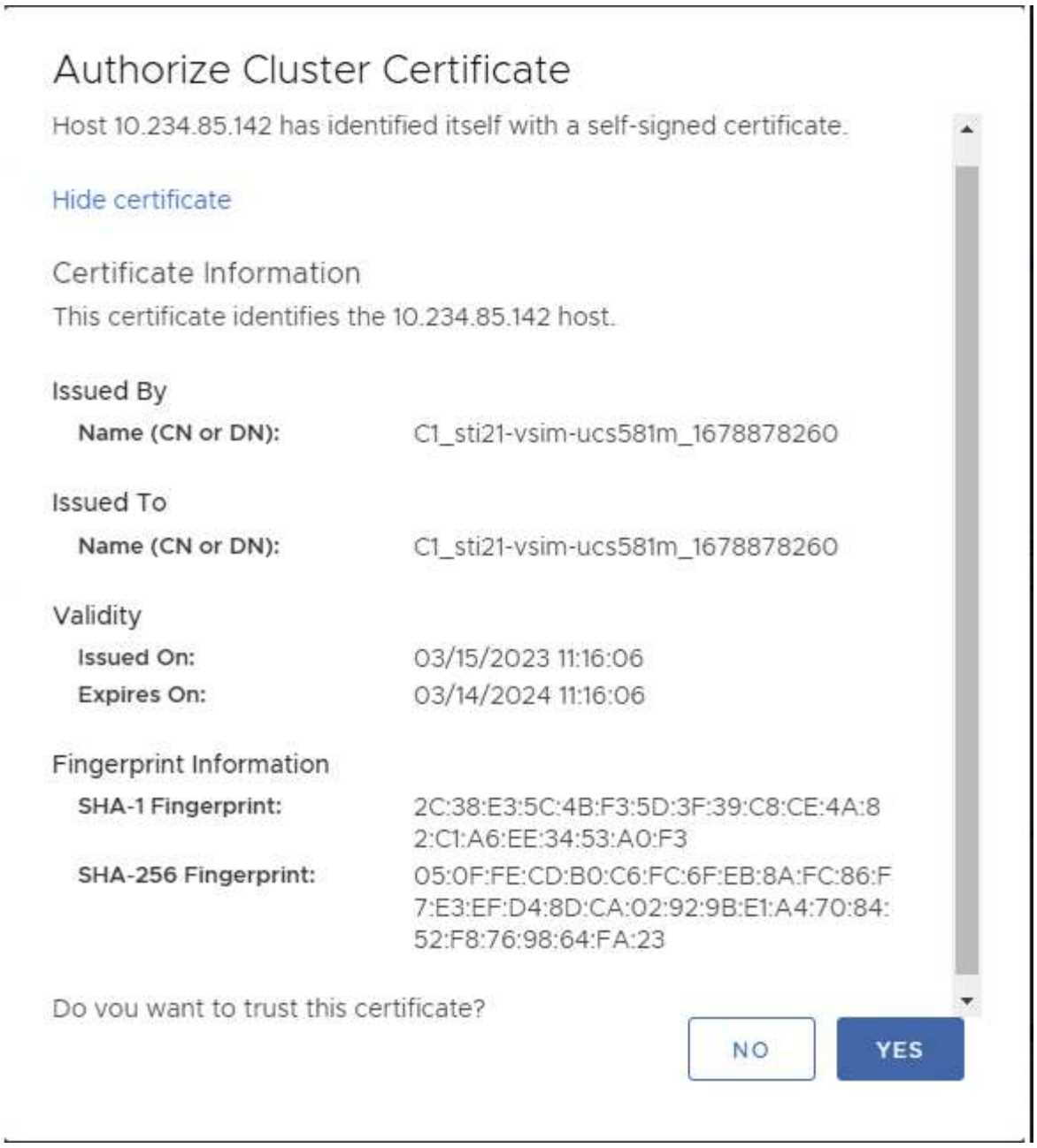
Durante o fluxo de trabalho de adição de cluster, se o cluster que está sendo adicionado suportar MTLS, o MTLS será configurado por padrão. O usuário não precisa fazer nenhuma configuração para isso. A captura

de tela abaixo mostra a tela apresentada ao usuário durante a adição do cluster.




Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
10.224.58.52
Name or IP address:
10.234.85.142
Username:
admin
Password:
Port:
443
Advanced options
CANCEL
ADD

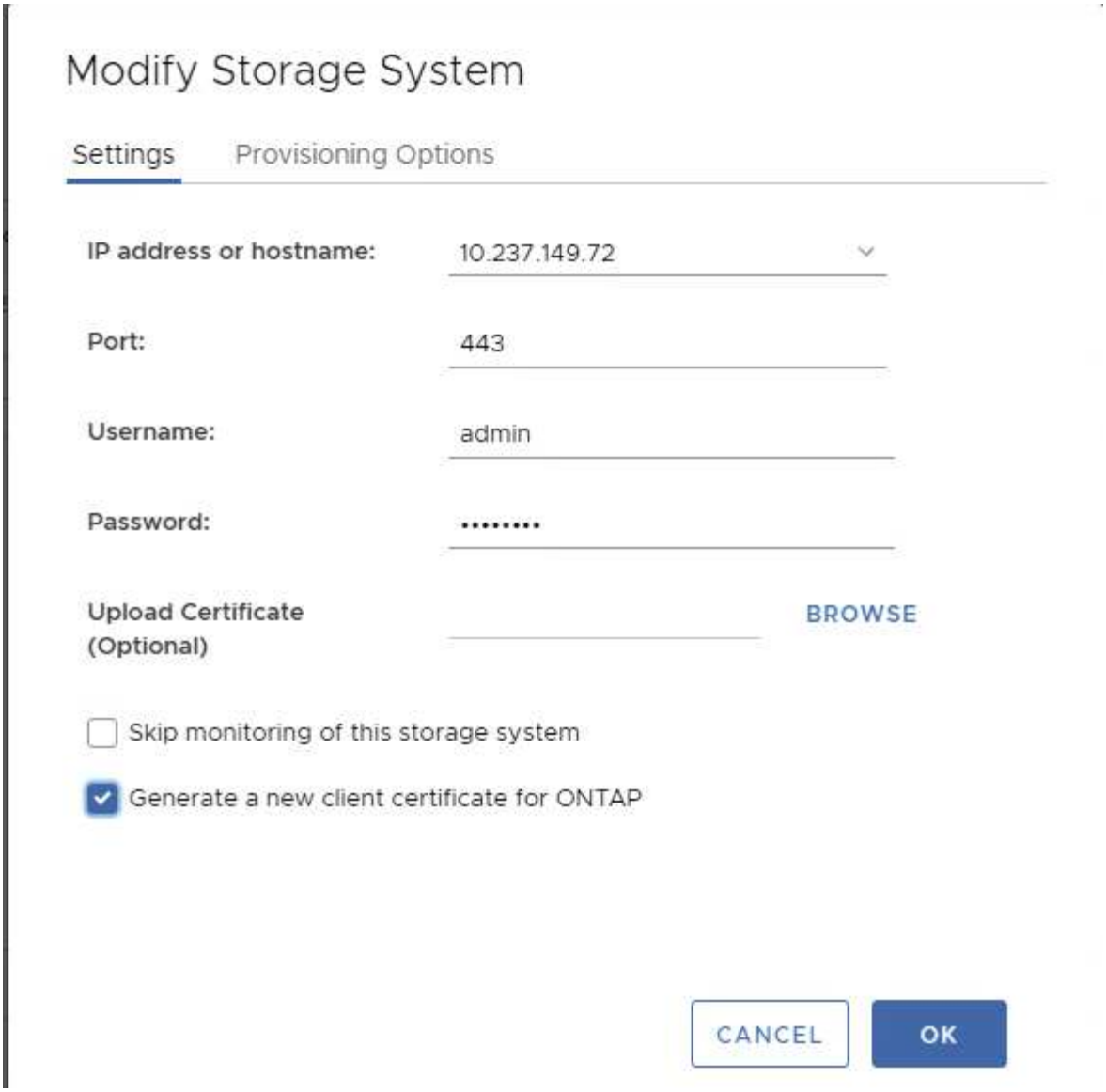

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
Authorize Cluster Certificate
Host 10.234.85.142 has identified itself with a self-signed certificate.
Show certificate
Do you want to trust this certificate?
NO
YES
CANCEL
ADD

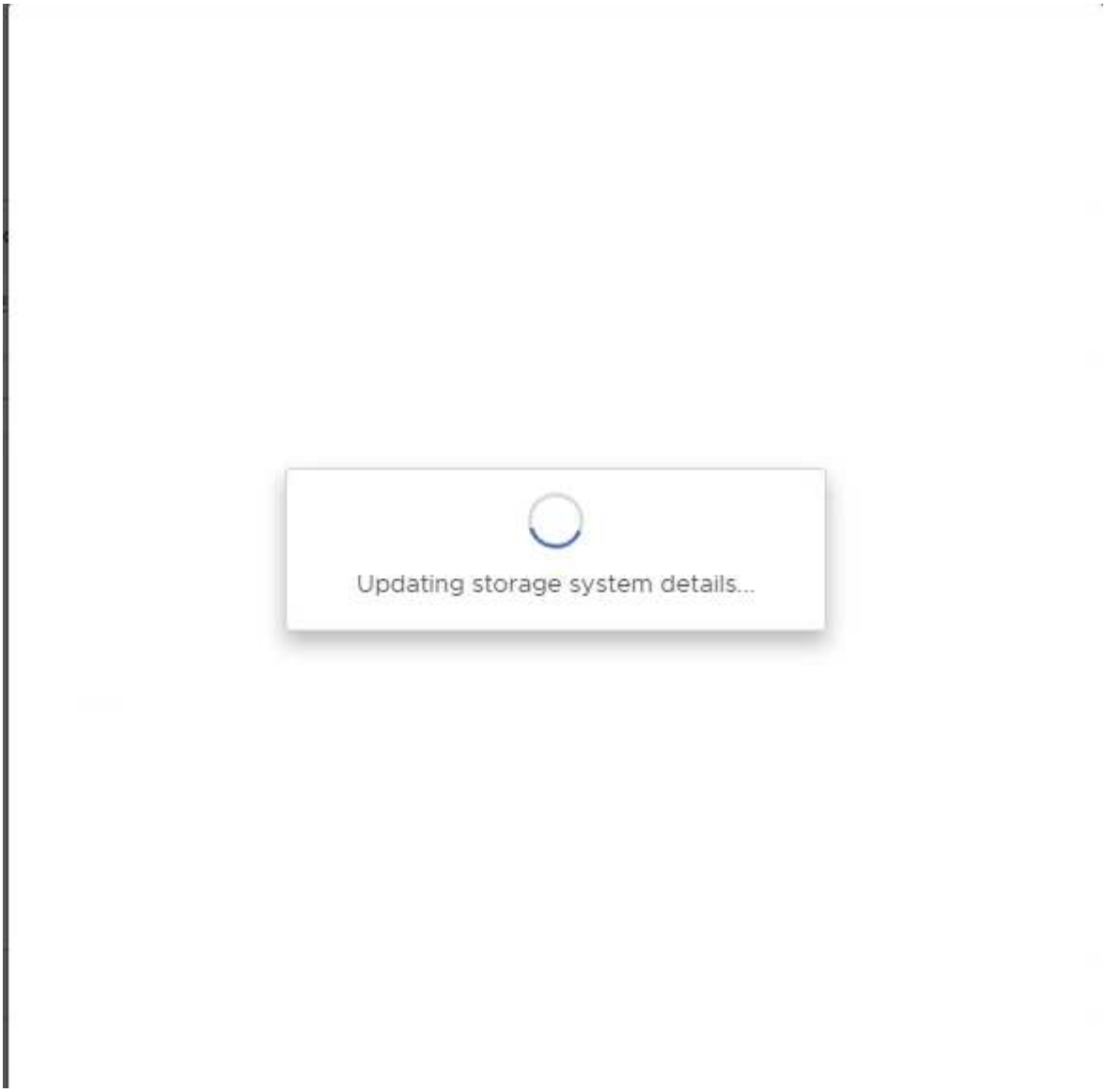


Cluster Edit (Editar cluster)

Durante a operação de edição de cluster, existem dois cenários:

- Se o certificado ONTAP expirar, o usuário terá que obter o novo certificado e enviá-lo.
- Se o certificado OTV expirar, o usuário pode regenerá-lo marcando a caixa de seleção.
  - *Gerar um novo certificado de cliente para o ONTAP.*


Modify Storage System
Settings
Provisioning Options
IP address or hostname:
10.237.149.72
Port:
443
Username:
admin
Password:
Upload Certificate (Optional)
BROWSE
Skip monitoring of this storage system
Generate a new client certificate for ONTAP
CANCEL
OK



Certificado HTTPS de 9,13 das ferramentas ONTAP

Por padrão, as ferramentas do ONTAP usam um certificado autoassinado criado automaticamente durante a instalação para proteger o acesso HTTPS à IU da Web. As ferramentas do ONTAP oferecem os seguintes recursos:

1. Regenere o certificado HTTPS

Durante a instalação das ferramentas do ONTAP, um certificado de CA HTTPS é instalado e o certificado é armazenado no keystore. O usuário tem a opção de regenerar o certificado HTTPS por meio do console de manutenção.

As opções acima podem ser acessadas no console *mant* navegando até *'Application Configuration'* → *'Re-Generate certificates'.*

ONTAP Tools 9,13 banner de login

O banner de login a seguir é exibido depois que o usuário insere um nome de usuário no

prompt de login. Observe que o SSH está desativado por padrão e permite somente logins únicos quando habilitado a partir do console da VM.

```
WARNING: Unauthorized access to this system is forbidden and will be
prosecuted by law. By accessing this system, you agree that your actions
may be monitored if unauthorized usage is suspected.
```

Depois que o usuário concluir o login através do canal SSH, o seguinte texto é exibido:

```
Linux UnifiedVSC 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21)
x86_64
```

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

Tempo limite de inatividade para ferramentas ONTAP 9,13

Para impedir o acesso não autorizado, é configurado um tempo limite de inatividade, que faz logout automaticamente de usuários inativos por um determinado período durante o uso de recursos autorizados. Isso garante que somente usuários autorizados possam acessar os recursos e ajuda a manter a segurança.

- Por padrão, as sessões do vSphere Client são encerradas após 120 minutos de tempo ocioso, exigindo que o usuário faça login novamente para continuar usando o cliente. Você pode alterar o valor do tempo limite editando o arquivo webclient.properties.você pode configurar o tempo limite do vSphere Client "Configure o valor de tempo limite do vSphere Client"
- As ferramentas do ONTAP têm um tempo de logout de sessão da web-cli de 30 minutos.

Máximo de solicitações simultâneas por usuário (Network security protection/dos Attack) Ferramentas do ONTAP para VMware vSphere 9,13

Por padrão, o número máximo de solicitações simultâneas por usuário é 48. O usuário raiz nas ferramentas do ONTAP pode alterar esse valor dependendo dos requisitos de seu ambiente. **Este valor não deve ser definido para um valor muito alto, pois isso fornece um mecanismo contra ataques de negação de serviço (dos).**

Os usuários podem alterar o número máximo de sessões simultâneas e outros parâmetros suportados no arquivo ***/opt/NetApp/vscserver/etc/dosfilterParams.json***.

Podemos configurar o filtro seguindo os seguintes parâmetros:

- ***delayMS***: O atraso em milissegundos dado a todas as solicitações acima do limite de taxa antes de serem consideradas. Dê -1 apenas para rejeitar o pedido.
- ***estrangulems***: Quanto tempo para sincronizar a espera pelo semáforo.
- ***maxRequestMs***: Quanto tempo para permitir que essa solicitação seja executada.
- ***ipWhitelist***: Uma lista separada por vírgulas de endereços IP que não serão limitados por taxa. (Isso pode ser vCenter, ESXi e SRA IPs)
- ***maxRequestsPerSec***: O número máximo de solicitações de uma conexão por segundo.

Valores padrão no arquivo *dosfilterParams*:

```
{"delayMs":"-1",
"throttleMs":"1800000",
"maxRequestMs":"300000",
"ipWhitelist":"10.224.58.52",
"maxRequestsPerSec":"48"}
```

Configuração do protocolo de tempo de rede (NTP) para ferramentas ONTAP 9,13

Às vezes, problemas de segurança podem ocorrer devido a discrepâncias nas configurações de tempo de rede. É importante garantir que todos os dispositivos dentro de uma rede tenham configurações de tempo precisas para evitar esses problemas.

Virtual Appliance

Você pode configurar o(s) servidor(s) NTP a partir do console de manutenção no dispositivo virtual. Os usuários podem adicionar os detalhes do servidor NTP em *Configuração do sistema> Adicionar novo servidor NTP* opção

Por padrão, o serviço para NTP é ntpd. Este é um serviço legado e não funciona bem para máquinas virtuais em certos casos.

Debian

No Debian, o usuário pode acessar o arquivo /etc/NTP.conf para obter detalhes do servidor ntp.

Políticas de senha para ferramentas do ONTAP 9,13

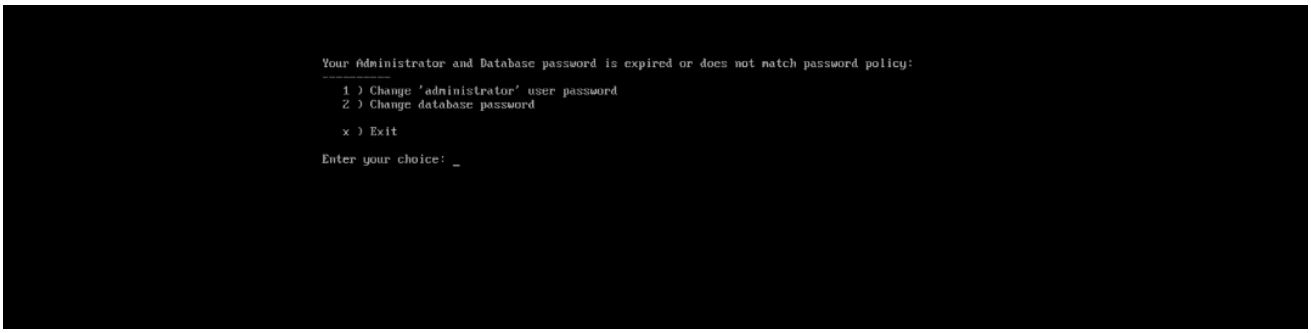
Os usuários que implantarem ferramentas do ONTAP pela primeira vez ou atualizarem para a versão 9,12 ou posterior precisarão seguir a política de senha forte para o administrador e os usuários do banco de dados. Durante o processo de implantação, novos usuários serão solicitados a inserir suas senhas. Para usuários brownfield atualizando para a versão 9,12 ou posterior, a opção de seguir a política de senha forte estará disponível no console de manutenção.

- Uma vez que o usuário faça login no console de manutenção, as senhas serão verificadas em relação ao conjunto de regras complexas e, se for encontrado que não foi seguido, o usuário será solicitado a

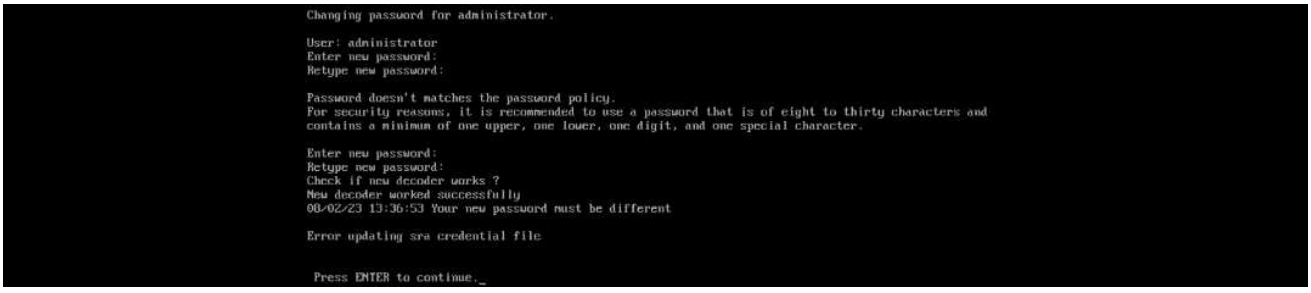
redefinir o mesmo.

- A validade padrão da senha é de 90 dias e após 75 dias o usuário começará a receber a notificação para alterar a senha.
- É necessário definir uma nova senha em cada ciclo, o sistema não receberá a última senha como a nova senha.
- Sempre que um usuário fizer login no console de manutenção, ele verificará as políticas de senha, como as capturas de tela abaixo, antes de carregar o Menu Principal:

- Se não for encontrado seguindo a política de senha ou sua configuração de atualização a partir das ferramentas ONTAP 9,11 ou antes. Em seguida, o utilizador verá o seguinte ecrã para repor a palavra-passe:



- Se o usuário tentar definir senha fraca ou fornecer a última senha novamente, o usuário verá o seguinte erro:



Informações sobre direitos autorais

Informações sobre marcas comerciais