Começar

Cloud Volumes ONTAP

NetApp
February 17, 2026

Índice

Começar

Saiba mais sobre o Cloud Volumes ONTAP

O Cloud Volumes ONTAP permite que você otimize seus custos e desempenho de armazenamento em nuvem, ao mesmo tempo em que melhora a proteção, a segurança e a conformidade dos dados.

O Cloud Volumes ONTAP é um dispositivo de armazenamento somente de software que executa o software de gerenciamento de dados ONTAP na nuvem. Ele fornece armazenamento de nível empresarial com os seguintes recursos principais:

- Eficiências de armazenamento

  Aproveite a desduplicação de dados, a compactação de dados, o provisionamento fino e a clonagem integrados para minimizar os custos de armazenamento.

- Alta disponibilidade

  Garanta a confiabilidade empresarial e operações contínuas em caso de falhas no seu ambiente de nuvem.

- Proteção de dados

  O Cloud Volumes ONTAP utiliza o SnapMirror, a tecnologia de replicação líder do setor da NetApp, para replicar dados locais para a nuvem, facilitando a disponibilidade de cópias secundárias para vários casos de uso.

  O Cloud Volumes ONTAP também se integra ao NetApp Backup and Recovery para fornecer recursos de backup e restauração para proteção e arquivamento de longo prazo dos seus dados na nuvem.

  "Saiba mais sobre backup e recuperação"

- Camadas de dados

  Alterne entre pools de armazenamento de alto e baixo desempenho sob demanda, sem deixar os aplicativos offline.

- Consistência da aplicação

  Garanta a consistência das cópias do NetApp Snapshot usando o NetApp SnapCenter.

  "Saiba mais sobre o SnapCenter"

- Segurança de dados

  O Cloud Volumes ONTAP oferece suporte à criptografia de dados e proteção contra vírus e ransomware.

- Controles de conformidade de privacidade

  A integração com a NetApp Data Classification ajuda você a entender o contexto dos dados e identificar dados confidenciais.

  "Saiba mais sobre Classificação de Dados"

Licenças para recursos do ONTAP estão incluídas no Cloud Volumes ONTAP.

"Ver configurações Cloud Volumes ONTAP suportadas"

"Saiba mais sobre o Cloud Volumes ONTAP"

Versões ONTAP suportadas para implantações do Cloud Volumes ONTAP

O NetApp Console permite que você escolha entre várias versões diferentes do ONTAP ao adicionar um sistema Cloud Volumes ONTAP .

Versões do Cloud Volumes ONTAP diferentes das listadas aqui não estão disponíveis para novas implantações. A versão de patch ou a versão genérica (Disponibilidade Geral) em uma versão aqui representa a versão base disponível para implantação. Para obter detalhes sobre os patches disponíveis, consulte a "notas de lançamento versioned" para cada versão.

Para obter informações sobre upgrade, consulte "Caminhos de atualização suportados".

AWS

Nó único

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8
- 9,7 P5
- 9,5 P6

Par HA

- 9.18.1

- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8
- 9,7 P5
- 9,5 P6

Azul

Nó único

- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

Par HA

- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

Google Cloud

Nó único

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8
- 9,7 P5

Par HA

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8

Comece na Amazon Web Services

Início rápido para Cloud Volumes ONTAP na AWS

Comece a usar o Cloud Volumes ONTAP na AWS em poucas etapas.

1 Criar um agente de console

Se você não tem um "Agente de console" no entanto, você precisa criar um. "Aprenda a criar um agente de console na AWS" .

Observe que se você quiser implantar o Cloud Volumes ONTAP em uma sub-rede onde não há acesso à Internet disponível, será necessário instalar manualmente o agente do Console e acessar a interface do usuário do NetApp Console que está em execução nesse agente do Console. "Aprenda a instalar manualmente o agente do Console em um local sem acesso à Internet" .

2 Planeje sua configuração

O Console oferece pacotes pré-configurados que correspondem aos seus requisitos de carga de trabalho, ou você pode criar sua própria configuração. Se você escolher sua própria configuração, deverá entender as opções disponíveis. "Saber mais" .

3 Configure sua rede

1. Certifique-se de que sua VPC e sub-redes oferecerão suporte à conectividade entre o agente do Console e o Cloud Volumes ONTAP.
2. Habilite o acesso de saída à Internet da VPC de destino para o NetApp AutoSupport.

   Esta etapa não é necessária se você estiver implantando o Cloud Volumes ONTAP em um local onde não há acesso à Internet disponível.

3. Configure um endpoint VPC para o serviço Amazon Simple Storage Service (Amazon S3).

   Um endpoint VPC é necessário se você quiser hierarquizar dados frios do Cloud Volumes ONTAP para armazenamento de objetos de baixo custo.

"Saiba mais sobre os requisitos de rede" .

4 Configurar o AWS KMS

Se você quiser usar a criptografia da Amazon com o Cloud Volumes ONTAP, precisará garantir que exista uma Chave Mestra do Cliente (CMK) ativa. Você também precisa modificar a política de chave para cada CMK adicionando a função do IAM que fornece permissões ao agente do Console como um *usuário de chave*. "Saber mais" .

5 Inicie o Cloud Volumes ONTAP usando o Console

Clique em **Adicionar Sistema**, selecione o tipo de sistema que você gostaria de implantar e conclua as

etapas do assistente. "Leia as instruções passo a passo" .

Links relacionados

- "Crie um agente de console para AWS"
- "Crie um agente de console no AWS Marketplace"
- "Instalar e configurar um agente do Console no local"
- "Permissões da AWS para o agente do Console"

Planeje sua configuração do Cloud Volumes ONTAP na AWS

Ao implantar o Cloud Volumes ONTAP na AWS, você pode escolher um sistema pré-configurado que corresponda aos seus requisitos de carga de trabalho ou pode criar sua própria configuração. Se você escolher sua própria configuração, deverá entender as opções disponíveis.

Escolha uma licença do Cloud Volumes ONTAP

Várias opções de licenciamento estão disponíveis para o Cloud Volumes ONTAP. Cada opção permite que você escolha um modelo de consumo que atenda às suas necessidades.

- "Saiba mais sobre as opções de licenciamento do Cloud Volumes ONTAP"
- "Aprenda como configurar o licenciamento"

Escolha uma região com suporte

O Cloud Volumes ONTAP é suportado na maioria das regiões da AWS. "Veja a lista completa de regiões suportadas" .

Regiões mais recentes da AWS devem ser habilitadas antes que você possa criar e gerenciar recursos nessas regiões. "Documentação da AWS: Aprenda como habilitar uma região" .

Escolha uma Zona Local com suporte

Selecionar uma Zona Local é opcional. O Cloud Volumes ONTAP é suportado em algumas zonas locais da AWS, incluindo Cingapura. O Cloud Volumes ONTAP na AWS oferece suporte apenas ao modo de alta disponibilidade (HA) em uma única zona de disponibilidade. Implantações de nó único não são suportadas.

> O Cloud Volumes ONTAP não oferece suporte para camadas de dados e camadas de nuvem em zonas locais da AWS. Além disso, zonas locais com instâncias que não foram qualificadas para o Cloud Volumes ONTAP não são suportadas. Um exemplo disso é Miami, que não está disponível como uma Zona Local, porque tem apenas instâncias Gen6 que não são suportadas e não qualificadas.

"Documentação da AWS: Veja a lista completa de Zonas Locais" . As Zonas Locais devem ser habilitadas antes que você possa criar e gerenciar recursos nessas zonas.

"Documentação da AWS: Introdução às Zonas Locais da AWS" .

Escolha uma instância suportada

O Cloud Volumes ONTAP oferece suporte a vários tipos de instância, dependendo do tipo de licença

escolhido.

"Configurações com suporte para Cloud Volumes ONTAP na AWS"

Entenda os limites de armazenamento

O limite de capacidade bruta para um sistema Cloud Volumes ONTAP está vinculado à licença. Limites adicionais afetam o tamanho dos agregados e volumes. Você deve estar ciente desses limites ao planejar sua configuração.

"Limites de armazenamento para Cloud Volumes ONTAP na AWS"

Dimensione seu sistema na AWS

Dimensionar seu sistema Cloud Volumes ONTAP pode ajudar você a atender aos requisitos de desempenho e capacidade. Você deve estar ciente de alguns pontos importantes ao escolher um tipo de instância, tipo de disco e tamanho de disco:

Tipo de instância

- Adapte seus requisitos de carga de trabalho ao rendimento máximo e IOPS para cada tipo de instância EC2.
- Se vários usuários gravarem no sistema ao mesmo tempo, escolha um tipo de instância que tenha CPUs suficientes para gerenciar as solicitações.
- Se você tem um aplicativo que é lido com frequência, escolha um sistema com RAM suficiente.
  - "Documentação da AWS: Tipos de instância do Amazon EC2"
  - "Documentação da AWS: Instâncias otimizadas para Amazon EBS"

Tipo de disco EBS

Em um nível mais alto, as diferenças entre os tipos de disco EBS são as seguintes. Para saber mais sobre os casos de uso de discos EBS, consulte "Documentação da AWS: Tipos de volume do EBS" .

- Os discos *SSD de uso geral (gp3)* são os SSDs de menor custo que equilibram custo e desempenho para uma ampla gama de cargas de trabalho. O desempenho é definido em termos de IOPS e taxa de transferência. Os discos gp3 são suportados com o Cloud Volumes ONTAP 9.7 e posteriores.

  Quando você seleciona um disco gp3, o NetApp Console preenche os valores padrão de IOPS e taxa de transferência que fornecem desempenho equivalente a um disco gp2 com base no tamanho do disco selecionado. Você pode aumentar os valores para obter melhor desempenho a um custo mais alto, mas não oferecemos suporte a valores menores porque isso pode resultar em desempenho inferior. Resumindo, mantenha os valores padrões ou aumente-os. Não os abaixe. "Documentação da AWS: Saiba mais sobre discos gp3 e seu desempenho" .

  Observe que o Cloud Volumes ONTAP oferece suporte ao recurso Amazon EBS Elastic Volumes com discos gp3. "Saiba mais sobre o suporte do Elastic Volumes" .

- Os discos *SSD de uso geral (gp2)* equilibram custo e desempenho para uma ampla gama de cargas de trabalho. O desempenho é definido em termos de IOPS.
- Os discos *Provisioned IOPS SSD (io1)* são para aplicativos críticos que exigem o mais alto desempenho a um custo mais alto.

  Observe que o Cloud Volumes ONTAP oferece suporte ao recurso Amazon EBS Elastic Volumes com discos io1. "Saiba mais sobre o suporte do Elastic Volumes" .

- Os discos *Throughput Optimized HDD (st1)* são para cargas de trabalho acessadas com frequência que exigem throughput rápido e consistente a um preço mais baixo.

> O armazenamento em camadas de dados no Amazon Simple Storage Service (Amazon S3) não é compatível se o seu sistema Cloud Volumes ONTAP estiver em uma AWS Local Zone, pois o acesso aos buckets do Amazon S3 fora da Local Zone envolve maior latência e impacta as atividades do Cloud Volumes ONTAP.

Tamanho do disco EBS

Se você escolher uma configuração que não suporte o"Recurso de volumes elásticos do Amazon EBS" , então você precisa escolher um tamanho de disco inicial ao iniciar um sistema Cloud Volumes ONTAP . Depois disso, você pode"deixe o Console gerenciar a capacidade de um sistema para você" , mas se você quiser"crie agregados você mesmo" , esteja ciente do seguinte:

- Todos os discos em um agregado devem ter o mesmo tamanho.
- O desempenho dos discos EBS está vinculado ao tamanho do disco. O tamanho determina o IOPS de base e a duração máxima de burst para discos SSD e a taxa de transferência de base e burst para discos HDD.
- No final das contas, você deve escolher o tamanho do disco que lhe dará o *desempenho sustentado* que você precisa.
- Mesmo se você escolher discos maiores (por exemplo, seis discos de 4 TiB), talvez não obtenha todos os IOPS porque a instância EC2 pode atingir seu limite de largura de banda.

  Para obter mais detalhes sobre o desempenho do disco EBS, consulte "Documentação da AWS: Tipos de volume do EBS" .

  Conforme observado acima, a escolha de um tamanho de disco não é suportada com configurações do Cloud Volumes ONTAP que suportam o recurso Amazon EBS Elastic Volumes. "Saiba mais sobre o suporte do Elastic Volumes" .

Exibir discos de sistema padrão

Além do armazenamento para dados do usuário, o Console também adquire armazenamento em nuvem para dados do sistema Cloud Volumes ONTAP (dados de inicialização, dados raiz, dados principais e NVRAM). Para fins de planejamento, pode ser útil revisar esses detalhes antes de implantar o Cloud Volumes ONTAP.

"Visualizar os discos padrão para dados do sistema Cloud Volumes ONTAP na AWS" .

> O agente do Console também requer um disco do sistema. "Exibir detalhes sobre a configuração padrão do agente do Console" .

Preparar para implantar o Cloud Volumes ONTAP em um AWS Outpost

Se você tiver um AWS Outpost, poderá implantar o Cloud Volumes ONTAP nesse Outpost selecionando a VPC do Outpost durante o processo de implantação. A experiência é a mesma de qualquer outra VPC que reside na AWS. Observe que você precisará primeiro implantar um agente de console no seu AWS Outpost.

Há algumas limitações a serem apontadas:

- Somente sistemas Cloud Volumes ONTAP de nó único são suportados no momento

- As instâncias do EC2 que você pode usar com o Cloud Volumes ONTAP são limitadas ao que está disponível no seu Outpost
- Somente SSDs de uso geral (gp2) são suportados no momento

Coletar informações de rede

Ao iniciar o Cloud Volumes ONTAP na AWS, você precisa especificar detalhes sobre sua rede VPC. Você pode usar uma planilha para coletar informações do seu administrador.

Nó único ou par HA em uma única AZ

Informações da AWS	Seu valor
Região	
VPC	
Sub-rede	
Grupo de segurança (se estiver usando o seu próprio)	

Par HA em múltiplas AZs

Informações da AWS	Seu valor
Região	
VPC	
Grupo de segurança (se estiver usando o seu próprio)	
Zona de disponibilidade do nó 1	
Sub-rede do nó 1	
Zona de disponibilidade do nó 2	
Sub-rede do nó 2	
Zona de disponibilidade do mediador	
Sub-rede do mediador	
Par de chaves para o mediador	
Endereço IP flutuante para porta de gerenciamento de cluster	
Endereço IP flutuante para dados no nó 1	
Endereço IP flutuante para dados no nó 2	
Tabelas de rotas para endereços IP flutuantes	

Escolha uma velocidade de gravação

O Console permite que você escolha uma configuração de velocidade de gravação para o Cloud Volumes ONTAP. Antes de escolher uma velocidade de gravação, você deve entender as diferenças entre as configurações normal e alta, bem como os riscos e recomendações ao usar alta velocidade de gravação. "Saiba mais sobre velocidade de gravação" .

Escolha um perfil de uso de volume

O ONTAP inclui vários recursos de eficiência de armazenamento que podem reduzir a quantidade total de armazenamento necessária. Ao criar um volume no Console, você pode escolher um perfil que habilite esses recursos ou um perfil que os desabilite. Você deve aprender mais sobre esses recursos para ajudar a decidir qual perfil usar.

Os recursos de eficiência de armazenamento da NetApp oferecem os seguintes benefícios:

Provisionamento fino
: Apresenta mais armazenamento lógico para hosts ou usuários do que você realmente tem em seu pool de armazenamento físico. Em vez de pré-alocar espaço de armazenamento, o espaço de armazenamento é alocado dinamicamente para cada volume à medida que os dados são gravados.

Desduplicação
: Melhora a eficiência localizando blocos idênticos de dados e substituindo-os por referências a um único bloco compartilhado. Essa técnica reduz os requisitos de capacidade de armazenamento eliminando blocos redundantes de dados que residem no mesmo volume.

Compressão
: Reduz a capacidade física necessária para armazenar dados compactando dados dentro de um volume no armazenamento primário, secundário e de arquivo.

Configure sua rede

Configurar a rede AWS para o Cloud Volumes ONTAP

O NetApp Console gerencia a configuração de componentes de rede para o Cloud Volumes ONTAP, como endereços IP, máscaras de rede e rotas. Você precisa ter certeza de que o acesso de saída à Internet esteja disponível, que endereços IP privados suficientes estejam disponíveis, que as conexões corretas estejam em vigor e muito mais.

Requisitos gerais

Certifique-se de ter atendido aos seguintes requisitos na AWS.

Acesso de saída à Internet para nós do Cloud Volumes ONTAP

Os sistemas Cloud Volumes ONTAP exigem acesso de saída à Internet para acessar endpoints externos para diversas funções. O Cloud Volumes ONTAP não poderá operar corretamente se esses endpoints estiverem bloqueados em ambientes com requisitos de segurança rigorosos.

O agente do Console entra em contato com vários endpoints para operações diárias. Para obter informações sobre os pontos de extremidade usados, consulte "Exibir endpoints contatados pelo agente do Console" e "Preparar a rede para usar o Console" .

Pontos de extremidade Cloud Volumes ONTAP

O Cloud Volumes ONTAP usa esses endpoints para se comunicar com vários serviços.

Pontos finais	Aplicável para	Propósito	Modos de implantação	Impacto se o ponto final não estiver disponível
\ https://netapp-cloud-account.auth0.com	Autenticação	Usado para autenticação no Console.	Modos padrão e restrito.	A autenticação do usuário falha e os seguintes serviços permanecem indisponíveis: • Serviços Cloud Volumes ONTAP • Serviços ONTAP • Protocolos e serviços de proxy
\ https://api.bluexp.netapp.com/tenancy	Arrendamento	Usado para recuperar o recurso Cloud Volumes ONTAP do Console para autorizar recursos e usuários.	Modos padrão e restrito.	Os recursos do Cloud Volumes ONTAP e os usuários não estão autorizados.
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Usado para enviar dados de telemetria do AutoSupport para o suporte da NetApp .	Modos padrão e restrito.	As informações do AutoSupport continuam não entregues.

Pontos finais	Aplicável para	Propósito	Modos de implantação	Impacto se o ponto final não estiver disponível
O ponto final comercial exato para o serviço AWS (com sufixo `amazonaws.com`) depende da região da AWS que você está usando. Consulte o "Documentação da AWS para detalhes" .	• CloudFormation • Nuvem de Computação Elástica (EC2) • Gerenciamento de Identidade e Acesso (IAM) • Serviço de Gerenciamento de Chaves (KMS) • Serviço de Token de Segurança (STS) • Amazon Simple Storage Service (S3)	Comunicação com serviços da AWS.	Modos padrão e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço da AWS para executar operações específicas na AWS.
O ponto de extremidade governamental exato para o serviço da AWS depende da região da AWS que você está usando. Os pontos finais são sufixados com `amazonaws.com` e `c2s.ic.gov` . Consulte "SDK da AWS" e "Documentação da AWS" para maiores informações.	• CloudFormation • Nuvem de Computação Elástica (EC2) • Gerenciamento de Identidade e Acesso (IAM) • Serviço de Gerenciamento de Chaves (KMS) • Serviço de Token de Segurança (STS) • Serviço de Armazenamento Simples (S3)	Comunicação com serviços da AWS.	Modo restrito.	O Cloud Volumes ONTAP não pode se comunicar com o serviço da AWS para executar operações específicas na AWS.

Acesso de saída à Internet para o mediador HA

A instância do mediador HA deve ter uma conexão de saída com o serviço AWS EC2 para que possa auxiliar no failover de armazenamento. Para fornecer a conexão, você pode adicionar um endereço IP público, especificar um servidor proxy ou usar uma opção manual.

A opção manual pode ser um gateway NAT ou um endpoint VPC de interface da sub-rede de destino para o serviço AWS EC2. Para obter detalhes sobre os endpoints VPC, consulte o "Documentação da AWS: Interface VPC Endpoints (AWS PrivateLink)" .

Configuração de proxy de rede do agente do NetApp Console

Você pode usar a configuração de servidores proxy do agente do NetApp Console para habilitar o acesso de saída à Internet do Cloud Volumes ONTAP. O Console suporta dois tipos de proxies:

- **Proxy explícito**: O tráfego de saída do Cloud Volumes ONTAP usa o endereço HTTP do servidor proxy especificado durante a configuração de proxy do agente do Console. O administrador também pode ter configurado credenciais de usuário e certificados de CA raiz para autenticação adicional. Se um certificado de CA raiz estiver disponível para o proxy explícito, certifique-se de obter e carregar o mesmo certificado para o seu sistema Cloud Volumes ONTAP usando o "ONTAP CLI: instalação do certificado de segurança" comando.
- **Proxy transparente**: A rede está configurada para rotear automaticamente o tráfego de saída do Cloud Volumes ONTAP por meio do proxy para o agente do Console. Ao configurar um proxy transparente, o administrador precisa fornecer apenas um certificado de CA raiz para conectividade do Cloud Volumes ONTAP, não o endereço HTTP do servidor proxy. Certifique-se de obter e carregar o mesmo certificado de CA raiz para o seu sistema Cloud Volumes ONTAP usando o "ONTAP CLI: instalação do certificado de segurança" comando.

Para obter informações sobre como configurar servidores proxy, consulte o "Configurar o agente do Console para usar um servidor proxy" .

Endereços IP privados

O Console aloca automaticamente o número necessário de endereços IP privados para o Cloud Volumes ONTAP. Você precisa garantir que sua rede tenha endereços IP privados suficientes disponíveis.

O número de LIFs que o Console aloca para Cloud Volumes ONTAP depende de se você implanta um sistema de nó único ou um par de HA. Uma LIF é um endereço IP associado a uma porta física.

Endereços IP para um sistema de nó único

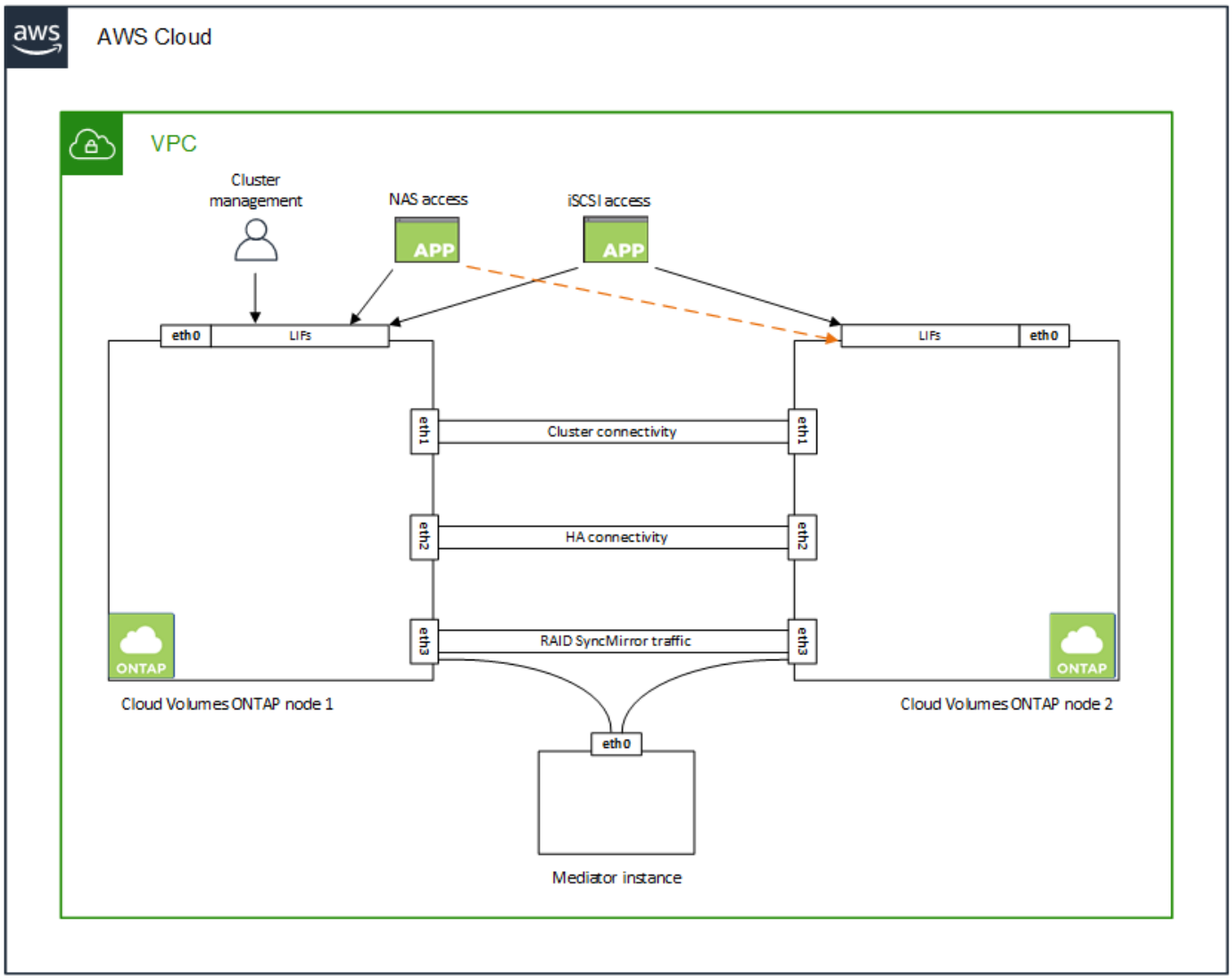
O Console aloca 6 endereços IP para um sistema de nó único.

A tabela a seguir fornece detalhes sobre os LIFs associados a cada endereço IP privado.

LIF	Propósito
Gerenciamento de cluster	Gerenciamento administrativo de todo o cluster (par HA).
Gerenciamento de nós	Gerenciamento administrativo de um nó.
Interaglomerado	Comunicação entre clusters, backup e replicação.
Dados NAS	Acesso do cliente por meio de protocolos NAS.
Dados iSCSI	Acesso do cliente através do protocolo iSCSI. Também usado pelo sistema para outros fluxos de trabalho de rede importantes. Este LIF é necessário e não deve ser excluído.
Gerenciamento de VM de armazenamento	Um LIF de gerenciamento de VM de armazenamento é usado com ferramentas de gerenciamento como o SnapCenter.

Endereços IP para pares HA

Os pares de HA requerem mais endereços IP do que um sistema de nó único. Esses endereços IP são distribuídos por diferentes interfaces ethernet, conforme mostrado na imagem a seguir:



O número de endereços IP privados necessários para um par de HA depende do modelo de implantação escolhido. Um par de HA implantado em uma *única* Zona de Disponibilidade (AZ) da AWS requer 15 endereços IP privados, enquanto um par de HA implantado em *várias* AZs requer 13 endereços IP privados.

As tabelas a seguir fornecem detalhes sobre os LIFs associados a cada endereço IP privado.

LIF	Interface	Nó	Propósito
Gerenciamento de cluster	eth0	nó 1	Gerenciamento administrativo de todo o cluster (par HA).
Gerenciamento de nós	eth0	nó 1 e nó 2	Gerenciamento administrativo de um nó.
Interaglomerado	eth0	nó 1 e nó 2	Comunicação entre clusters, backup e replicação.

LIF	Interface	Nó	Propósito
Dados NAS	eth0	nó 1	Acesso do cliente por meio de protocolos NAS.
Dados iSCSI	eth0	nó 1 e nó 2	Acesso do cliente através do protocolo iSCSI. Também usado pelo sistema para outros fluxos de trabalho de rede importantes. Esses LIFs são necessários e não devem ser excluídos.
Conectividade de cluster	eth1	nó 1 e nó 2	Permite que os nós se comuniquem entre si e movam dados dentro do cluster.
Conectividade HA	eth2	nó 1 e nó 2	Comunicação entre os dois nós em caso de failover.
Tráfego RSM iSCSI	eth3	nó 1 e nó 2	Tráfego RAID SyncMirror iSCSI, bem como comunicação entre os dois nós Cloud Volumes ONTAP e o mediador.
Mediador	eth0	Mediador	Um canal de comunicação entre os nós e o mediador para auxiliar nos processos de aquisição e devolução de armazenamento.

LIF	Interface	Nó	Propósito
Gerenciamento de nós	eth0	nó 1 e nó 2	Gerenciamento administrativo de um nó.
Interaglomerado	eth0	nó 1 e nó 2	Comunicação entre clusters, backup e replicação.
Dados iSCSI	eth0	nó 1 e nó 2	Acesso do cliente através do protocolo iSCSI. Esses LIFs também gerenciam a migração de endereços IP flutuantes entre nós. Esses LIFs são necessários e não devem ser excluídos.
Conectividade de cluster	eth1	nó 1 e nó 2	Permite que os nós se comuniquem entre si e movam dados dentro do cluster.
Conectividade HA	eth2	nó 1 e nó 2	Comunicação entre os dois nós em caso de failover.
Tráfego RSM iSCSI	eth3	nó 1 e nó 2	Tráfego RAID SyncMirror iSCSI, bem como comunicação entre os dois nós Cloud Volumes ONTAP e o mediador.
Mediador	eth0	Mediador	Um canal de comunicação entre os nós e o mediador para auxiliar nos processos de aquisição e devolução de armazenamento.

Quando implantados em várias Zonas de Disponibilidade, vários LIFs são associados a"endereços IP flutuantes" , que não contam para o limite de IP privado da AWS.

Grupos de segurança

Você não precisa criar grupos de segurança porque o Console faz isso para você. Se você precisar usar o seu próprio, consulte"Regras do grupo de segurança" .

Procurando informações sobre o agente do Console? "Exibir regras de grupo de segurança para o agente do Console"

Conexão para hierarquização de dados

Se você deseja usar EBS como camada de desempenho e Amazon S3 como camada de capacidade, é necessário garantir que Cloud Volumes ONTAP tenha uma conexão com o S3. A melhor maneira de fornecer essa conexão é criando um endpoint de VPC para o serviço S3. Para obter instruções, consulte a "Documentação da AWS: Criando um endpoint de gateway".

Ao criar o VPC Endpoint, certifique-se de selecionar a região, a VPC e a tabela de rotas que correspondem à instância do Cloud Volumes ONTAP . Você também deve modificar o grupo de segurança para adicionar uma regra HTTPS de saída que habilite o tráfego para o ponto de extremidade S3. Caso contrário, o Cloud Volumes ONTAP não poderá se conectar ao serviço S3.

Se você tiver algum problema, consulte o "Central de conhecimento do AWS Support: Por que não consigo me conectar a um bucket do S3 usando um endpoint de VPC de gateway?"

Conexões com sistemas ONTAP

Para replicar dados entre um sistema Cloud Volumes ONTAP na AWS e sistemas ONTAP em outras redes, você deve ter uma conexão VPN entre a VPC da AWS e a outra rede, por exemplo, sua rede corporativa. Para obter instruções, consulte o "Documentação da AWS: Configurando uma conexão VPN da AWS" .

DNS e Active Directory para CIFS

Se você quiser provisionar armazenamento CIFS, deverá configurar o DNS e o Active Directory na AWS ou estender sua configuração local para a AWS.

O servidor DNS deve fornecer serviços de resolução de nomes para o ambiente do Active Directory. Você pode configurar conjuntos de opções DHCP para usar o servidor DNS EC2 padrão, que não deve ser o servidor DNS usado pelo ambiente do Active Directory.

Para obter instruções, consulte o "Documentação da AWS: Serviços de Domínio do Active Directory na Nuvem AWS: Implantação de Referência de Início Rápido" .

Compartilhamento de VPC

A partir da versão 9.11.1, os pares de HA do Cloud Volumes ONTAP são suportados na AWS com compartilhamento de VPC. O compartilhamento de VPC permite que sua organização compartilhe sub-redes com outras contas da AWS. Para usar esta configuração, você deve configurar seu ambiente AWS e então implantar o par HA usando a API.

"Aprenda a implantar um par HA em uma sub-rede compartilhada" .

Requisitos para pares de HA em várias AZs

Requisitos adicionais de rede da AWS se aplicam às configurações de alta disponibilidade do Cloud Volumes ONTAP que usam várias zonas de disponibilidade (AZs). Você deve revisar esses requisitos antes de iniciar

um par de HA porque deve inserir os detalhes de rede no Console ao adicionar um sistema Cloud Volumes ONTAP .

Para entender como os pares HA funcionam, consulte"Pares de alta disponibilidade" .

Zonas de disponibilidade

Este modelo de implantação de HA usa várias AZs para garantir alta disponibilidade dos seus dados. Você deve usar uma AZ dedicada para cada instância do Cloud Volumes ONTAP e a instância do mediador, que fornece um canal de comunicação entre o par HA.

Uma sub-rede deve estar disponível em cada Zona de Disponibilidade.

Endereços IP flutuantes para dados NAS e gerenciamento de cluster/SVM

As configurações de HA em várias AZs usam endereços IP flutuantes que migram entre nós se ocorrerem falhas. Eles não são nativamente acessíveis de fora do VPC, a menos que você"configurar um gateway de trânsito da AWS" .

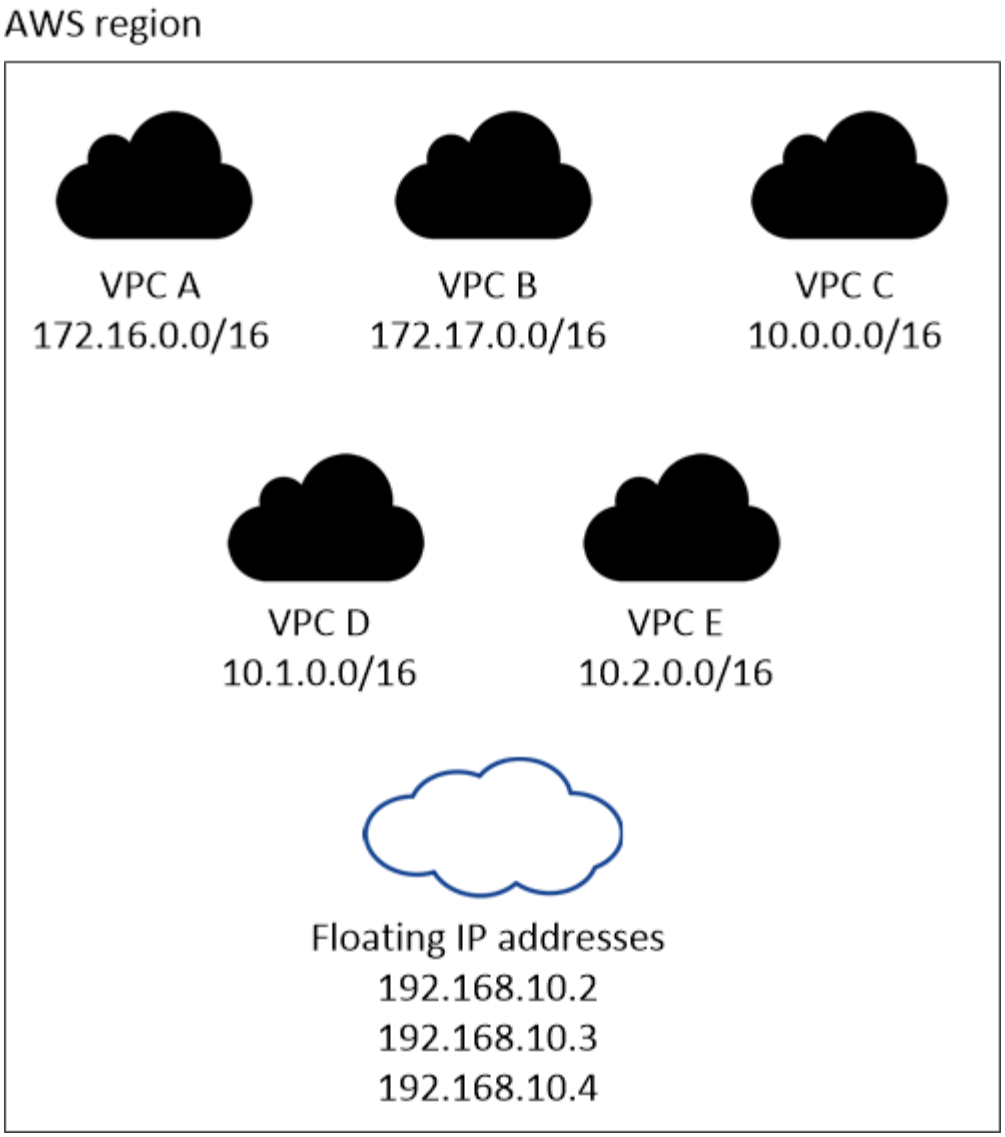
Um endereço IP flutuante é para gerenciamento de cluster, um é para dados NFS/CIFS no nó 1 e um é para dados NFS/CIFS no nó 2. Um quarto endereço IP flutuante para gerenciamento de SVM é opcional.

Um endereço IP flutuante é necessário para o LIF de gerenciamento do SVM se você usar o SnapDrive para Windows ou o SnapCenter com o par HA.

Você precisa inserir os endereços IP flutuantes ao adicionar um sistema Cloud Volumes ONTAP HA. O Console aloca os endereços IP ao par HA quando inicia o sistema.

Os endereços IP flutuantes devem estar fora dos blocos CIDR para todas as VPCs na região da AWS na qual você implanta a configuração de HA. Pense nos endereços IP flutuantes como uma sub-rede lógica que está fora das VPCs na sua região.

O exemplo a seguir mostra a relação entre endereços IP flutuantes e as VPCs em uma região da AWS. Embora os endereços IP flutuantes estejam fora dos blocos CIDR para todas as VPCs, eles podem ser roteados para sub-redes por meio de tabelas de rotas.



O Console cria automaticamente endereços IP estáticos para acesso iSCSI e para acesso NAS de clientes fora da VPC. Você não precisa atender a nenhum requisito para esses tipos de endereços IP.

Gateway de trânsito para permitir acesso IP flutuante de fora da VPC

Se necessário,"configurar um gateway de trânsito da AWS" para permitir o acesso aos endereços IP flutuantes de um par de HA de fora da VPC onde o par de HA reside.

Tabelas de rotas

Depois de especificar os endereços IP flutuantes, você será solicitado a selecionar as tabelas de rotas que devem incluir rotas para os endereços IP flutuantes. Isso permite o acesso do cliente ao par HA.

Se você tiver apenas uma tabela de rotas para as sub-redes na sua VPC (a tabela de rotas principal), o Console adicionará automaticamente os endereços IP flutuantes a essa tabela de rotas. Se você tiver mais de uma tabela de rotas, é muito importante selecionar as tabelas de rotas corretas ao iniciar o par HA. Caso contrário, alguns clientes podem não ter acesso ao Cloud Volumes ONTAP.

Por exemplo, você pode ter duas sub-redes associadas a diferentes tabelas de rotas. Se você selecionar a tabela de rotas A, mas não a tabela de rotas B, os clientes na sub-rede associada à tabela de rotas A

poderão acessar o par HA, mas os clientes na sub-rede associada à tabela de rotas B não poderão.

Para obter mais informações sobre tabelas de rotas, consulte o "Documentação da AWS: Tabelas de rotas" .

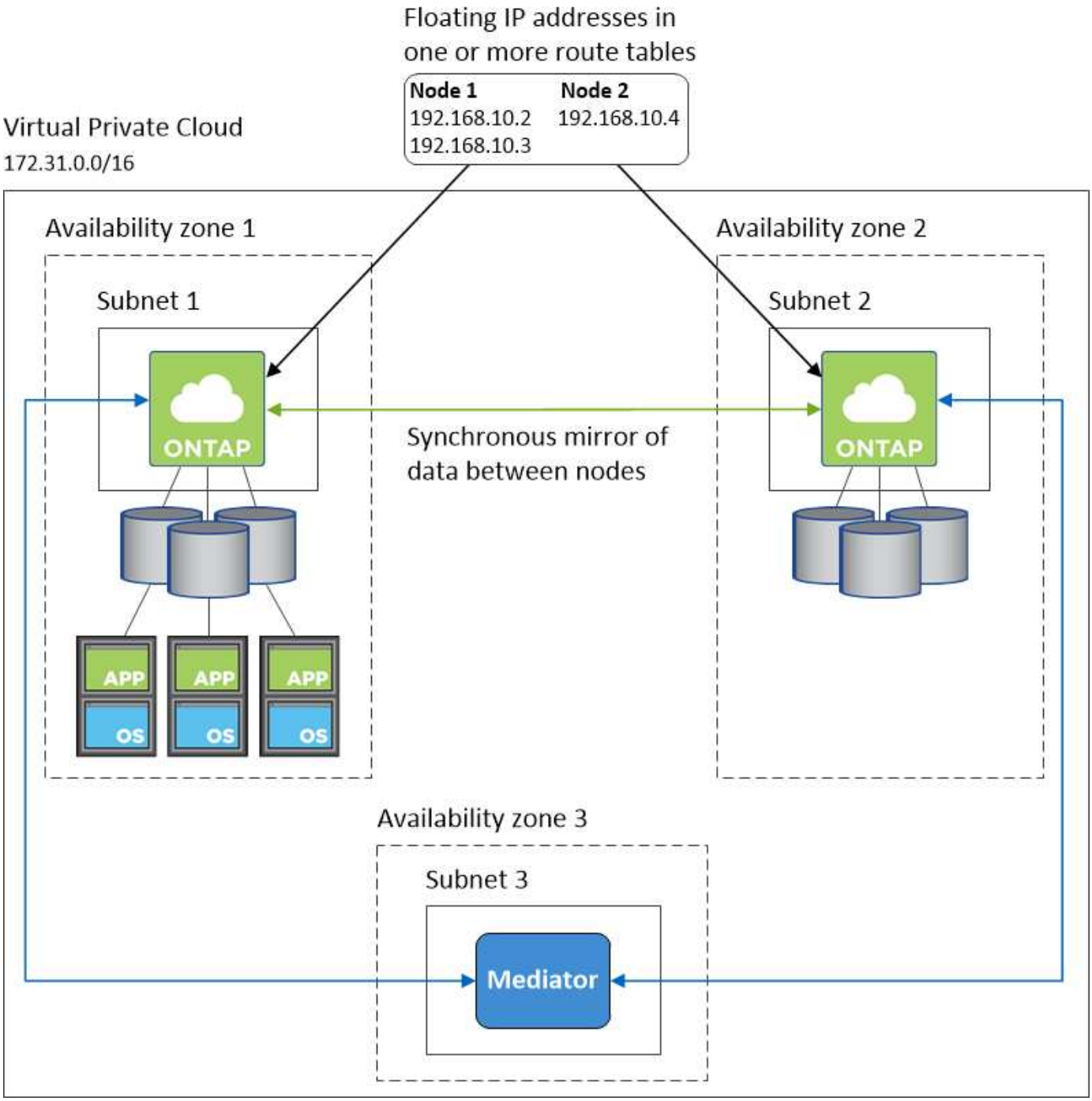
Conexão com ferramentas de gerenciamento da NetApp

Para usar ferramentas de gerenciamento do NetApp com configurações de HA que estão em várias AZs, você tem duas opções de conexão:

1. Implante as ferramentas de gerenciamento do NetApp em uma VPC diferente e"configurar um gateway de trânsito da AWS" . O gateway permite o acesso ao endereço IP flutuante para a interface de gerenciamento do cluster de fora da VPC.
2. Implante as ferramentas de gerenciamento do NetApp na mesma VPC com uma configuração de roteamento semelhante à dos clientes NAS.

Exemplo de configuração de HA

A imagem a seguir ilustra os componentes de rede específicos de um par de HA em várias AZs: três Zonas de Disponibilidade, três sub-redes, endereços IP flutuantes e uma tabela de rotas.



Requisitos para o agente do console

Se você ainda não criou um agente do Console, revise os requisitos de rede.

- "Exibir requisitos de rede para o agente do Console"
- "Regras de grupo de segurança na AWS"

Tópicos relacionados

- "Verifique a configuração do AutoSupport para o Cloud Volumes ONTAP"
- "Saiba mais sobre as portas internas do ONTAP" .

Configurar um gateway de trânsito da AWS para pares de alta disponibilidade do Cloud Volumes ONTAP

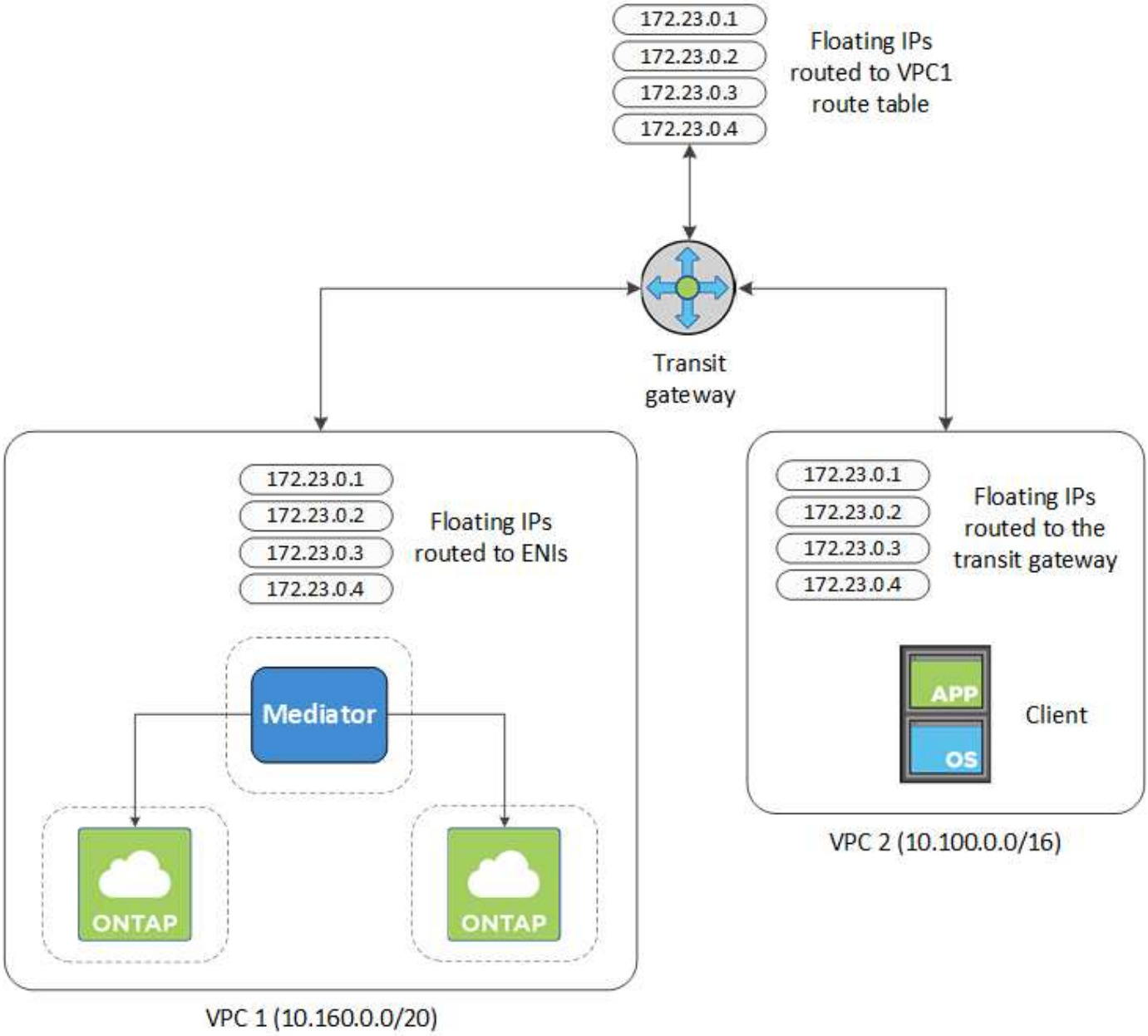
Configure um gateway de trânsito da AWS para permitir o acesso a um par de HA"endereços IP flutuantes" de fora da VPC onde o par HA reside.

Quando uma configuração do Cloud Volumes ONTAP HA é distribuída entre várias zonas de disponibilidade da AWS, endereços IP flutuantes são necessários para acesso a dados do NAS de dentro da VPC. Esses endereços IP flutuantes podem migrar entre nós quando ocorrem falhas, mas não são nativamente acessíveis de fora da VPC. Endereços IP privados separados fornecem acesso a dados de fora da VPC, mas não fornecem failover automático.

Endereços IP flutuantes também são necessários para a interface de gerenciamento de cluster e o LIF de gerenciamento SVM opcional.

Se você configurar um gateway de trânsito da AWS, habilitará o acesso aos endereços IP flutuantes de fora da VPC onde o par HA reside. Isso significa que clientes NAS e ferramentas de gerenciamento NetApp fora do VPC podem acessar os IPs flutuantes.

Aqui está um exemplo que mostra duas VPCs conectadas por um gateway de trânsito. Um sistema HA reside em uma VPC, enquanto um cliente reside na outra. Você pode então montar um volume NAS no cliente usando o endereço IP flutuante.

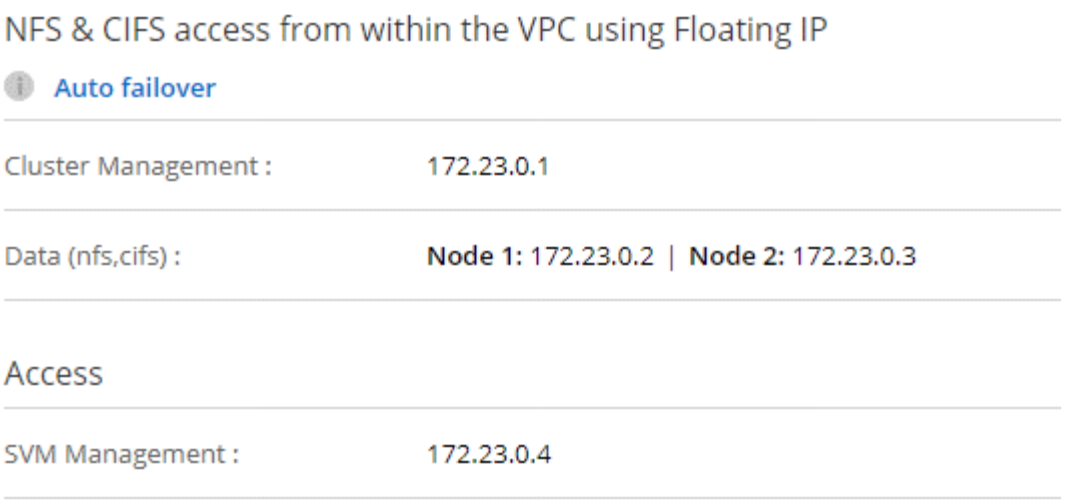


As etapas a seguir ilustram como configurar uma configuração semelhante.

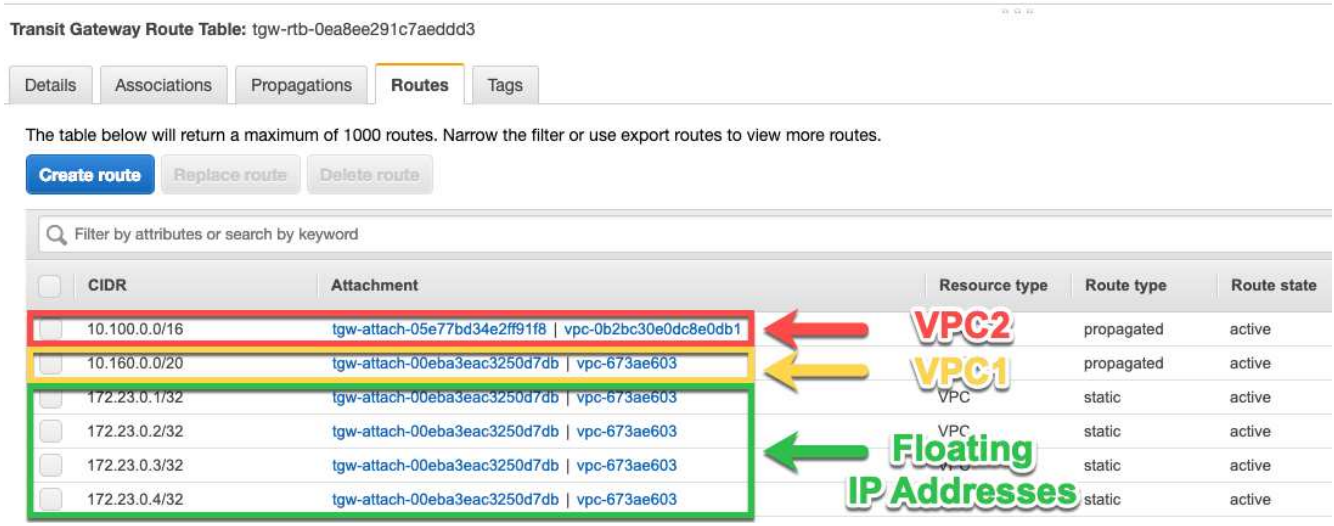
Passos

1. "Crie um gateway de trânsito e anexe as VPCs ao gateway" .
2. Associe as VPCs à tabela de rotas do gateway de trânsito.
   a. No serviço **VPC**, clique em **Tabelas de rotas do gateway de trânsito**.
   b. Selecione a tabela de rotas.
   c. Clique em **Associações** e depois selecione **Criar associação**.
   d. Escolha os anexos (VPCs) a serem associados e clique em **Criar associação**.
3. Crie rotas na tabela de rotas do gateway de trânsito especificando os endereços IP flutuantes do par HA.

   Você pode encontrar os endereços IP flutuantes na página de informações do sistema no NetApp Console. Aqui está um exemplo:



A imagem de exemplo a seguir mostra a tabela de rotas para o gateway de trânsito. Inclui rotas para os blocos CIDR das duas VPCs e quatro endereços IP flutuantes usados pelo Cloud Volumes ONTAP.

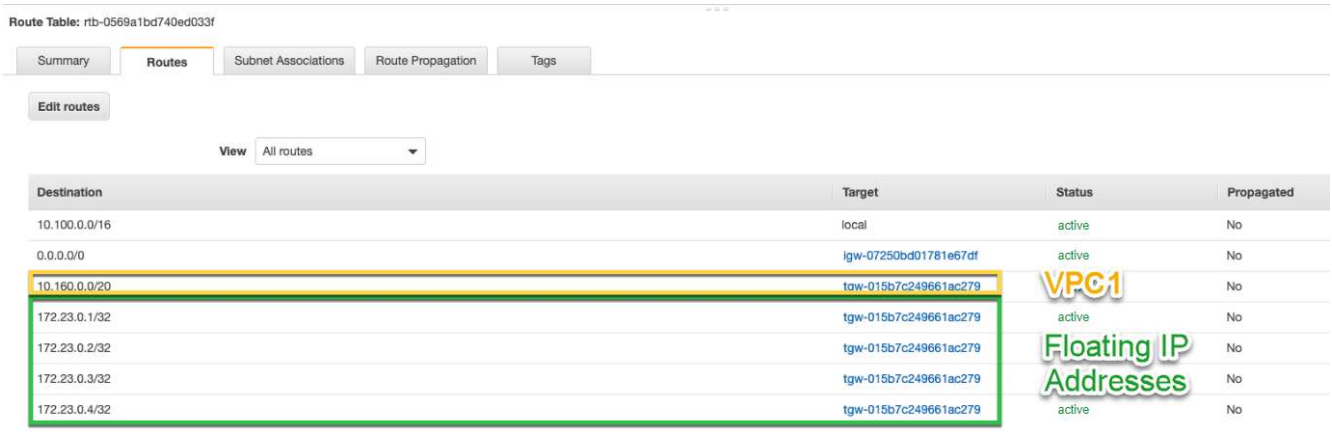


4. Modifique a tabela de rotas de VPCs que precisam acessar os endereços IP flutuantes.

   a. Adicione entradas de rota aos endereços IP flutuantes.

   b. Adicione uma entrada de rota ao bloco CIDR da VPC onde o par HA reside.

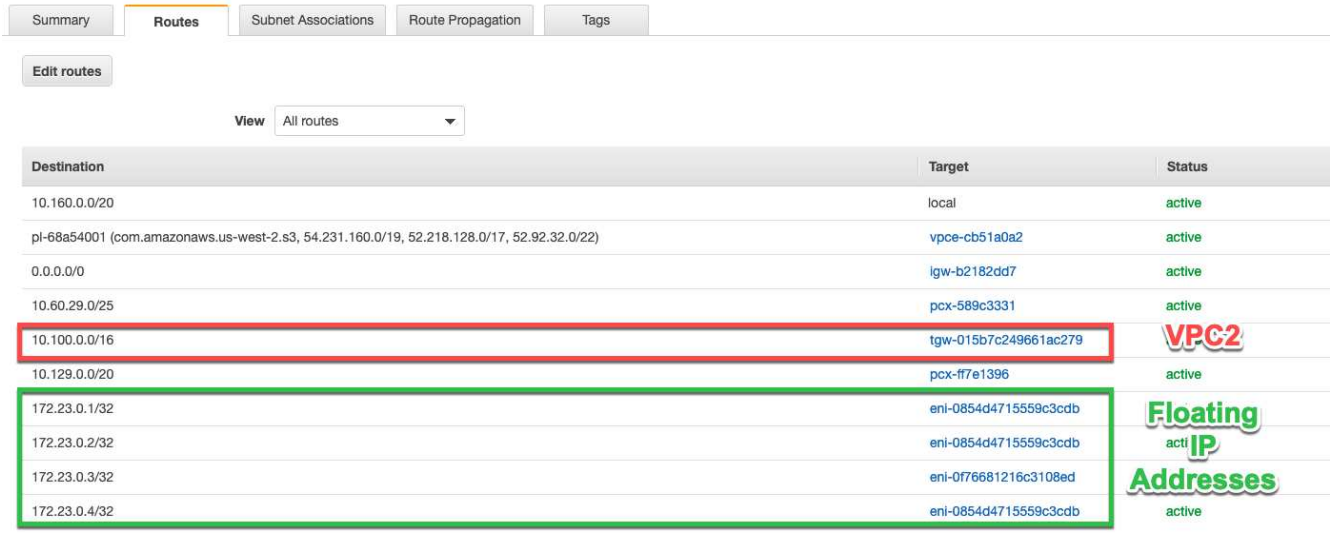
      A imagem de exemplo a seguir mostra a tabela de rotas para a VPC 2, que inclui rotas para a VPC 1 e os endereços IP flutuantes.



5. Modifique a tabela de rotas para a VPC do par HA adicionando uma rota à VPC que precisa de acesso aos endereços IP flutuantes.

   Esta etapa é importante porque conclui o roteamento entre as VPCs.

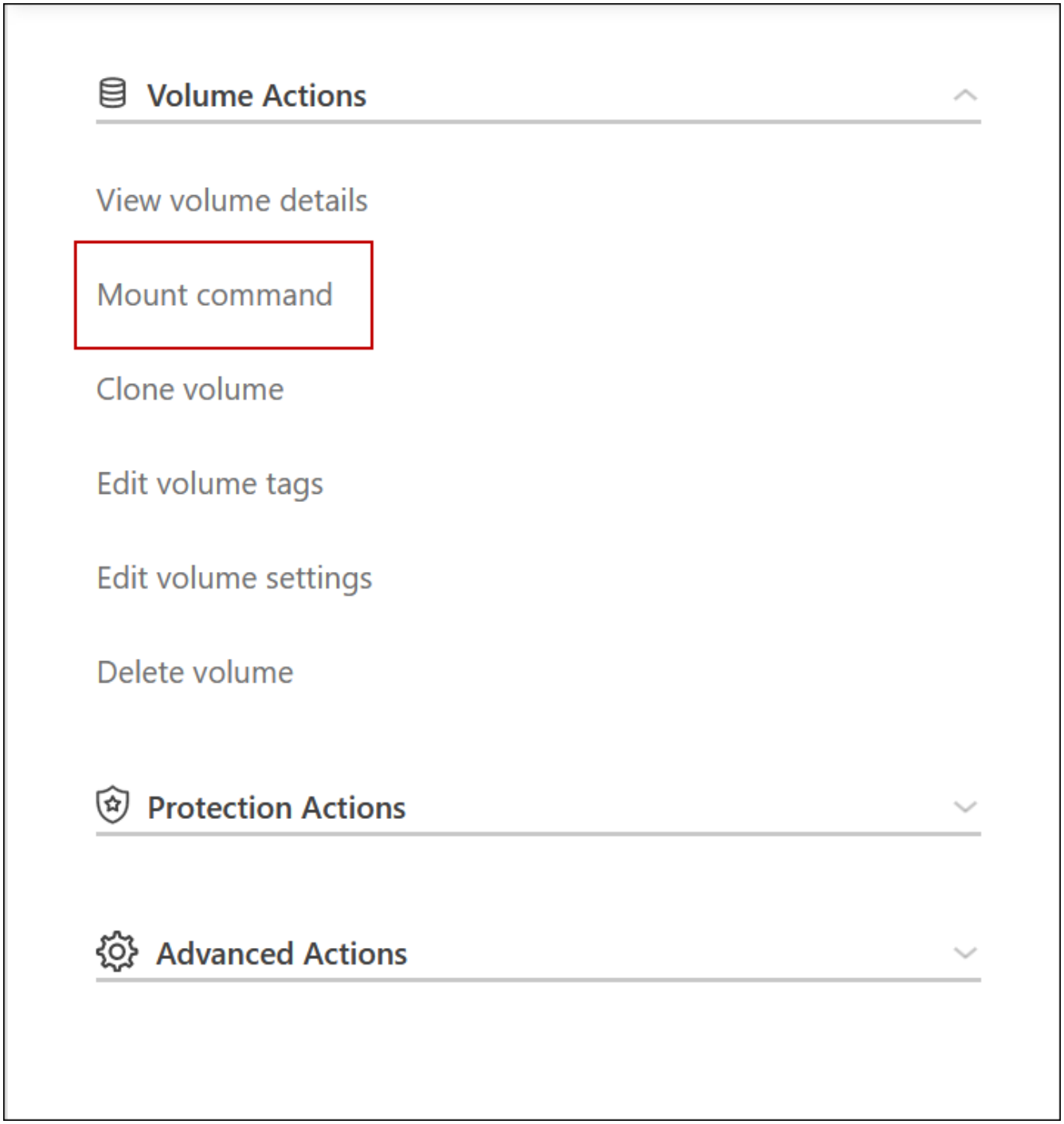
   A imagem de exemplo a seguir mostra a tabela de rotas para a VPC 1. Inclui uma rota para os endereços IP flutuantes e para a VPC 2, que é onde reside um cliente. O Console adicionou automaticamente os IPs flutuantes à tabela de rotas quando implantou o par HA.



6. Atualize as configurações dos grupos de segurança para Todo o tráfego para a VPC.
   a. Em Nuvem Privada Virtual, clique em **Sub-redes**.
   b. Clique na aba **Tabela de rotas**, selecione o ambiente desejado para um dos endereços IP flutuantes para um par HA.
   c. Clique em **Grupos de segurança**.
   d. Selecione **Editar regras de entrada**.
   e. Clique em **Adicionar regra**.
   f. Em Tipo, selecione **Todo o tráfego** e, em seguida, selecione o endereço IP da VPC.
   g. Clique em **Salvar regras** para aplicar as alterações.
7. Monte volumes em clientes usando o endereço IP flutuante.

   Você pode encontrar o endereço IP correto no Console por meio da opção **Comando de montagem** no

painel Gerenciar volumes no Console.



8. Se você estiver montando um volume NFS, configure a política de exportação para corresponder à sub-rede da VPC do cliente.

   "Aprenda a editar um volume" .

Links relacionados

- "Pares de alta disponibilidade na AWS"
- "Requisitos de rede para Cloud Volumes ONTAP na AWS"

Implantar pares de alta disponibilidade do Cloud Volumes ONTAP em uma sub-rede compartilhada da AWS

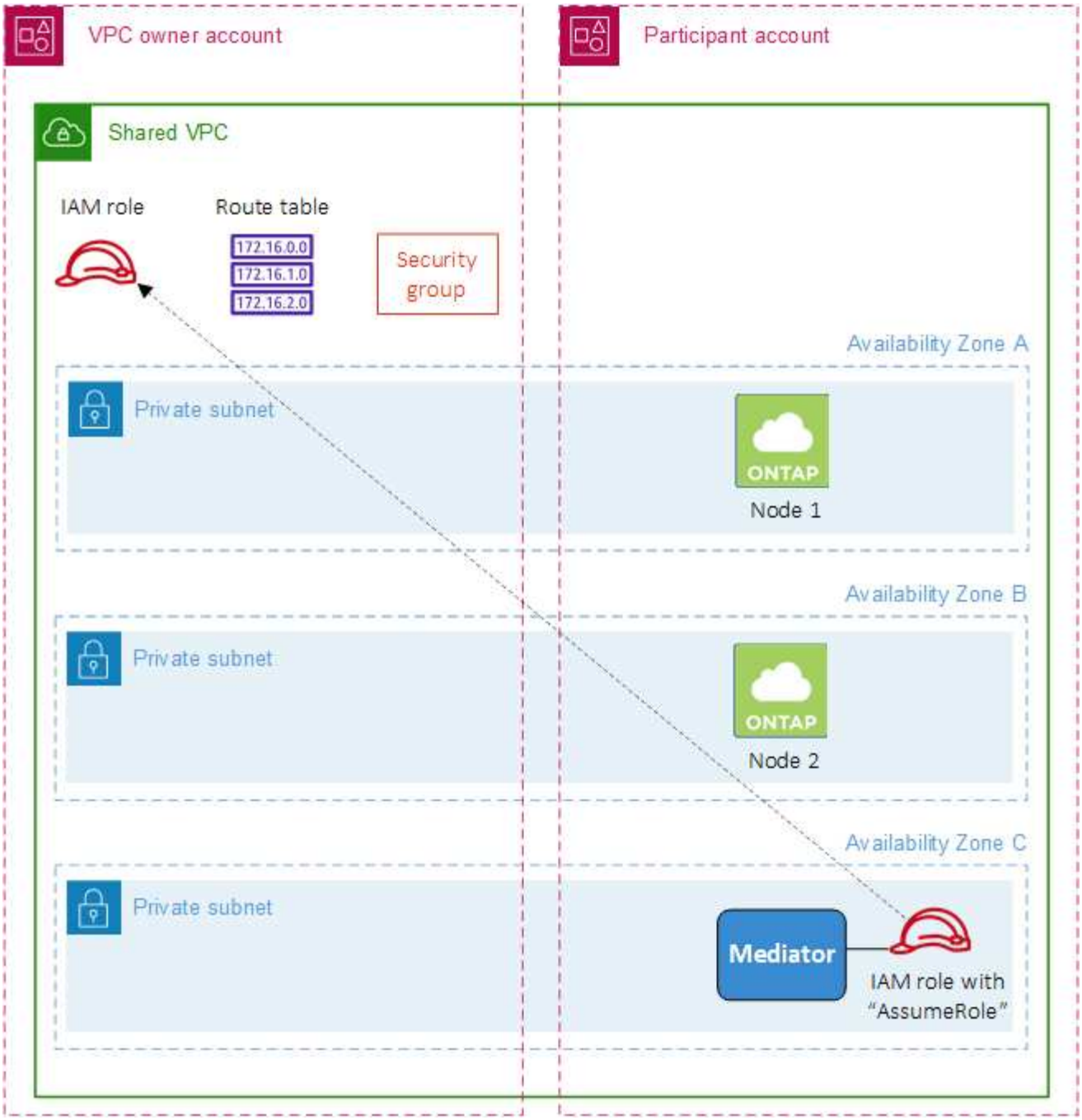
A partir da versão 9.11.1, os pares de HA do Cloud Volumes ONTAP são suportados na AWS com compartilhamento de VPC. O compartilhamento de VPC permite que sua organização compartilhe sub-redes com outras contas da AWS. Para usar esta configuração, você deve configurar seu ambiente AWS e então implantar o par HA usando a API.

Com "Compartilhamento de VPC" , uma configuração do Cloud Volumes ONTAP HA é distribuída em duas contas:

- A conta do proprietário da VPC, que possui a rede (VPC, sub-redes, tabelas de rotas e grupo de segurança do Cloud Volumes ONTAP)
- A conta do participante, onde as instâncias do EC2 são implantadas em sub-redes compartilhadas (isso inclui os dois nós de HA e o mediador)

No caso de uma configuração de HA do Cloud Volumes ONTAP implantada em várias Zonas de Disponibilidade, o mediador de HA precisa de permissões específicas para gravar nas tabelas de rotas na conta do proprietário da VPC. Você precisa fornecer essas permissões configurando uma função do IAM que o mediador pode assumir.

A imagem a seguir mostra os componentes envolvidos nesta implantação:



Conforme descrito nas etapas abaixo, você precisará compartilhar as sub-redes com a conta do participante e, em seguida, criar a função do IAM e o grupo de segurança na conta do proprietário da VPC.

Quando você cria o sistema Cloud Volumes ONTAP , o NetApp Console cria e anexa automaticamente uma função do IAM ao mediador. Esta função assume a função do IAM que você criou na conta do proprietário da VPC para fazer alterações nas tabelas de rotas associadas ao par HA.

Passos

1. Compartilhe as sub-redes na conta do proprietário da VPC com a conta do participante.

   Esta etapa é necessária para implantar o par HA em sub-redes compartilhadas.

   "Documentação da AWS: Compartilhe uma sub-rede"

2. Na conta do proprietário da VPC, crie um grupo de segurança para o Cloud Volumes ONTAP.

   "Consulte as regras do grupo de segurança para o Cloud Volumes ONTAP" . Observe que você não precisa criar um grupo de segurança para o mediador HA. O Console faz isso por você.

3. Na conta do proprietário da VPC, crie uma função do IAM que inclua as seguintes permissões:

```
Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
```

4. Use a API para criar um novo sistema Cloud Volumes ONTAP .

   Observe que você deve especificar os seguintes campos:

   - "ID do Grupo de Segurança"

     O campo "securityGroupId" deve especificar o grupo de segurança que você criou na conta do proprietário da VPC (consulte a etapa 2 acima).

   - "assumeRoleArn" no objeto "haParams"

     O campo "assumeRoleArn" deve incluir o ARN da função do IAM que você criou na conta do proprietário da VPC (consulte a etapa 3 acima).

     Por exemplo:

```
"haParams": {
     "assumeRoleArn":
"arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
}
```

   +
   "Saiba mais sobre a API Cloud Volumes ONTAP"

Configurar a criação de grupos de posicionamento para pares de alta disponibilidade do Cloud Volumes ONTAP em AZs únicas da AWS

As implantações de alta disponibilidade (HA) do Cloud Volumes ONTAP na Zona de disponibilidade única (AZ) da AWS podem falhar e ser revertidas se a criação do grupo de posicionamento falhar. A criação do grupo de posicionamento também falha e a implantação é revertida se o nó Cloud Volumes ONTAP e a instância do mediador não

estiverem disponíveis. Para evitar isso, você pode modificar a configuração para permitir que a implantação seja concluída mesmo se a criação do grupo de posicionamento falhar.

Ao ignorar o processo de reversão, o processo de implantação do Cloud Volumes ONTAP é concluído com sucesso e notifica você de que a criação do grupo de posicionamento está incompleta.

Passos

1. Use SSH para se conectar ao host do agente do NetApp Console e efetuar login.
2. Navegar para `/opt/application/netapp/cloudmanager/docker_occm/data` .
3. Editar `app.conf` alterando o valor do `rollback-on-placement-group-failure` parâmetro para `false` . O valor padrão deste parâmetro é `true` .

```
{
    "occm" : {
        "aws" : {
            "rollback-on-placement-group-failure" : false
        }
    }
}
```

4. Salve o arquivo e faça logoff do agente do Console. Não é necessário reiniciar o agente do Console.

Regras de entrada e saída do grupo de segurança da AWS para o Cloud Volumes ONTAP

O NetApp Console cria grupos de segurança da AWS que incluem as regras de entrada e saída que o Cloud Volumes ONTAP precisa para operar com sucesso. Talvez você queira consultar as portas para fins de teste ou, se preferir, usar seus próprios grupos de segurança.

Regras para Cloud Volumes ONTAP

O grupo de segurança do Cloud Volumes ONTAP exige regras de entrada e saída.

Regras de entrada

Ao adicionar um sistema Cloud Volumes ONTAP e escolher um grupo de segurança predefinido, você pode optar por permitir o tráfego dentro de um dos seguintes:

- **Somente VPC selecionada**: a origem do tráfego de entrada é o intervalo de sub-rede da VPC para o sistema Cloud Volumes ONTAP e o intervalo de sub-rede da VPC onde o agente do Console reside. Esta é a opção recomendada.
- **Todas as VPCs**: a origem do tráfego de entrada é o intervalo de IP 0.0.0.0/0.

Protocolo	Porta	Propósito
Todos os ICMP	Todos	Executando ping na instância
HTTP	80	Acesso HTTP ao console da web do ONTAP System Manager usando o endereço IP do LIF de gerenciamento do cluster
HTTPS	443	Conectividade com o agente do Console e acesso HTTPS ao console da Web do ONTAP System Manager usando o endereço IP do LIF de gerenciamento do cluster
SSH	22	Acesso SSH ao endereço IP do LIF de gerenciamento de cluster ou de um LIF de gerenciamento de nó
TCP	111	Chamada de procedimento remoto para NFS
TCP	139	Sessão de serviço NetBIOS para CIFS
TCP	161-162	Protocolo simples de gerenciamento de rede
TCP	445	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
TCP	635	Montagem NFS
TCP	749	Kerberos
TCP	2049	Daemon do servidor NFS
TCP	3260	Acesso iSCSI através do LIF de dados iSCSI
TCP	4045	Daemon de bloqueio NFS
TCP	4046	Monitor de status de rede para NFS
TCP	10000	Backup usando NDMP
TCP	11104	Gerenciamento de sessões de comunicação entre clusters para SnapMirror
TCP	11105	Transferência de dados do SnapMirror usando LIFs intercluster
UDP	111	Chamada de procedimento remoto para NFS
UDP	161-162	Protocolo simples de gerenciamento de rede
UDP	635	Montagem NFS
UDP	2049	Daemon do servidor NFS
UDP	4045	Daemon de bloqueio NFS
UDP	4046	Monitor de status de rede para NFS
UDP	4049	Protocolo NFS rquotad

Regras de saída

O grupo de segurança predefinido para o Cloud Volumes ONTAP abre todo o tráfego de saída. Se isso for aceitável, siga as regras básicas de saída. Se precisar de regras mais rígidas, use as regras de saída avançadas.

Regras básicas de saída

O grupo de segurança predefinido para o Cloud Volumes ONTAP inclui as seguintes regras de saída.

Protocolo	Porta	Propósito
Todos os ICMP	Todos	Todo o tráfego de saída
Todos os TCP	Todos	Todo o tráfego de saída
Todos os UDP	Todos	Todo o tráfego de saída

Regras avançadas de saída

Se precisar de regras rígidas para o tráfego de saída, você pode usar as seguintes informações para abrir apenas as portas necessárias para a comunicação de saída pelo Cloud Volumes ONTAP.

A origem é a interface (endereço IP) no sistema Cloud Volumes ONTAP .

Serviço	Protocolo	Porta	Fonte	Destino	Propósito
Diretório ativo	TCP	88	Gerenciamento de nós LIF	Floresta do Active Directory	Autenticação Kerberos V
	UDP	137	Gerenciamento de nós LIF	Floresta do Active Directory	Serviço de nomes NetBIOS
	UDP	138	Gerenciamento de nós LIF	Floresta do Active Directory	Serviço de datagrama NetBIOS
	TCP	139	Gerenciamento de nós LIF	Floresta do Active Directory	Sessão de serviço NetBIOS
	TCP e UDP	389	Gerenciamento de nós LIF	Floresta do Active Directory	LDAP
	TCP	445	Gerenciamento de nós LIF	Floresta do Active Directory	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
	TCP	464	Gerenciamento de nós LIF	Floresta do Active Directory	Alteração e definição de senha do Kerberos V (SET_CHANGE)
	UDP	464	Gerenciamento de nós LIF	Floresta do Active Directory	Administração de chaves Kerberos
	TCP	749	Gerenciamento de nós LIF	Floresta do Active Directory	Kerberos V alterar e definir senha (RPCSEC_GSS)
	TCP	88	Dados LIF (NFS, CIFS, iSCSI)	Floresta do Active Directory	Autenticação Kerberos V
	UDP	137	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Serviço de nomes NetBIOS
	UDP	138	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Serviço de datagrama NetBIOS
	TCP	139	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Sessão de serviço NetBIOS
	TCP e UDP	389	Dados LIF (NFS, CIFS)	Floresta do Active Directory	LDAP
	TCP	445	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
	TCP	464	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Alteração e definição de senha do Kerberos V (SET_CHANGE)
	UDP	464	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Administração de chaves Kerberos
	TCP	749	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Alterar e definir senha do Kerberos V (RPCSEC_GSS)

Serviço	Protocolo	Porta	Fonte	Destino	Propósito
AutoSupport	HTTPS	443	Gerenciamento de nós LIF	meusuporte.netapp.com	AutoSupport (HTTPS é o padrão)
	HTTP	80	Gerenciamento de nós LIF	meusuporte.netapp.com	AutoSupport (somente se o protocolo de transporte for alterado de HTTPS para HTTP)
	TCP	3128	Gerenciamento de nós LIF	Agente de console	Envio de mensagens do AutoSupport por meio de um servidor proxy no agente do Console, se uma conexão de saída com a Internet não estiver disponível
Backup para S3	TCP	5010	LIF interaglomerado	Ponto de extremidade de backup ou ponto de extremidade de restauração	Operações de backup e restauração para o recurso Backup para S3
Conjunto	Todo o tráfego	Todo o tráfego	Todos os LIFs em um nó	Todos os LIFs no outro nó	Comunicações entre clusters (somente Cloud Volumes ONTAP HA)
	TCP	3000	Gerenciamento de nós LIF	Mediador HA	Chamadas ZAPI (somente Cloud Volumes ONTAP HA)
	ICMP	1	Gerenciamento de nós LIF	Mediador HA	Mantenha-se ativo (somente Cloud Volumes ONTAP HA)
Backups de configuração	HTTP	80	Gerenciamento de nós LIF	http://<endereço-IP-do-agente-do-console>/occm/offboxconfig	Envie backups de configuração para o agente do Console."Documentação do ONTAP"
DHCP	UDP	68	Gerenciamento de nós LIF	DHCP	Cliente DHCP para configuração inicial
DHCPS	UDP	67	Gerenciamento de nós LIF	DHCP	Servidor DHCP
DNS	UDP	53	Gerenciamento de nós LIF e dados LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	Gerenciamento de nós LIF	Servidores de destino	Cópia do NDMP
SMTP	TCP	25	Gerenciamento de nós LIF	Servidor de e-mail	Alertas SMTP podem ser usados para AutoSupport

Serviço	Protocolo	Porta	Fonte	Destino	Propósito
SNMP	TCP	161	Gerenciamento de nós LIF	Servidor de monitoramento	Monitoramento por armadilhas SNMP
	UDP	161	Gerenciamento de nós LIF	Servidor de monitoramento	Monitoramento por armadilhas SNMP
	TCP	162	Gerenciamento de nós LIF	Servidor de monitoramento	Monitoramento por armadilhas SNMP
	UDP	162	Gerenciamento de nós LIF	Servidor de monitoramento	Monitoramento por armadilhas SNMP
SnapMirror	TCP	11104	LIF interaglomerado	LIFs interaglomerados ONTAP	Gerenciamento de sessões de comunicação entre clusters para SnapMirror
	TCP	11105	LIF interaglomerado	LIFs interaglomerados ONTAP	Transferência de dados do SnapMirror
Log de sistema	UDP	514	Gerenciamento de nós LIF	Servidor Syslog	Mensagens de encaminhamento do Syslog

Regras para o grupo de segurança externa do mediador HA

O grupo de segurança externo predefinido para o mediador Cloud Volumes ONTAP HA inclui as seguintes regras de entrada e saída.

Regras de entrada

O grupo de segurança predefinido para o mediador HA inclui a seguinte regra de entrada.

Protocolo	Porta	Fonte	Propósito
TCP	3000	CIDR do agente do console	Acesso à API RESTful a partir do agente do Console

Regras de saída

O grupo de segurança predefinido para o mediador HA abre todo o tráfego de saída. Se isso for aceitável, siga as regras básicas de saída. Se precisar de regras mais rígidas, use as regras de saída avançadas.

Regras básicas de saída

O grupo de segurança predefinido para o mediador HA inclui as seguintes regras de saída.

Protocolo	Porta	Propósito
Todos os TCP	Todos	Todo o tráfego de saída
Todos os UDP	Todos	Todo o tráfego de saída

Regras avançadas de saída

Se precisar de regras rígidas para o tráfego de saída, você pode usar as seguintes informações para abrir apenas as portas necessárias para a comunicação de saída pelo mediador HA.

Protocolo	Porta	Destino	Propósito
HTTP	80	Endereço IP do agente do console na instância do AWS EC2	Baixe atualizações para o mediador
HTTPS	443	ec2.amazonaws.com	Auxiliar no failover de armazenamento
UDP	53	ec2.amazonaws.com	Auxiliar no failover de armazenamento

Em vez de abrir as portas 443 e 53, você pode criar um endpoint de VPC de interface da sub-rede de destino para o serviço AWS EC2.

Regras para o grupo de segurança interna de configuração de HA

O grupo de segurança interno predefinido para uma configuração do Cloud Volumes ONTAP HA inclui as seguintes regras. Este grupo de segurança permite a comunicação entre os nós HA e entre o mediador e os nós.

O Console sempre cria esse grupo de segurança. Você não tem a opção de usar o seu próprio.

Regras de entrada

O grupo de segurança predefinido inclui as seguintes regras de entrada.

Protocolo	Porta	Propósito
Todo o tráfego	Todos	Comunicação entre o mediador HA e os nós HA

Regras de saída

O grupo de segurança predefinido inclui as seguintes regras de saída.

Protocolo	Porta	Propósito
Todo o tráfego	Todos	Comunicação entre o mediador HA e os nós HA

Regras para o agente do Console

"Exibir regras de grupo de segurança para o agente do Console"

Configurar o Cloud Volumes ONTAP para usar uma chave gerenciada pelo cliente na AWS

Se você quiser usar a criptografia da Amazon com o Cloud Volumes ONTAP, precisará configurar o AWS Key Management Service (KMS).

Passos

1. Certifique-se de que exista uma Chave Mestra do Cliente (CMK) ativa.

A CMK pode ser uma CMK gerenciada pela AWS ou uma CMK gerenciada pelo cliente. Ele pode estar na mesma conta da AWS que o NetApp Console e o Cloud Volumes ONTAP ou em uma conta da AWS diferente.

"Documentação da AWS: Chaves Mestras do Cliente (CMKs)"

2. Modifique a política de chave para cada CMK adicionando a função do IAM que fornece permissões ao Console como um *usuário de chave*.

   Adicionar a função de Gerenciamento de Identidade e Acesso (IAM) como um usuário-chave concede ao Console permissões para usar a CMK com o Cloud Volumes ONTAP.

   "Documentação da AWS: Editando Chaves"

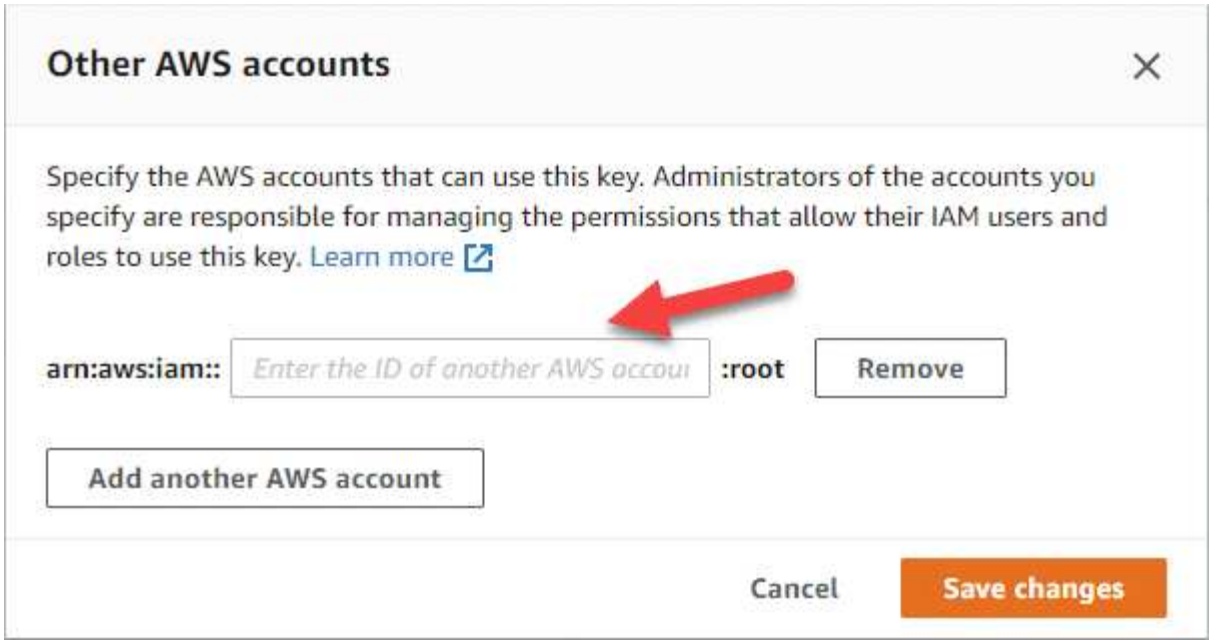
3. Se a CMK estiver em uma conta diferente da AWS, conclua as seguintes etapas:

   a. Acesse o console do KMS a partir da conta onde o CMK reside.
   b. Selecione a chave.
   c. No painel **Configuração geral**, copie o ARN da chave.

      Você precisará fornecer o ARN ao Console ao criar o sistema Cloud Volumes ONTAP .

   d. No painel **Outras contas da AWS**, adicione a conta da AWS que fornece permissões ao Console.

      Normalmente, esta é a conta onde o Console é implantado. Se o Console não estiver instalado na AWS, use a conta para a qual você forneceu as chaves de acesso da AWS ao Console.



e. Agora mude para a conta da AWS que fornece permissões ao Console e abra o console do IAM.

f. Crie uma política do IAM que inclua as permissões listadas abaixo.

g. Anexe a política à função do IAM ou ao usuário do IAM que fornece permissões ao Console.

   A política a seguir fornece as permissões que o Console precisa para usar a CMK da conta externa da AWS. Não se esqueça de modificar a região e o ID da conta nas seções "Recurso".

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
            ]
        },
        {
            "Sid": "AllowAttachmentOfPersistentResources",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

+
Para obter detalhes adicionais sobre este processo, consulte o "Documentação da AWS: Permitindo que usuários em outras contas usem uma chave KMS" .

4. Se você estiver usando uma CMK gerenciada pelo cliente, modifique a política de chave para a CMK adicionando a função IAM do Cloud Volumes ONTAP como um *usuário de chave*.

Esta etapa é necessária se você habilitou o armazenamento em camadas de dados no Cloud Volumes ONTAP e deseja criptografar os dados armazenados no bucket do Amazon Simple Storage Service (Amazon S3) (Amazon S3).

Você precisará executar esta etapa *depois* de implantar o Cloud Volumes ONTAP porque a função do IAM é criada quando você cria um sistema Cloud Volumes ONTAP . (É claro que você tem a opção de usar uma função IAM existente do Cloud Volumes ONTAP , então é possível executar esta etapa antes.)

"Documentação da AWS: Editando Chaves"

Configurar funções do AWS IAM para nós do Cloud Volumes ONTAP

As funções de gerenciamento de identidade e acesso (IAM) da AWS com as permissões necessárias devem ser anexadas a cada nó do Cloud Volumes ONTAP . O mesmo vale para o mediador HA. É mais fácil deixar que o NetApp Console crie as funções do IAM para você, mas você pode usar suas próprias funções.

Esta tarefa é opcional. Ao criar um sistema Cloud Volumes ONTAP , a opção padrão é deixar o Console criar as funções do IAM para você. Se as políticas de segurança da sua empresa exigirem que você mesmo crie as funções do IAM, siga as etapas abaixo.

É necessário fornecer sua própria função de IAM no AWS Secret Cloud. "Aprenda a implantar o Cloud Volumes ONTAP no C2S" .

Passos

1. Acesse o console do AWS IAM.
2. Crie políticas do IAM que incluam as seguintes permissões:
    - Política básica para nós Cloud Volumes ONTAP

Regiões padrão

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }
    ]
}
```

Regiões GovCloud (EUA)

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-us-gov:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Regiões ultrasecretas

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Regiões secretas

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso-b:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

- Política de backup para nós Cloud Volumes ONTAP

  Se você planeja usar o NetApp Backup and Recovery com seus sistemas Cloud Volumes ONTAP , a função do IAM para os nós deve incluir a segunda política mostrada abaixo.

Regiões padrão

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

Regiões GovCloud (EUA)

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

Regiões ultrasecretas

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

Regiões secretas

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso-b:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso-b:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

- Mediador HA

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses",
                "sts:AssumeRole",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

3. Crie uma função do IAM e anexe as políticas que você criou à função.

Resultado

Agora você tem funções do IAM que pode selecionar ao criar um novo sistema Cloud Volumes ONTAP .

Mais informações

- "Documentação da AWS: Criando políticas do IAM"
- "Documentação da AWS: Criando funções do IAM"

Configurar licenciamento para Cloud Volumes ONTAP na AWS

Depois de decidir qual opção de licenciamento você deseja usar com o Cloud Volumes ONTAP, algumas etapas são necessárias antes que você possa escolher essa opção de licenciamento ao criar um novo sistema.

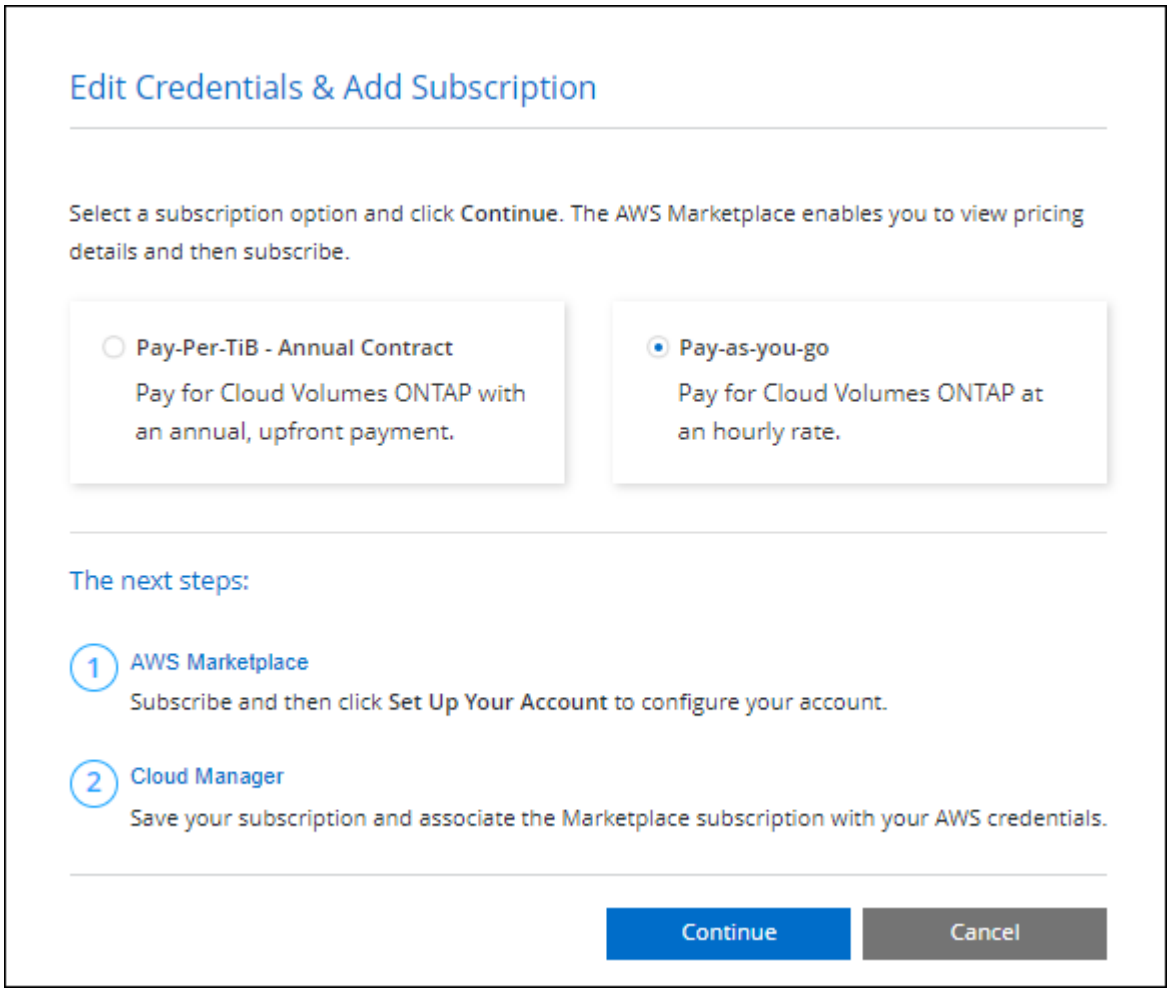
Freemium

Selecione a oferta Freemium para usar o Cloud Volumes ONTAP gratuitamente com até 500 GiB de capacidade provisionada. "Saiba mais sobre a oferta Freemium" .

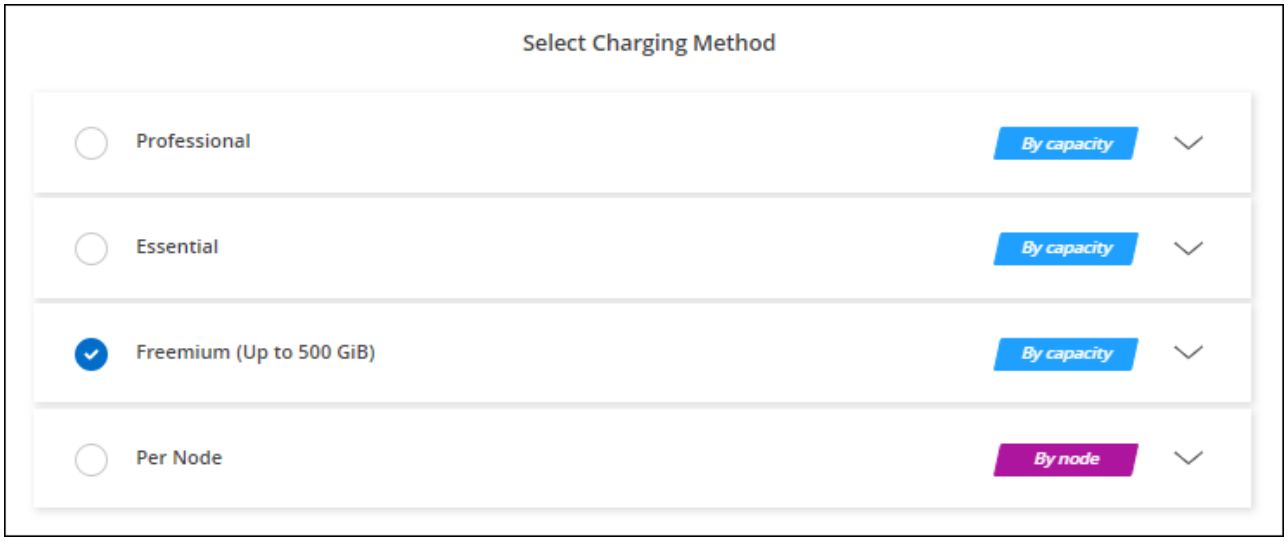
Passos

1. No menu de navegação esquerdo do NetApp Console, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas.
    a. Na página **Detalhes e credenciais**, clique em **Editar credenciais > Adicionar assinatura** e siga as instruções para assinar a oferta de pagamento conforme o uso no AWS Marketplace.

Você não será cobrado pela assinatura do marketplace, a menos que exceda 500 GiB de capacidade provisionada, momento em que o sistema será automaticamente convertido para o"Pacote Essentials" .



a. Após retornar ao Console, selecione **Freemium** quando chegar à página de métodos de cobrança.



"Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP na AWS" .

Licença baseada em capacidade

O licenciamento baseado em capacidade permite que você pague pelo Cloud Volumes ONTAP por TiB de capacidade. O licenciamento baseado em capacidade está disponível na forma de um *pacote*: o pacote Essentials ou o pacote Professional.

Os pacotes Essentials e Professional estão disponíveis nos seguintes modelos de consumo ou opções de compra:

- Uma licença (traga sua própria licença (BYOL)) adquirida da NetApp
- Uma assinatura por hora, paga conforme o uso (PAYGO) do AWS Marketplace
- Um contrato anual do AWS Marketplace

"Saiba mais sobre licenciamento baseado em capacidade" .

As seções a seguir descrevem como começar a usar cada um desses modelos de consumo.

Traga sua própria bebida

Pague antecipadamente comprando uma licença (BYOL) da NetApp para implantar sistemas Cloud Volumes ONTAP em qualquer provedor de nuvem.

A NetApp restringiu a compra, extensão e renovação de licenças BYOL. Para obter mais informações, consulte "Disponibilidade restrita de licenciamento BYOL para Cloud Volumes ONTAP" .

Passos

1. "Entre em contato com a equipe de vendas da NetApp para obter uma licença"
2. "Adicione sua conta do site de suporte da NetApp ao console"

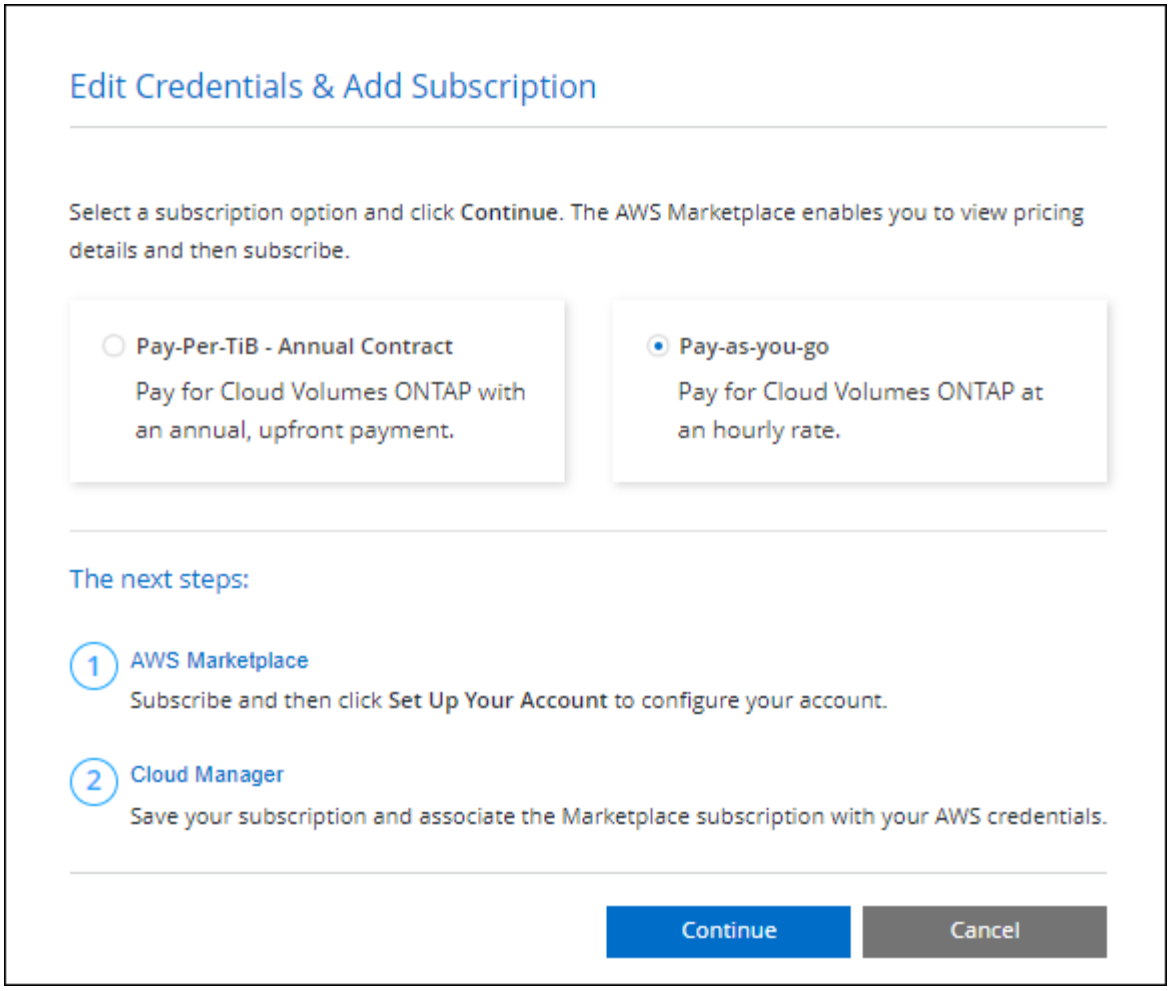
   O Console consulta automaticamente o serviço de licenciamento da NetApp para obter detalhes sobre as licenças associadas à sua conta do Site de Suporte da NetApp . Se não houver erros, o Console adicionará automaticamente as licenças ao Console.

   Sua licença deve estar disponível no Console antes que você possa usá-la com o Cloud Volumes ONTAP. Se necessário, você pode"adicione manualmente a licença ao Console" .

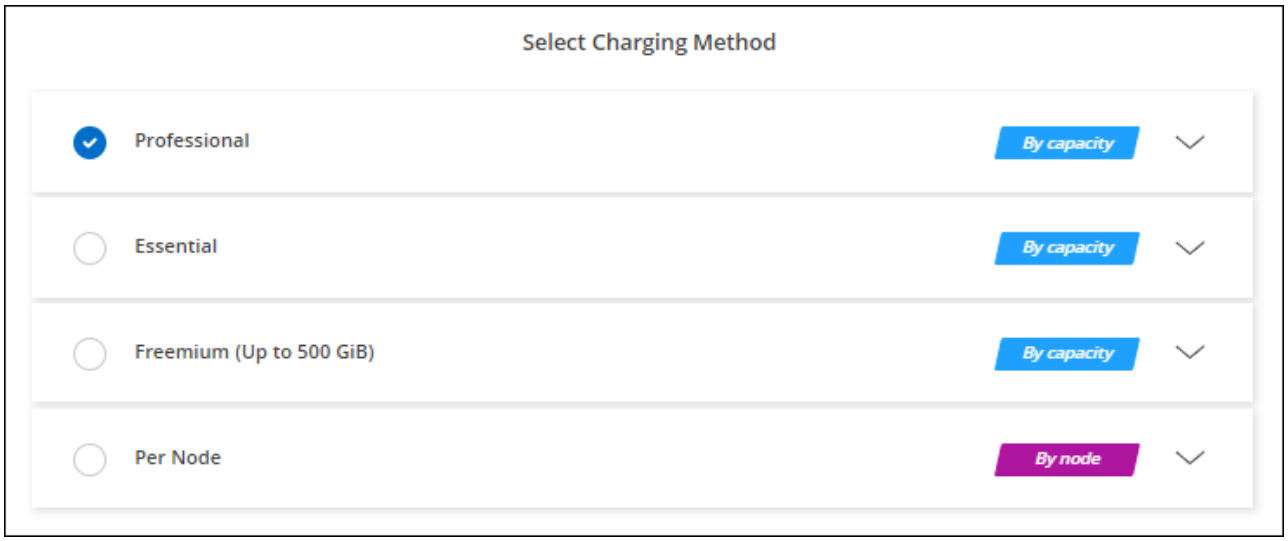
3. Na página **Sistemas** do Console, clique em **Adicionar Sistema** e siga as etapas.

   a. Na página **Detalhes e credenciais**, clique em **Editar credenciais > Adicionar assinatura** e siga as instruções para assinar a oferta de pagamento conforme o uso no AWS Marketplace.

      A licença que você comprou da NetApp é sempre cobrada primeiro, mas você será cobrado pela taxa horária no mercado se exceder sua capacidade licenciada ou se o prazo de sua licença expirar.



a. Após retornar ao Console, selecione um pacote baseado em capacidade quando chegar à página de métodos de cobrança.



"Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP na AWS" .

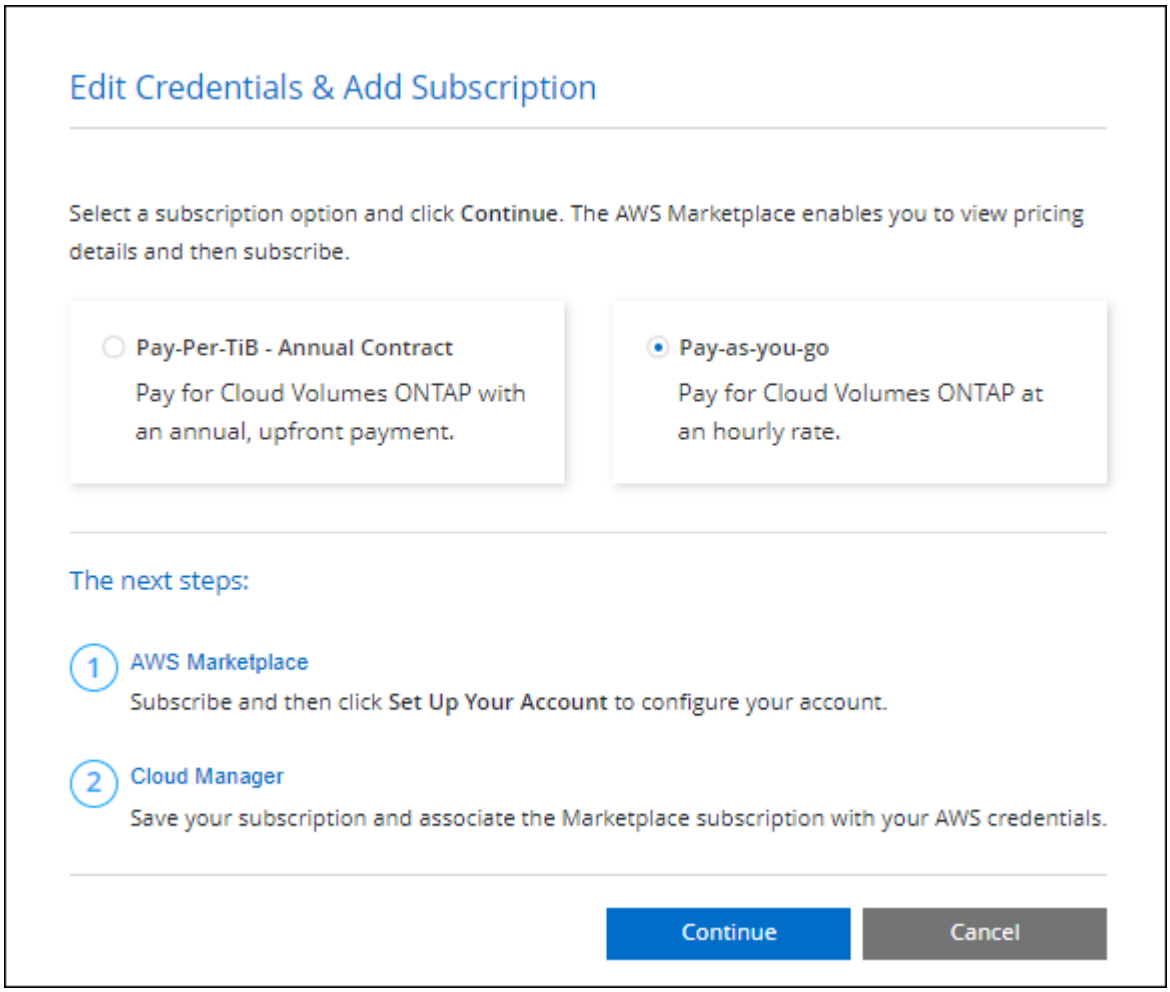
Assinatura PAYGO

Pague por hora assinando a oferta do marketplace do seu provedor de nuvem.

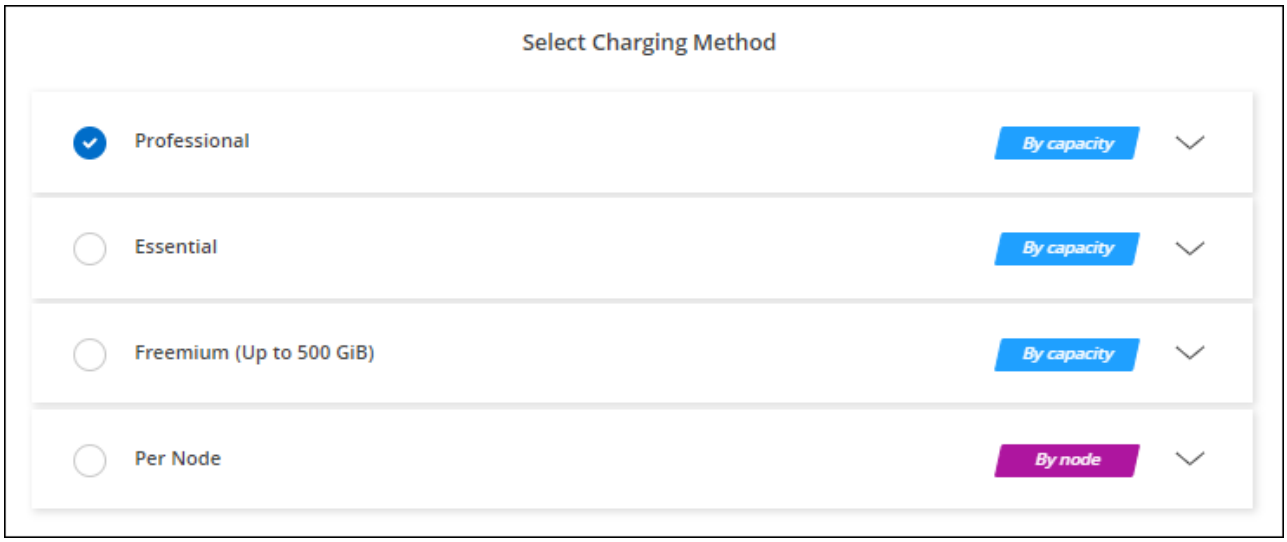
Quando você cria um sistema Cloud Volumes ONTAP , o Console solicita que você assine o contrato disponível no AWS Marketplace. Essa assinatura é então associada ao sistema de cobrança. Você pode usar a mesma assinatura para sistemas Cloud Volumes ONTAP adicionais.

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas.
   a. Na página **Detalhes e credenciais**, clique em **Editar credenciais > Adicionar assinatura** e siga as instruções para assinar a oferta de pagamento conforme o uso no AWS Marketplace



   b. Após retornar ao Console, selecione um pacote baseado em capacidade quando chegar à página de métodos de cobrança.



"Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP na AWS" .

Você pode gerenciar as assinaturas do AWS Marketplace associadas às suas contas da AWS na página Configurações > Credenciais. "Aprenda a gerenciar suas contas e assinaturas da AWS"

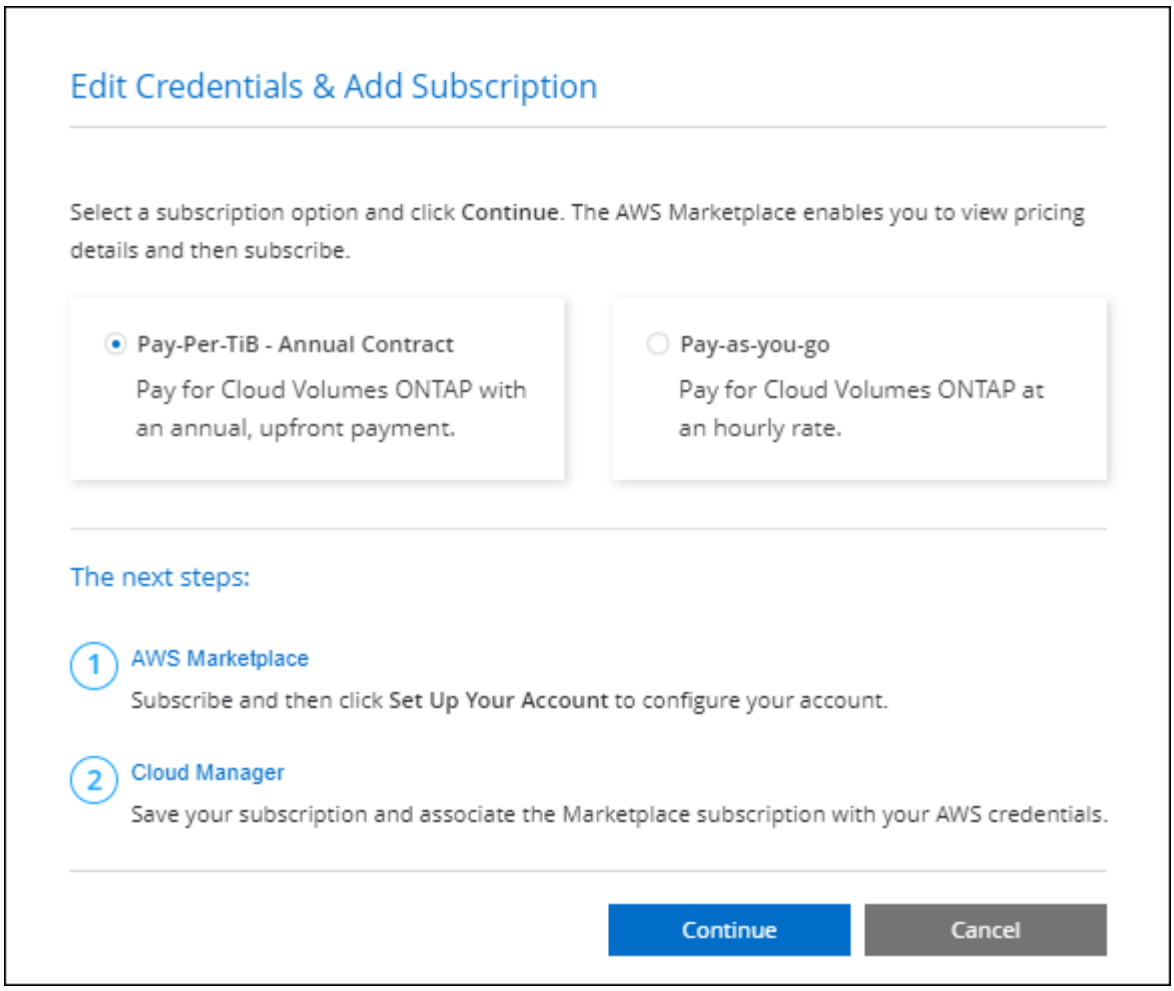
Contrato anual

Pague anualmente comprando um contrato anual no marketplace do seu provedor de nuvem.

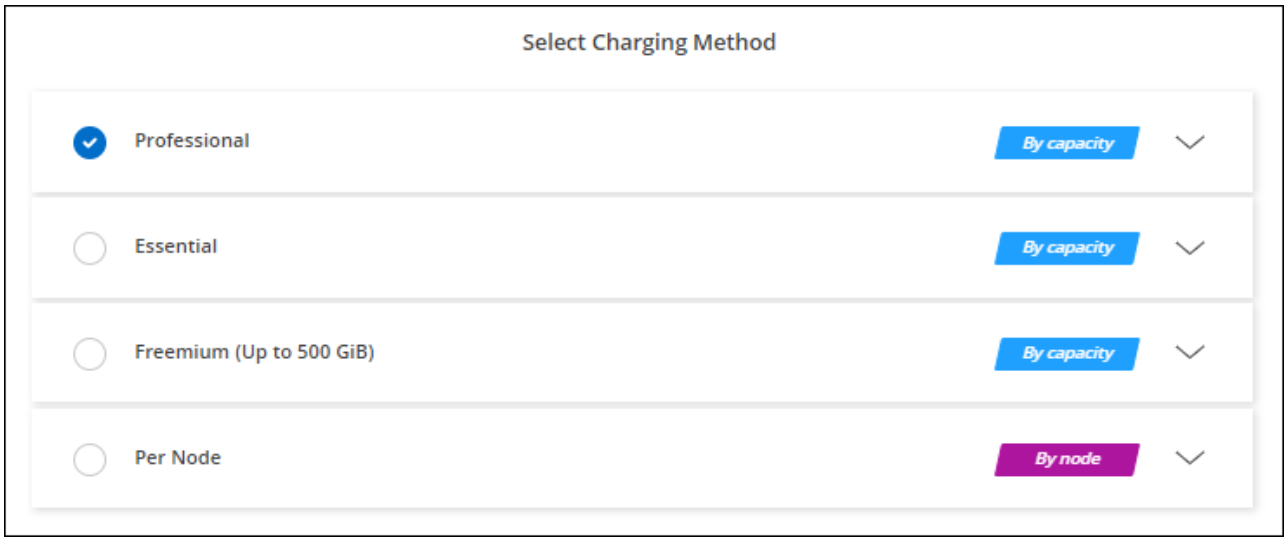
Semelhante a uma assinatura por hora, o Console solicita que você assine o contrato anual disponível no AWS Marketplace.

Passos

1. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas.
   a. Na página **Detalhes e credenciais**, clique em **Editar credenciais > Adicionar assinatura** e siga as instruções para assinar o contrato anual no AWS Marketplace.



b. Após retornar ao Console, selecione um pacote baseado em capacidade quando chegar à página de métodos de cobrança.



"Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP na AWS" .

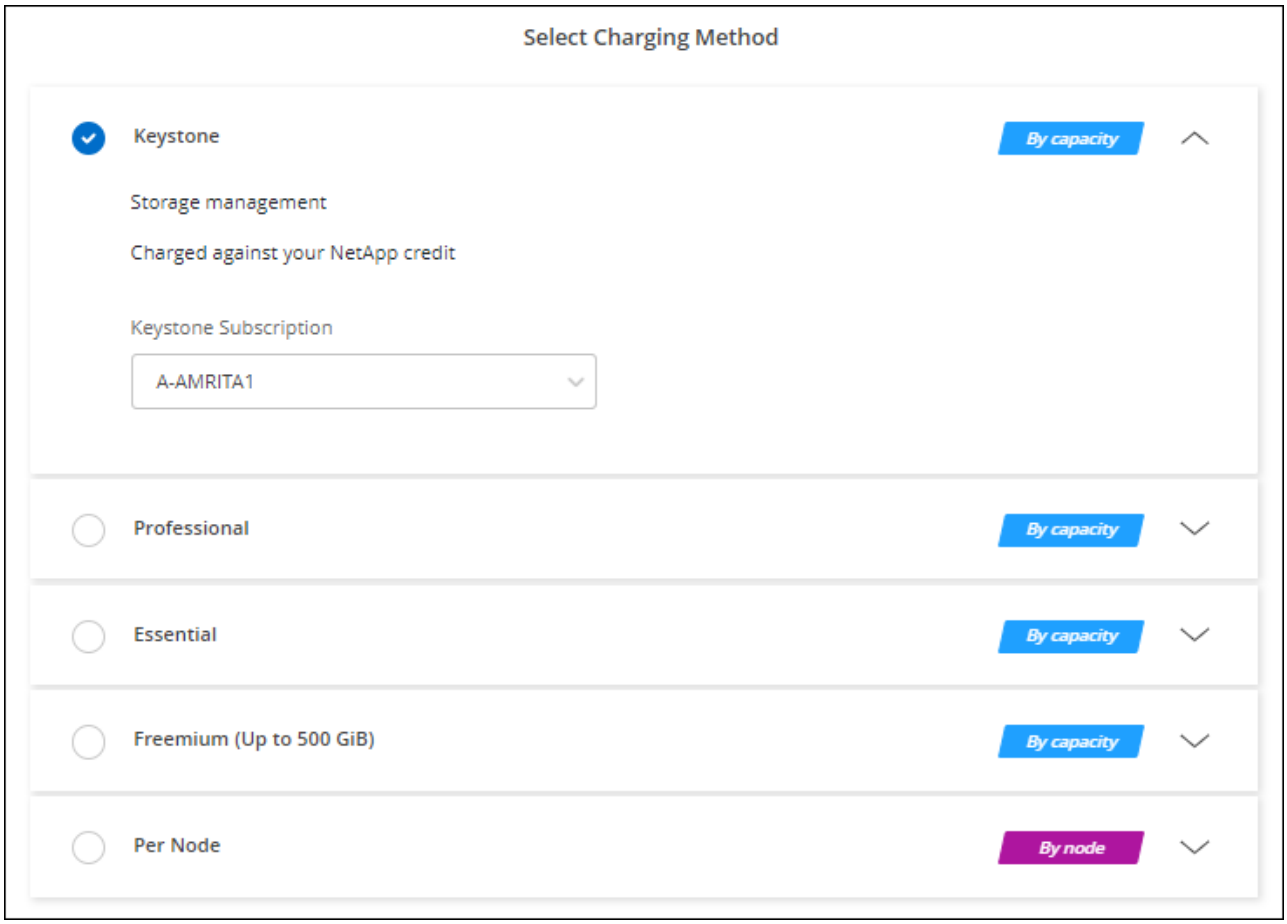
Assinatura Keystone

Uma assinatura Keystone é um serviço baseado em assinatura com pagamento conforme o crescimento. "Saiba mais sobre as assinaturas do NetApp Keystone" .

Passos

1. Se você ainda não tem uma assinatura, "entre em contato com a NetApp"
2. Entre em contato com a NetApp para autorizar sua conta de usuário com uma ou mais assinaturas Keystone .
3. Depois que a NetApp autorizar sua conta,"vincule suas assinaturas para uso com o Cloud Volumes ONTAP" .
4. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas.

    a. Selecione o método de cobrança da Assinatura Keystone quando solicitado a escolher um método de cobrança.



"Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP na AWS" .

Licença baseada em nó

Uma licença baseada em nó é a licença da geração anterior para o Cloud Volumes ONTAP. Uma licença baseada em nó pode ser adquirida da NetApp (BYOL) e está disponível para renovações de licença apenas em casos específicos. Para obter informações, consulte:

- "Fim da disponibilidade de licenças baseadas em nós"

- "Fim da disponibilidade de licenças baseadas em nós"
- "Converter uma licença baseada em nós para uma licença baseada em capacidade."

Implante o Cloud Volumes ONTAP na AWS usando implantação rápida

Você pode implantar o Cloud Volumes ONTAP na AWS usando um método de implantação rápida para configurações de nó único e de alta disponibilidade (HA). Este processo simplificado reduz as etapas de implantação em comparação ao método avançado. Ele também oferece mais clareza no fluxo de trabalho, definindo automaticamente valores padrão em uma única página e minimizando a navegação.

Antes de começar

Você precisa do seguinte para adicionar um sistema Cloud Volumes ONTAP na AWS a partir do NetApp Console.

- Um agente do Console que está ativo e em execução.
  - Você deveria ter um "Agente de console associado ao seu projeto ou área de trabalho" .
  - "Você deve estar preparado para deixar o agente do Console em execução o tempo todo" .
- Uma compreensão da configuração que você deseja usar.

  Você deve ter se preparado escolhendo uma configuração e obtendo informações de rede da AWS com seu administrador. Para mais detalhes, consulte"Planejando sua configuração do Cloud Volumes ONTAP" .
- Uma compreensão do que é necessário para configurar o licenciamento do Cloud Volumes ONTAP.

  "Aprenda como configurar o licenciamento" .
- DNS e Active Directory para configurações CIFS.

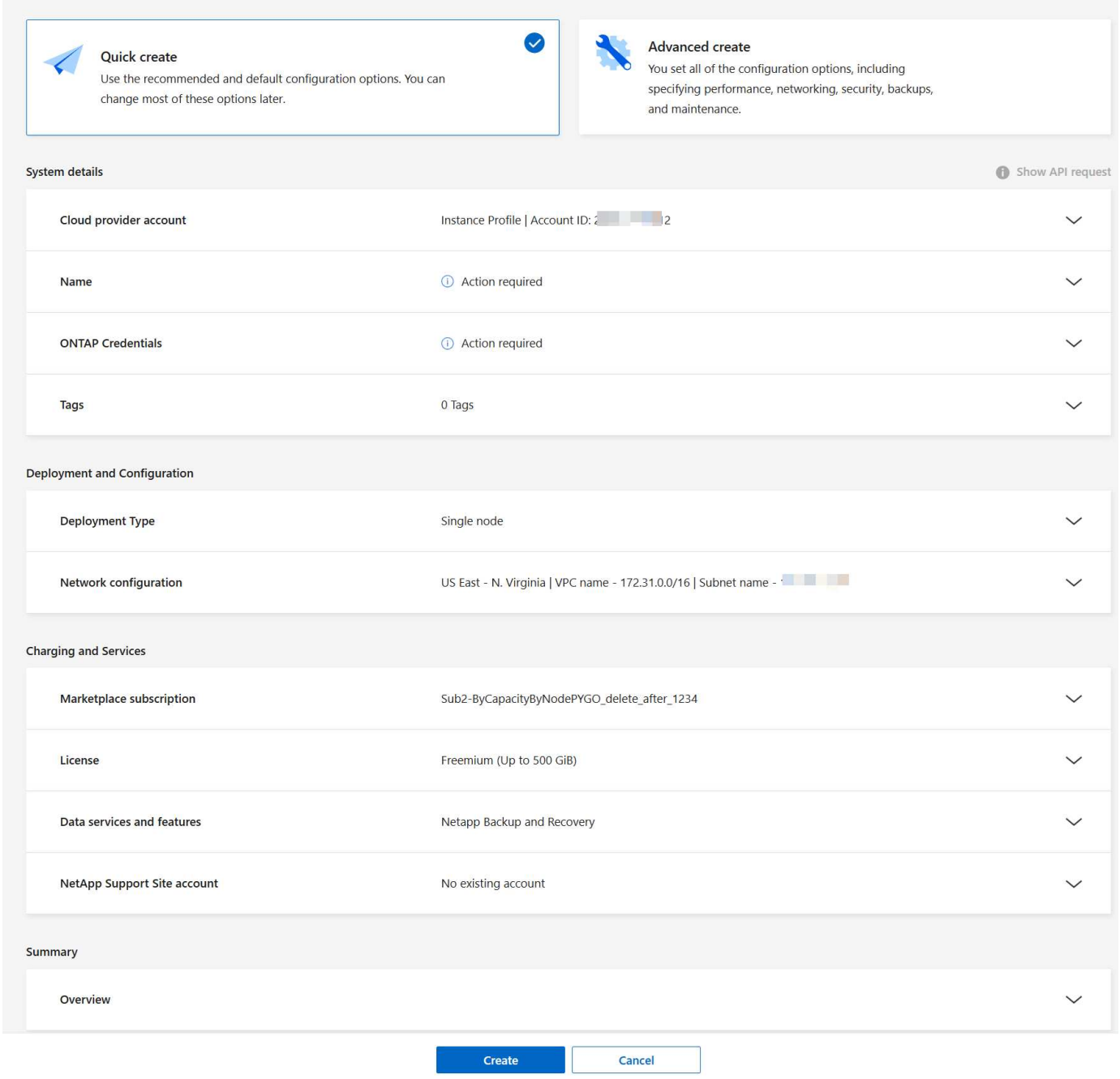
  Para mais detalhes, consulte"Requisitos de rede para Cloud Volumes ONTAP na AWS" .

Sobre esta tarefa

Imediatamente após a criação do sistema Cloud Volumes ONTAP , o NetApp Console inicia uma instância de teste na VPC especificada para verificar a conectividade. Se for bem-sucedido, o Console encerra imediatamente a instância e começa a implantar o sistema. Se o Console não puder verificar a conectividade, a criação do sistema falhará. A instância de teste é uma `t2.nano` (para locação VPC padrão) ou um `m3.medium` (para locação de VPC dedicada).

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página Canvas, clique em **Adicionar Sistema** e siga as instruções.
3. Selecione **Amazon Web Services** > * Cloud Volumes ONTAP* > **Adicionar novo**. A opção **Criação rápida** é selecionada por padrão.



detalhes do sistema

1. **Conta do provedor de nuvem**: Os detalhes da conta são preenchidos automaticamente com base no agente do Console selecionado. Se você tiver várias contas, selecione aquela que deseja usar. Se um agente do Console não estiver disponível, você será solicitado a "criar um agente de console" .
2. **Nome**: O nome do sistema. O Console usa o nome do sistema (cluster) para nomear o sistema Cloud Volumes ONTAP e a instância do Amazon EC2. Ele também usa o nome como prefixo para o grupo de segurança predefinido, se você selecionar essa opção.
3. * Credenciais ONTAP * Estas são as credenciais para a conta de administrador do cluster Cloud Volumes ONTAP . Você pode usar essas credenciais para se conectar ao Cloud Volumes ONTAP por meio do ONTAP System Manager ou do ONTAP CLI. Você pode manter o nome de usuário padrão *admin* ou alterá-lo para um nome de usuário personalizado.
4. **Tags** As tags da AWS são metadados para seus recursos da AWS. O Console adiciona as tags à instância do Cloud Volumes ONTAP e a cada recurso da AWS associado à instância. Você pode adicionar

até 15 tags da interface do usuário ao criar um sistema Cloud Volumes ONTAP e, depois, adicionar mais depois que ele for criado. Observe que a API não limita você a quatro tags ao criar um sistema. Para obter informações sobre tags, consulte "Documentação da AWS: Marcando seus recursos do Amazon EC2" .

Implantação e configuração

1. **Tipo de implantação**: selecione o tipo de implantação que você deseja usar: nó único, alta disponibilidade (HA) em uma única zona de disponibilidade (AZ) ou HA em várias AZs.
2. **Configuração de rede**: Insira as informações de rede que você registrou no "Planilha AWS" .
   a. **Região da AWS**: Por padrão, a região da conta de nuvem associada que tem VPC com recursos de sub-rede é selecionada.
   b. **VPC**: insira uma VPC para a região da AWS com uma sub-rede. Se não houver sub-redes, o valor padrão para a VPC será selecionado.
   c. **Sub-rede**: você pode selecionar uma sub-rede para a VPC somente para uma implantação de nó único ou implantação de HA em uma única AZ.

Alta disponibilidade

Se você selecionou a configuração HA, insira as seguintes informações:

HA em AZ único

1. **Acesso do mediador**: especifique as informações de acesso do mediador. O mediador é uma instância separada que monitora a integridade do par HA e fornece quorum em caso de falha. Forneça o nome do par de chaves para permitir que a instância do mediador se conecte ao serviço AWS EC2 e selecione o método de conexão.

HA em várias AZ

1. **Zonas de disponibilidade e mediador**: selecione as zonas de disponibilidade (AZs) para cada nó, o mediador e as sub-redes correspondentes onde você deseja implantar o par Cloud Volumes ONTAP HA.
2. **IPs flutuantes**: se você escolher várias AZs, especifique os endereços IP flutuantes para os serviços NFS e CIFS e para o gerenciamento de cluster e SVM. Os endereços IP devem estar fora do bloco CIDR para todas as VPCs na região. Para obter detalhes adicionais, consulte"Requisitos de rede da AWS para Cloud Volumes ONTAP HA em várias AZs" .
3. **Acesso do mediador**: especifique as informações de acesso do mediador. O mediador é uma instância separada que monitora a integridade do par HA e fornece quorum em caso de falha. Forneça o nome do par de chaves para permitir que a instância do mediador se conecte ao serviço AWS EC2 e selecione o método de conexão.
4. **Tabelas de rotas**: se você escolher várias zonas de disponibilidade, selecione as tabelas de rotas que incluem rotas para os endereços IP flutuantes. Se você tiver mais de uma tabela de rotas, é importante selecionar as tabelas de rotas corretas. Caso contrário, alguns clientes podem não ter acesso ao par Cloud Volumes ONTAP HA. Para obter mais informações sobre tabelas de rotas, consulte o "Documentação da AWS: Tabelas de rotas" .

Cobrança e Serviços

1. **Assinatura do Marketplace**: Selecione a assinatura do marketplace da AWS que você deseja usar com este sistema Cloud Volumes ONTAP .
2. **Licença**: Selecione o tipo de licença que deseja usar com este sistema Cloud Volumes ONTAP . Você pode escolher entre licenças Professional, Essential e Premium. Para obter informações sobre diferentes licenças, consulte"Saiba mais sobre as licenças do Cloud Volumes ONTAP" .

3. **Serviços e recursos de dados**: mantenha os serviços ativados ou desative os serviços que você não deseja usar com o Cloud Volumes ONTAP.
    - "Saiba mais sobre a classificação da NetApp"
    - "Saiba mais sobre o NetApp Backup and Recovery"
    - "Saiba mais sobre o armazenamento WORM no Cloud Volumes ONTAP"

    Se você quiser utilizar WORM e camadas de dados, desabilite o Backup e Recuperação e implante um sistema Cloud Volumes ONTAP com versão 9.8 ou superior.

    - * Conta do site de suporte da NetApp *: se você tiver várias contas, selecione aquela que deseja usar.

Resumo

Verifique ou edite os detalhes inseridos e clique em **Criar**.

Após a conclusão do processo de implantação, não modifique as configurações do Cloud Volumes ONTAP geradas pelo sistema no portal de nuvem da AWS, especialmente as tags do sistema. Quaisquer alterações feitas nessas configurações podem levar a comportamento inesperado ou perda de dados.

Links relacionados

- "Planejando sua configuração do Cloud Volumes ONTAP"
- "Implantar o Cloud Volumes ONTAP na AWS usando implantação avançada"

Inicie o Cloud Volumes ONTAP na AWS

Você pode iniciar o Cloud Volumes ONTAP em uma configuração de sistema único ou como um par de HA na AWS. Este método fornece uma experiência de implantação avançada que oferece mais opções de configuração e flexibilidade do que o método de implantação rápida.

Antes de começar

Você precisa do seguinte antes de começar.

- Um agente do Console que está ativo e em execução.
    - Você deveria ter um "Agente de console associado ao seu sistema" .
    - "Você deve estar preparado para deixar o agente do Console em execução o tempo todo" .
- Uma compreensão da configuração que você deseja usar.

  Você deve ter se preparado escolhendo uma configuração e obtendo informações de rede da AWS com seu administrador. Para mais detalhes, consulte"Planejando sua configuração do Cloud Volumes ONTAP" .

- Uma compreensão do que é necessário para configurar o licenciamento do Cloud Volumes ONTAP.

  "Aprenda como configurar o licenciamento" .

- DNS e Active Directory para configurações CIFS.

Para mais detalhes, consulte"Requisitos de rede para Cloud Volumes ONTAP na AWS" .

Inicie um sistema Cloud Volumes ONTAP de nó único na AWS

Se você quiser iniciar o Cloud Volumes ONTAP na AWS, precisará criar um novo sistema no NetApp Console.

Sobre esta tarefa

Imediatamente após a criação do sistema, o Console inicia uma instância de teste na VPC especificada para verificar a conectividade. Se for bem-sucedido, o Console encerra imediatamente a instância e começa a implantar o sistema Cloud Volumes ONTAP . Se a conectividade não puder ser verificada, a criação do sistema falhará. A instância de teste é uma `t2.nano` (para locação VPC padrão) ou `m3.medium` (para locação de VPC dedicada).

Passos

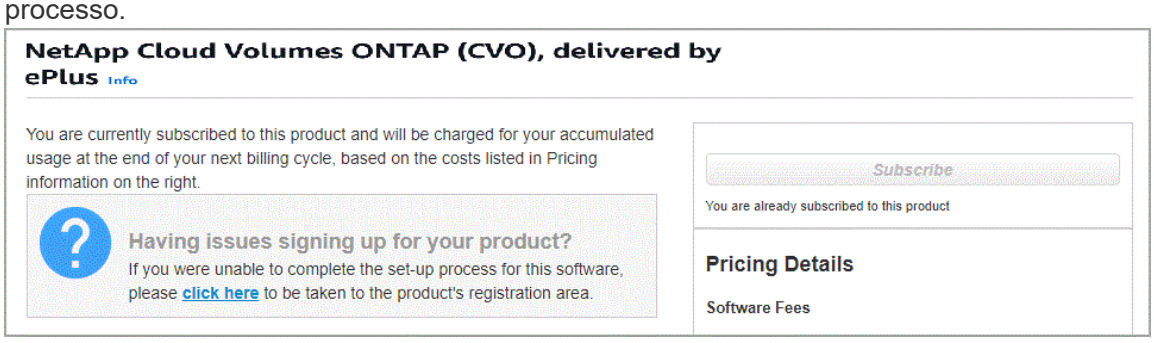
1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as instruções.
3. Selecione **Amazon Web Services** e * Cloud Volumes ONTAP Single Node*.
4. Selecione **Criação avançada**. Como o modo **Criação rápida** é selecionado por padrão, você pode ver uma mensagem para valores padrão. Clique em **Continuar**.
5. Se você for solicitado, "criar um agente de console" .
6. **Detalhes e credenciais**: Opcionalmente, altere as credenciais e a assinatura da AWS, insira um nome de sistema, adicione tags, se necessário, e insira uma senha.

   Alguns campos nesta página são autoexplicativos. A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Nome do sistema	O Console usa o nome do sistema para nomear o sistema Cloud Volumes ONTAP e a instância do Amazon EC2. Ele também usa o nome como prefixo para o grupo de segurança predefinido, se você selecionar essa opção.
Adicionar tags	As tags da AWS são metadados para seus recursos da AWS. O Console adiciona as tags à instância do Cloud Volumes ONTAP e a cada recurso da AWS associado à instância. Você pode adicionar até quatro tags da interface do usuário ao criar um sistema e depois adicionar mais depois que ele for criado. Observe que a API não limita você a quatro tags ao criar um sistema. Para obter informações sobre tags, consulte "Documentação da AWS: Marcando seus recursos do Amazon EC2" .
Nome de usuário e senha	Estas são as credenciais para a conta de administrador do cluster Cloud Volumes ONTAP . Você pode usar essas credenciais para se conectar ao Cloud Volumes ONTAP por meio do ONTAP System Manager ou do ONTAP CLI. Mantenha o nome de usuário padrão *admin* ou altere-o para um nome de usuário personalizado.

Campo	Descrição
Editar credenciais	Escolha as credenciais da AWS associadas à conta onde você deseja implantar este sistema. Você também pode associar a assinatura do marketplace da AWS para usar com este sistema Cloud Volumes ONTAP . Clique em **Adicionar Assinatura** para associar as credenciais selecionadas a uma nova assinatura do marketplace da AWS. A assinatura pode ser para um contrato anual ou para pagar o Cloud Volumes ONTAP por hora. "Aprenda como adicionar credenciais adicionais da AWS ao NetApp Console" .

Se vários usuários do IAM trabalharem na mesma conta da AWS, cada usuário precisará se inscrever. Depois que o primeiro usuário se inscreve, o marketplace da AWS informa os usuários subsequentes que eles já estão inscritos, conforme mostrado na imagem abaixo. Enquanto uma assinatura estiver em vigor para a *conta* da AWS, cada usuário do IAM precisa se associar a essa assinatura. Se você vir a mensagem mostrada abaixo, clique no link **clique aqui** para acessar o site do Console e concluir o processo.



7. **Serviços**: mantenha os serviços habilitados ou desabilite os serviços individuais que você não deseja usar com o Cloud Volumes ONTAP.
   - "Saiba mais sobre a NetApp Data Classification"
   - "Saiba mais sobre o NetApp Backup and Recovery"

   Se você quiser utilizar WORM e camadas de dados, desabilite o Backup e Recuperação e implante um sistema Cloud Volumes ONTAP com versão 9.8 ou superior.

8. **Localização e conectividade**: insira as informações de rede que você registrou no "Planilha AWS" .

   A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
VPC	Se você tiver um AWS Outpost, poderá implantar um sistema Cloud Volumes ONTAP de nó único nesse Outpost selecionando a VPC do Outpost. A experiência é a mesma de qualquer outra VPC que reside na AWS.

Campo	Descrição
Grupo de segurança gerado	Se você deixar o Console gerar o grupo de segurança para você, precisará escolher como permitirá o tráfego: • Se você escolher **Somente VPC selecionada**, a origem do tráfego de entrada será o intervalo de sub-rede da VPC selecionada e o intervalo de sub-rede da VPC onde o agente do Console reside. Esta é a opção recomendada. • Se você escolher **Todas as VPCs**, a origem do tráfego de entrada será o intervalo de IP 0.0.0.0/0.
Usar grupo de segurança existente	Se você usar uma política de firewall existente, certifique-se de que ela inclua as regras necessárias. "Saiba mais sobre as regras de firewall para o Cloud Volumes ONTAP" .

9. **Criptografia de dados**: escolha nenhuma criptografia de dados ou criptografia gerenciada pela AWS.

   Para criptografia gerenciada pela AWS, você pode escolher uma Chave Mestra do Cliente (CMK) diferente da sua conta ou de outra conta da AWS.

   Não é possível alterar o método de criptografia de dados da AWS depois de criar um sistema Cloud Volumes ONTAP .

   "Aprenda a configurar o AWS KMS para Cloud Volumes ONTAP" .

   "Saiba mais sobre as tecnologias de criptografia suportadas" .

10. **Métodos de cobrança e conta NSS**: especifique qual opção de cobrança você gostaria de usar com este sistema e, em seguida, especifique uma conta do site de suporte da NetApp .
    - "Saiba mais sobre as opções de licenciamento do Cloud Volumes ONTAP" .
    - "Aprenda como configurar o licenciamento" .
11. * Configuração do Cloud Volumes ONTAP * (somente contrato anual do marketplace da AWS): revise a configuração padrão e clique em **Continuar** ou clique em **Alterar configuração** para selecionar sua própria configuração.

    Se você mantiver a configuração padrão, precisará apenas especificar um volume e depois revisar e aprovar a configuração.

12. **Pacotes pré-configurados**: selecione um dos pacotes para iniciar rapidamente o Cloud Volumes ONTAP ou clique em **Alterar configuração** para selecionar sua própria configuração.

    Se você escolher um dos pacotes, precisará apenas especificar um volume e depois revisar e aprovar a configuração.

13. **Função do IAM**: É melhor manter a opção padrão para deixar o Console criar a função para você.

    Se você preferir usar sua própria apólice, ela deve atender"requisitos de política para nós Cloud Volumes ONTAP" .

14. **Licenciamento**: Altere a versão do Cloud Volumes ONTAP conforme necessário e selecione um tipo de instância e a locação da instância.

Se uma versão mais recente do Release Candidate, Disponibilidade Geral ou patch estiver disponível para a versão selecionada, o Console atualizará o sistema para essa versão ao criá-lo. Por exemplo, a atualização ocorre se você selecionar Cloud Volumes ONTAP 9.13.1 e 9.13.1 P4 estiver disponível. A atualização não ocorre de uma versão para outra, por exemplo, da 9.13 para a 9.14.

15. **Recursos de armazenamento subjacentes**: escolha um tipo de disco, configure o armazenamento subjacente e escolha se deseja manter a hierarquização de dados ativada.

    Observe o seguinte:

    - O tipo de disco é para o volume inicial (e agregado). Você pode escolher um tipo de disco diferente para volumes subsequentes (e agregados).
    - Se você escolher um disco gp3 ou io1, o Console usará o recurso Elastic Volumes na AWS para aumentar automaticamente a capacidade do disco de armazenamento subjacente, conforme necessário. Você pode escolher a capacidade inicial com base em suas necessidades de armazenamento e revisá-la após a implantação do Cloud Volumes ONTAP . "Saiba mais sobre o suporte para Elastic Volumes na AWS" .
    - Se você escolher um disco gp2 ou st1, poderá selecionar um tamanho de disco para todos os discos no agregado inicial e para quaisquer agregados adicionais que o Console criar quando você usar a opção de provisionamento simples. Você pode criar agregados que usam um tamanho de disco diferente usando a opção de alocação avançada.
    - Você pode escolher uma política específica de níveis de volume ao criar ou editar um volume.
    - Se você desabilitar a hierarquização de dados, poderá habilitá-la em agregações subsequentes.

      "Aprenda como funciona a hierarquização de dados" .

16. **Velocidade de gravação e WORM**:

    a. Escolha a velocidade de gravação **Normal** ou **Alta**, se desejar.

       "Saiba mais sobre velocidade de gravação" .

    b. Ative o armazenamento WORM (escreva uma vez e leia muitas vezes), se desejar.

       O WORM não pode ser habilitado se a hierarquização de dados estiver habilitada para as versões 9.7 e anteriores do Cloud Volumes ONTAP . A reversão ou o downgrade para o Cloud Volumes ONTAP 9.8 é bloqueado após a ativação do WORM e da hierarquização.

    "Saiba mais sobre o armazenamento WORM" .

    a. Se você ativar o armazenamento WORM, selecione o período de retenção.

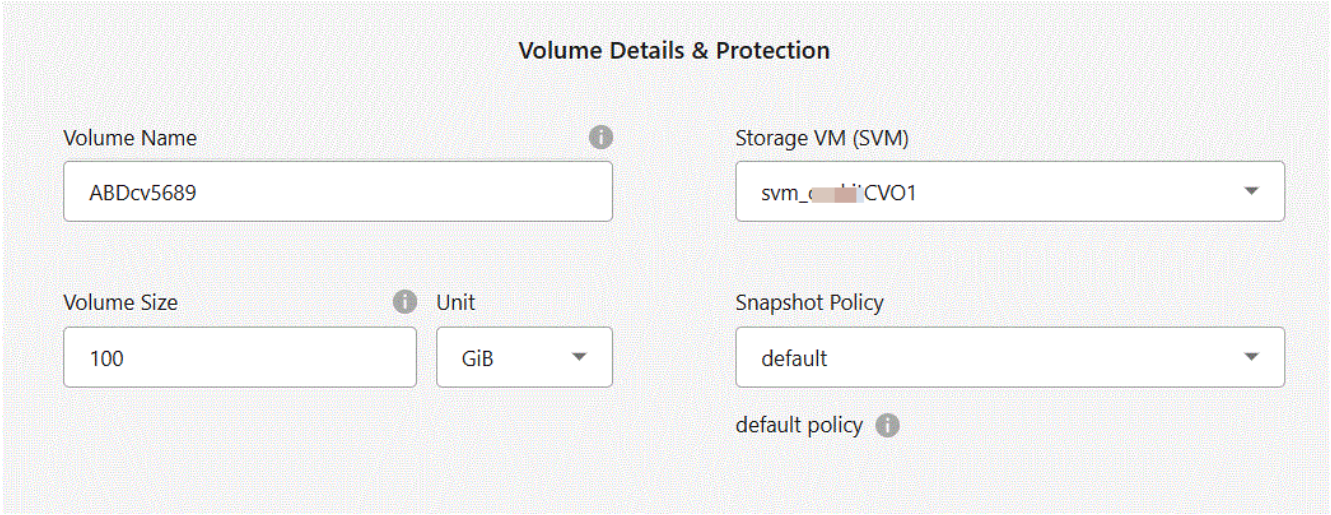
17. **Criar volume**: insira detalhes para o novo volume ou clique em **Ignorar**.

    "Saiba mais sobre os protocolos e versões de clientes suportados" .

    Alguns campos nesta página são autoexplicativos. A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Tamanho	O tamanho máximo que você pode inserir depende muito se você habilita o provisionamento fino, que permite criar um volume maior que o armazenamento físico disponível atualmente.
Controle de acesso (somente para NFS)	Uma política de exportação define os clientes na sub-rede que podem acessar o volume. Por padrão, o Console insere um valor que fornece acesso a todas as instâncias na sub-rede.
Permissões e usuários/grupos (somente para CIFS)	Esses campos permitem que você controle o nível de acesso a um compartilhamento para usuários e grupos (também chamados de listas de controle de acesso ou ACLs). Você pode especificar usuários ou grupos locais ou de domínio do Windows, ou usuários ou grupos do UNIX. Se você especificar um nome de usuário de domínio do Windows, deverá incluir o domínio do usuário usando o formato domínio\nome de usuário.
Política de Snapshot	Uma política de cópia de instantâneo especifica a frequência e o número de cópias de instantâneo do NetApp criadas automaticamente. Uma cópia do NetApp Snapshot é uma imagem do sistema de arquivos de um momento específico que não tem impacto no desempenho e requer armazenamento mínimo. Você pode escolher a política padrão ou nenhuma. Você pode escolher nenhum para dados transitórios: por exemplo, tempdb para Microsoft SQL Server.
Opções avançadas (somente para NFS)	Selecione uma versão do NFS para o volume: NFSv3 ou NFSv4.
Grupo iniciador e IQN (somente para iSCSI)	Os destinos de armazenamento iSCSI são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Os grupos de iniciadores são tabelas de nomes de nós de host iSCSI e controlam quais iniciadores têm acesso a quais LUNs. Os destinos iSCSI se conectam à rede por meio de adaptadores de rede Ethernet padrão (NICs), placas de mecanismo de descarregamento TCP (TOE) com iniciadores de software, adaptadores de rede convergentes (CNAs) ou adaptadores de bust de host dedicados (HBAs) e são identificados por nomes qualificados iSCSI (IQNs). Quando você cria um volume iSCSI, o Console cria automaticamente um LUN para você. Simplificamos criando apenas um LUN por volume, portanto não há gerenciamento envolvido. Depois de criar o volume,"use o IQN para conectar-se ao LUN de seus hosts" .

A imagem a seguir mostra a primeira página do assistente de criação de volume:



18. **Configuração CIFS**: Se você escolher o protocolo CIFS, configure um servidor CIFS.

Campo	Descrição
Endereço IP primário e secundário do DNS	Os endereços IP dos servidores DNS que fornecem resolução de nomes para o servidor CIFS. Os servidores DNS listados devem conter os registros de localização de serviço (SRV) necessários para localizar os servidores LDAP do Active Directory e os controladores de domínio para o domínio ao qual o servidor CIFS se juntará.
Domínio do Active Directory para ingressar	O FQDN do domínio do Active Directory (AD) ao qual você deseja que o servidor CIFS ingresse.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com privilégios suficientes para adicionar computadores à Unidade Organizacional (UO) especificada dentro do domínio do AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio do AD.
Unidade Organizacional	A unidade organizacional dentro do domínio do AD a ser associada ao servidor CIFS. O padrão é CN=Computadores. Se você configurar o AWS Managed Microsoft AD como o servidor AD para o Cloud Volumes ONTAP, deverá inserir **OU=Computers,OU=corp** neste campo.
Domínio DNS	O domínio DNS para a máquina virtual de armazenamento (SVM) do Cloud Volumes ONTAP . Na maioria dos casos, o domínio é o mesmo que o domínio do AD.
Servidor NTP	Selecione **Usar domínio do Active Directory** para configurar um servidor NTP usando o DNS do Active Directory. Se você precisar configurar um servidor NTP usando um endereço diferente, use a API. Consulte o "Documentação de automação do NetApp Console" para mais detalhes. Observe que você só pode configurar um servidor NTP ao criar um servidor CIFS. Não é configurável depois de criar o servidor CIFS.

19. **Perfil de uso, tipo de disco e política de camadas**: escolha se deseja habilitar recursos de eficiência de armazenamento e editar a política de camadas de volume, se necessário.

    Para mais informações, consulte"Compreendendo os perfis de uso de volume" ,"Visão geral da hierarquização de dados" , e "KB: Quais recursos de eficiência de armazenamento em linha são

suportados pelo CVO?"

20. **Revisar e aprovar**: revise e confirme suas seleções.
    a. Revise os detalhes sobre a configuração.
    b. Clique em **Mais informações** para revisar detalhes sobre o suporte e os recursos da AWS que o Console comprará.
    c. Selecione as caixas de seleção **Eu entendo…**.
    d. Clique em **Ir**.

Resultado

O Console inicia a instância do Cloud Volumes ONTAP . Você pode acompanhar o progresso na página **Auditoria**.

Se você tiver problemas para iniciar a instância do Cloud Volumes ONTAP , revise a mensagem de falha. Você também pode selecionar o sistema e clicar em **Recriar ambiente**.

Para obter ajuda adicional, acesse "Suporte NetApp Cloud Volumes ONTAP" .

Após a conclusão do processo de implantação, não modifique as configurações do Cloud Volumes ONTAP geradas pelo sistema no portal de nuvem da AWS, especialmente as tags do sistema. Quaisquer alterações feitas nessas configurações podem levar a comportamento inesperado ou perda de dados.

Depois que você terminar

- Se você provisionou um compartilhamento CIFS, conceda aos usuários ou grupos permissões para os arquivos e pastas e verifique se esses usuários podem acessar o compartilhamento e criar um arquivo.
- Se você quiser aplicar cotas aos volumes, use o ONTAP System Manager ou o ONTAP CLI.

  As cotas permitem que você restrinja ou rastreie o espaço em disco e o número de arquivos usados por um usuário, grupo ou qtree.

Inicie um par de Cloud Volumes ONTAP HA na AWS

Se você quiser iniciar um par de HA do Cloud Volumes ONTAP na AWS, precisará criar um sistema de HA no Console.

Limitação

No momento, os pares HA não são suportados pelo AWS Outposts.

Sobre esta tarefa

Imediatamente após a criação do sistema Cloud Volumes ONTAP , o Console inicia uma instância de teste na VPC especificada para verificar a conectividade. Se for bem-sucedido, o Console encerra imediatamente a instância e começa a implantar o sistema Cloud Volumes ONTAP . Se a conectividade não puder ser verificada, a criação do sistema falhará. A instância de teste é uma `t2.nano` (para locação VPC padrão) ou `m3.medium` (para locação de VPC dedicada).

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as instruções.

3. Selecione **Amazon Web Services** e * Cloud Volumes ONTAP HA*.

   Algumas zonas locais da AWS estão disponíveis.

   Antes de poder usar as Zonas Locais da AWS, você deve habilitar as Zonas Locais e criar uma sub-rede na Zona Local na sua conta da AWS. Siga as etapas **Optar por uma zona local da AWS** e **Estender sua Amazon VPC para a zona local** no"Tutorial da AWS "Comece a implantar aplicativos de baixa latência com zonas locais da AWS"" .

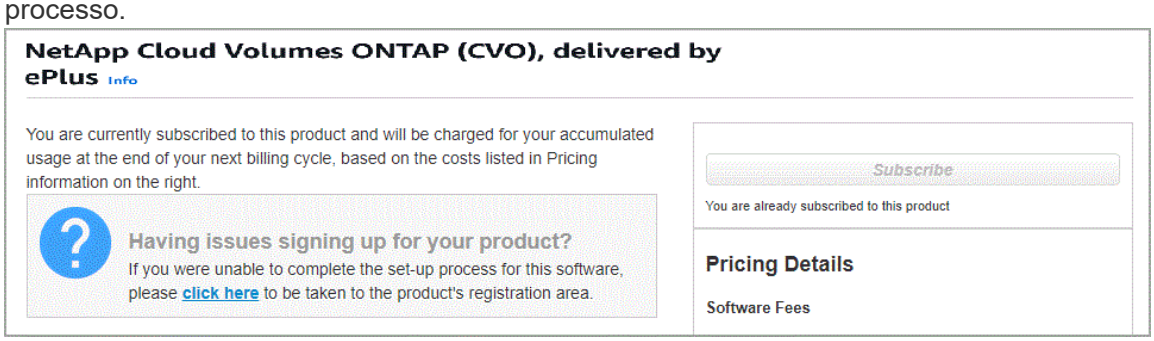
   Se você estiver executando o agente do Console 3.9.36 ou inferior, será necessário adicionar o `DescribeAvailabilityZones` permissão para a função AWS no console AWS EC2.

4. **Detalhes e credenciais**: Opcionalmente, altere as credenciais e a assinatura da AWS, insira um nome de sistema, adicione tags, se necessário, e insira uma senha.

   Alguns campos nesta página são autoexplicativos. A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Nome do sistema	O Console usa o nome do sistema para nomear o sistema Cloud Volumes ONTAP e a instância do Amazon EC2. Ele também usa o nome como prefixo para o grupo de segurança predefinido, se você selecionar essa opção.
Adicionar tags	As tags da AWS são metadados para seus recursos da AWS. O Console adiciona as tags à instância do Cloud Volumes ONTAP e a cada recurso da AWS associado à instância. Você pode adicionar até quatro tags da interface do usuário ao criar um sistema e depois adicionar mais depois que ele for criado. Observe que a API não limita você a quatro tags ao criar um sistema. Para obter informações sobre tags, consulte "Documentação da AWS: Marcando seus recursos do Amazon EC2" .
Nome de usuário e senha	Estas são as credenciais para a conta de administrador do cluster Cloud Volumes ONTAP . Você pode usar essas credenciais para se conectar ao Cloud Volumes ONTAP por meio do ONTAP System Manager ou do ONTAP CLI. Mantenha o nome de usuário padrão *admin* ou altere-o para um nome de usuário personalizado.
Editar credenciais	Selecione as credenciais da AWS e a assinatura do marketplace para usar com este sistema Cloud Volumes ONTAP . Clique em **Adicionar Assinatura** para associar as credenciais selecionadas a uma nova assinatura do marketplace da AWS. A assinatura pode ser para um contrato anual ou para pagar o Cloud Volumes ONTAP por hora. Se você adquiriu uma licença diretamente da NetApp (traga sua própria licença (BYOL)), não é necessária uma assinatura da AWS. A NetApp restringiu a compra, extensão e renovação de licenças BYOL. Para obter mais informações, consulte "Disponibilidade restrita de licenciamento BYOL para Cloud Volumes ONTAP" . "Aprenda como adicionar credenciais adicionais da AWS ao Console" .

Se vários usuários do IAM trabalharem na mesma conta da AWS, cada usuário precisará se inscrever. Depois que o primeiro usuário se inscreve, o marketplace da AWS informa os usuários subsequentes que eles já estão inscritos, conforme mostrado na imagem abaixo. Enquanto uma assinatura estiver em vigor para a *conta* da AWS, cada usuário do IAM precisa se associar a essa assinatura. Se você vir a mensagem mostrada abaixo, clique no link **clique aqui** para acessar o site do Console e concluir o processo.



5. **Serviços**: Mantenha os serviços ativados ou desative os serviços individuais que você não deseja usar com este sistema Cloud Volumes ONTAP .
   - "Saiba mais sobre a NetApp Data Classification"
   - "Saiba mais sobre backup e recuperação"

   Se você quiser utilizar WORM e camadas de dados, desabilite o Backup e Recuperação e implante um sistema Cloud Volumes ONTAP com versão 9.8 ou superior.

6. **Modelos de implantação de HA**: escolha uma configuração de HA.

   Para uma visão geral dos modelos de implantação, consulte"Cloud Volumes ONTAP HA para AWS" .

7. **Localização e conectividade** (zona de disponibilidade única (AZ)) ou **Região e VPC** (várias AZs): insira as informações de rede que você registrou na planilha da AWS.

   A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Grupo de segurança gerado	Se você deixar o Console gerar o grupo de segurança para você, precisará escolher como permitirá o tráfego: • Se você escolher **Somente VPC selecionada**, a origem do tráfego de entrada será o intervalo de sub-rede da VPC selecionada e o intervalo de sub-rede da VPC onde o agente do Console reside. Esta é a opção recomendada. • Se você escolher **Todas as VPCs**, a origem do tráfego de entrada será o intervalo de IP 0.0.0.0/0.
Usar grupo de segurança existente	Se você usar uma política de firewall existente, certifique-se de que ela inclua as regras necessárias. "Saiba mais sobre as regras de firewall para o Cloud Volumes ONTAP" .

8. **Conectividade e autenticação SSH**: escolha métodos de conexão para o par HA e o mediador.

9. **IPs flutuantes**: Se você escolher várias AZs, especifique os endereços IP flutuantes.

   Os endereços IP devem estar fora do bloco CIDR para todas as VPCs na região. Para obter detalhes adicionais, consulte"Requisitos de rede da AWS para Cloud Volumes ONTAP HA em várias AZs" .

10. **Tabelas de rotas**: Se você escolher várias zonas de disponibilidade, selecione as tabelas de rotas que devem incluir rotas para os endereços IP flutuantes.

    Se você tiver mais de uma tabela de rotas, é muito importante selecionar as tabelas de rotas corretas. Caso contrário, alguns clientes podem não ter acesso ao par Cloud Volumes ONTAP HA. Para obter mais informações sobre tabelas de rotas, consulte o "Documentação da AWS: Tabelas de rotas" .

11. **Criptografia de dados**: escolha nenhuma criptografia de dados ou criptografia gerenciada pela AWS.

    Para criptografia gerenciada pela AWS, você pode escolher uma Chave Mestra do Cliente (CMK) diferente da sua conta ou de outra conta da AWS.

    > Não é possível alterar o método de criptografia de dados da AWS depois de criar um sistema Cloud Volumes ONTAP .

    "Aprenda a configurar o AWS KMS para Cloud Volumes ONTAP" .

    "Saiba mais sobre as tecnologias de criptografia suportadas" .

12. **Métodos de cobrança e conta NSS**: especifique qual opção de cobrança você gostaria de usar com este sistema e, em seguida, especifique uma conta do site de suporte da NetApp .
    - "Saiba mais sobre as opções de licenciamento do Cloud Volumes ONTAP" .
    - "Aprenda como configurar o licenciamento" .
13. * Configuração do Cloud Volumes ONTAP * (somente contrato anual do AWS Marketplace): revise a configuração padrão e clique em **Continuar** ou clique em **Alterar configuração** para selecionar sua própria configuração.

    Se você mantiver a configuração padrão, precisará apenas especificar um volume e depois revisar e aprovar a configuração.

14. **Pacotes pré-configurados** (somente por hora ou BYOL): Selecione um dos pacotes para iniciar rapidamente o Cloud Volumes ONTAP ou clique em **Alterar configuração** para selecionar sua própria configuração.

    Se você escolher um dos pacotes, precisará apenas especificar um volume e depois revisar e aprovar a configuração.

15. **Função do IAM**: É melhor manter a opção padrão para deixar o Console criar a função para você.

    Se você preferir usar sua própria apólice, ela deve atender"requisitos de política para nós Cloud Volumes ONTAP e o mediador HA" .

16. **Licenciamento**: Altere a versão do Cloud Volumes ONTAP conforme necessário e selecione um tipo de instância e a locação da instância.

Se uma versão mais recente do Release Candidate, Disponibilidade Geral ou patch estiver disponível para a versão selecionada, o Console atualizará o sistema para essa versão ao criá-lo. Por exemplo, a atualização ocorre se você selecionar Cloud Volumes ONTAP 9.13.1 e 9.13.1 P4 estiver disponível. A atualização não ocorre de uma versão para outra, por exemplo, da 9.13 para a 9.14.

17. **Recursos de armazenamento subjacentes**: escolha um tipo de disco, configure o armazenamento subjacente e escolha se deseja manter a hierarquização de dados ativada.

    Observe o seguinte:

    - O tipo de disco é para o volume inicial (e agregado). Você pode escolher um tipo de disco diferente para volumes subsequentes (e agregados).
    - Se você escolher um disco gp3 ou io1, o Console usará o recurso Elastic Volumes na AWS para aumentar automaticamente a capacidade do disco de armazenamento subjacente, conforme necessário. Você pode escolher a capacidade inicial com base em suas necessidades de armazenamento e revisá-la após a implantação do Cloud Volumes ONTAP . "Saiba mais sobre o suporte para Elastic Volumes na AWS" .
    - Se você escolher um disco gp2 ou st1, poderá selecionar um tamanho de disco para todos os discos no agregado inicial e para quaisquer agregados adicionais que o Console criar quando você usar a opção de provisionamento simples. Você pode criar agregados que usam um tamanho de disco diferente usando a opção de alocação avançada.
    - Você pode escolher uma política específica de níveis de volume ao criar ou editar um volume.
    - Se você desabilitar a hierarquização de dados, poderá habilitá-la em agregações subsequentes.

      "Aprenda como funciona a hierarquização de dados" .

18. **Velocidade de gravação e WORM**:

    a. Escolha a velocidade de gravação **Normal** ou **Alta**, se desejar.

       "Saiba mais sobre velocidade de gravação" .

    b. Ative o armazenamento WORM (escreva uma vez e leia muitas vezes), se desejar.

       O WORM não pode ser habilitado se a hierarquização de dados estiver habilitada para as versões 9.7 e anteriores do Cloud Volumes ONTAP . A reversão ou o downgrade para o Cloud Volumes ONTAP 9.8 é bloqueado após a ativação do WORM e da hierarquização.

    "Saiba mais sobre o armazenamento WORM" .

    a. Se você ativar o armazenamento WORM, selecione o período de retenção.

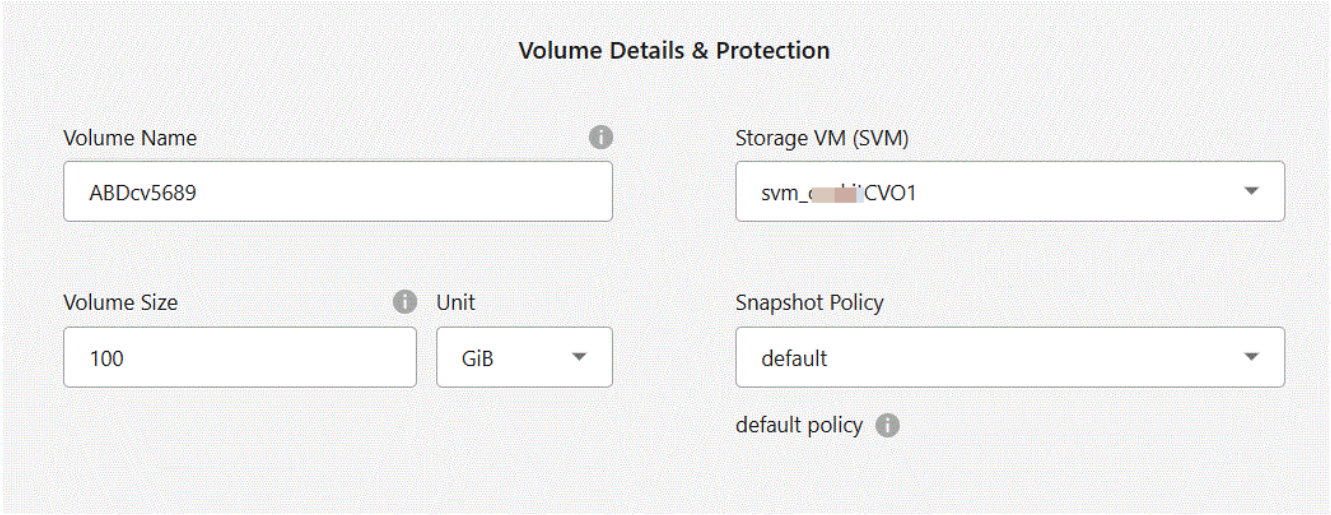
19. **Criar volume**: insira detalhes para o novo volume ou clique em **Ignorar**.

    "Saiba mais sobre os protocolos e versões de clientes suportados" .

    Alguns campos nesta página são autoexplicativos. A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Tamanho	O tamanho máximo que você pode inserir depende muito se você habilita o provisionamento fino, que permite criar um volume maior que o armazenamento físico disponível atualmente.
Controle de acesso (somente para NFS)	Uma política de exportação define os clientes na sub-rede que podem acessar o volume. Por padrão, o Console insere um valor que fornece acesso a todas as instâncias na sub-rede.
Permissões e usuários/grupos (somente para CIFS)	Esses campos permitem que você controle o nível de acesso a um compartilhamento para usuários e grupos (também chamados de listas de controle de acesso ou ACLs). Você pode especificar usuários ou grupos locais ou de domínio do Windows, ou usuários ou grupos do UNIX. Se você especificar um nome de usuário de domínio do Windows, deverá incluir o domínio do usuário usando o formato domínio\nome de usuário.
Política de Snapshot	Uma política de cópia de instantâneo especifica a frequência e o número de cópias de instantâneo do NetApp criadas automaticamente. Uma cópia do NetApp Snapshot é uma imagem do sistema de arquivos de um momento específico que não tem impacto no desempenho e requer armazenamento mínimo. Você pode escolher a política padrão ou nenhuma. Você pode escolher nenhum para dados transitórios: por exemplo, tempdb para Microsoft SQL Server.
Opções avançadas (somente para NFS)	Selecione uma versão do NFS para o volume: NFSv3 ou NFSv4.
Grupo iniciador e IQN (somente para iSCSI)	Os destinos de armazenamento iSCSI são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Os grupos de iniciadores são tabelas de nomes de nós de host iSCSI e controlam quais iniciadores têm acesso a quais LUNs. Os destinos iSCSI se conectam à rede por meio de adaptadores de rede Ethernet padrão (NICs), placas de mecanismo de descarregamento TCP (TOE) com iniciadores de software, adaptadores de rede convergentes (CNAs) ou adaptadores de bust de host dedicados (HBAs) e são identificados por nomes qualificados iSCSI (IQNs). Quando você cria um volume iSCSI, o Console cria automaticamente um LUN para você. Simplificamos criando apenas um LUN por volume, portanto não há gerenciamento envolvido. Depois de criar o volume,"use o IQN para conectar-se ao LUN de seus hosts" .

A imagem a seguir mostra a primeira página do assistente de criação de volume:



20. **Configuração CIFS**: Se você selecionou o protocolo CIFS, configure um servidor CIFS.

Campo	Descrição
Endereço IP primário e secundário do DNS	Os endereços IP dos servidores DNS que fornecem resolução de nomes para o servidor CIFS. Os servidores DNS listados devem conter os registros de localização de serviço (SRV) necessários para localizar os servidores LDAP do Active Directory e os controladores de domínio para o domínio ao qual o servidor CIFS se juntará.
Domínio do Active Directory para ingressar	O FQDN do domínio do Active Directory (AD) ao qual você deseja que o servidor CIFS ingresse.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com privilégios suficientes para adicionar computadores à Unidade Organizacional (UO) especificada dentro do domínio do AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio do AD.
Unidade Organizacional	A unidade organizacional dentro do domínio do AD a ser associada ao servidor CIFS. O padrão é CN=Computadores. Se você configurar o AWS Managed Microsoft AD como o servidor AD para o Cloud Volumes ONTAP, deverá inserir **OU=Computers,OU=corp** neste campo.
Domínio DNS	O domínio DNS para a máquina virtual de armazenamento (SVM) do Cloud Volumes ONTAP . Na maioria dos casos, o domínio é o mesmo que o domínio do AD.
Servidor NTP	Selecione **Usar domínio do Active Directory** para configurar um servidor NTP usando o DNS do Active Directory. Se você precisar configurar um servidor NTP usando um endereço diferente, use a API. Consulte o "Documentação de automação do NetApp Console" para mais detalhes. Observe que você só pode configurar um servidor NTP ao criar um servidor CIFS. Não é configurável depois de criar o servidor CIFS.

21. **Perfil de uso, tipo de disco e política de camadas**: escolha se deseja habilitar recursos de eficiência de armazenamento e editar a política de camadas de volume, se necessário.

    Para mais informações, consulte"Escolha um perfil de uso de volume" e"Visão geral da hierarquização de dados" .

22. **Revisar e aprovar**: revise e confirme suas seleções.
    a. Revise os detalhes sobre a configuração.
    b. Clique em **Mais informações** para revisar detalhes sobre o suporte e os recursos da AWS que o Console comprará.
    c. Selecione as caixas de seleção **Eu entendo…**.
    d. Clique em **Ir**.

Resultado

O Console inicia o par Cloud Volumes ONTAP HA. Você pode acompanhar o progresso na página **Auditoria**.

Se você tiver algum problema ao iniciar o par HA, revise a mensagem de falha. Você também pode selecionar o sistema e clicar em Recriar ambiente.

Para obter ajuda adicional, acesse "Suporte NetApp Cloud Volumes ONTAP" .

Depois que você terminar

- Se você provisionou um compartilhamento CIFS, conceda aos usuários ou grupos permissões para os arquivos e pastas e verifique se esses usuários podem acessar o compartilhamento e criar um arquivo.
- Se você quiser aplicar cotas aos volumes, use o ONTAP System Manager ou o ONTAP CLI.

  As cotas permitem que você restrinja ou rastreie o espaço em disco e o número de arquivos usados por um usuário, grupo ou qtree.

> Após a conclusão do processo de implantação, não modifique as configurações do Cloud Volumes ONTAP geradas pelo sistema no portal de nuvem da AWS, especialmente as tags do sistema. Quaisquer alterações feitas nessas configurações podem levar a comportamento inesperado ou perda de dados.

Links relacionados

- "Planejando sua configuração do Cloud Volumes ONTAP"
- "Implante o Cloud Volumes ONTAP na AWS usando implantação rápida"

Implantar o Cloud Volumes ONTAP no AWS Secret Cloud ou no AWS Top Secret Cloud

Semelhante a uma região padrão da AWS, você pode usar o NetApp Console em"Nuvem secreta da AWS" e em"Nuvem ultrassecreta da AWS" para implantar o Cloud Volumes ONTAP, que fornece recursos de nível empresarial para seu armazenamento em nuvem. AWS Secret Cloud e Top Secret Cloud são regiões fechadas específicas para a Comunidade de Inteligência dos EUA; as instruções nesta página se aplicam somente aos usuários das regiões AWS Secret Cloud e Top Secret Cloud.

Antes de começar

Antes de começar, revise as versões compatíveis no AWS Secret Cloud e no Top Secret Cloud e saiba mais sobre o modo privado no Console.

- Revise as seguintes versões suportadas no AWS Secret Cloud e Top Secret Cloud:
  - Cloud Volumes ONTAP 9.12.1 P2

- Versão 3.9.32 do agente do Console

  O agente do Console é necessário para implantar e gerenciar o Cloud Volumes ONTAP na AWS. Você fará login no Console a partir do software instalado na instância do agente do Console. O site SaaS do Console não é compatível com o AWS Secret Cloud e o Top Secret Cloud.

- Saiba mais sobre o modo privado

  No AWS Secret Cloud e Top Secret Cloud, o Console opera no *modo privado*. No modo privado, não há conectividade com a camada SaaS do Console. Você pode acessar o Console por meio de um aplicativo local baseado na Web que pode acessar o agente do Console.

  Para saber mais sobre como funciona o modo privado, consulte"o modo de implantação privada no Console" .

Etapa 1: configure sua rede

Configure sua rede AWS para que o Cloud Volumes ONTAP possa operar corretamente.

Passos

1. Escolha a VPC e as sub-redes nas quais você deseja iniciar a instância do agente do Console e as instâncias do Cloud Volumes ONTAP .
2. Certifique-se de que sua VPC e sub-redes oferecerão suporte à conectividade entre o agente do Console e o Cloud Volumes ONTAP.
3. Configure um endpoint VPC para o serviço Amazon Simple Storage Service (Amazon S3).

   Um endpoint VPC é necessário se você quiser hierarquizar dados frios do Cloud Volumes ONTAP para armazenamento de objetos de baixo custo.

Etapa 2: Configurar permissões

Configure políticas e funções do IAM que forneçam ao agente do Console e ao Cloud Volumes ONTAP as permissões necessárias para executar ações no AWS Secret Cloud ou Top Secret Cloud.

Você precisa de uma política do IAM e uma função do IAM para cada um dos seguintes:

- A instância do agente do Console
- Instâncias Cloud Volumes ONTAP
- Para pares de HA, a instância do mediador de HA do Cloud Volumes ONTAP (se você quiser implantar pares de HA)

Passos

1. Acesse o console do AWS IAM e clique em **Políticas**.
2. Crie uma política para a instância do agente do Console.

   Crie essas políticas para dar suporte aos buckets do S3 no seu ambiente AWS. Ao criar os buckets posteriormente, certifique-se de que os nomes dos buckets sejam prefixados com `fabric-pool-` . Este requisito se aplica às regiões AWS Secret Cloud e Top Secret Cloud.

Regiões secretas

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
```

```
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso-b:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
```

```
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

Regiões ultrasecretas

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
```

```
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
    ]
```

```
}
```

3. Crie uma política para o Cloud Volumes ONTAP.

Regiões secretas

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso-b:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Regiões ultrasecretas

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Para pares de HA, se você planeja implantar um par de HA do Cloud Volumes ONTAP , crie uma política para o mediador de HA.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

4. Crie funções do IAM com o tipo de função Amazon EC2 e anexe as políticas que você criou nas etapas anteriores.

   Crie a função:

   Semelhante às políticas, você deve ter uma função do IAM para o agente do Console e uma para os nós do Cloud Volumes ONTAP . Para pares de HA: semelhante às políticas, você deve ter uma função do IAM para o agente do Console, uma para os nós do Cloud Volumes ONTAP e uma para o mediador de HA (se quiser implantar pares de HA).

   Selecione a função:

   Você deve selecionar a função IAM do agente do Console ao iniciar a instância do agente do Console. Você pode selecionar as funções do IAM para o Cloud Volumes ONTAP ao criar um sistema Cloud Volumes ONTAP no Console. Para pares de HA, você pode selecionar as funções do IAM para o Cloud Volumes ONTAP e o mediador de HA ao criar um sistema Cloud Volumes ONTAP .

Etapa 3: configurar o AWS KMS

Se você quiser usar a criptografia da Amazon com o Cloud Volumes ONTAP, certifique-se de que os requisitos sejam atendidos para o AWS Key Management Service (KMS).

Passos

1. Certifique-se de que exista uma Chave Mestra do Cliente (CMK) ativa na sua conta ou em outra conta da AWS.

   A CMK pode ser uma CMK gerenciada pela AWS ou uma CMK gerenciada pelo cliente.

2. Se a CMK estiver em uma conta da AWS separada da conta onde você planeja implantar o Cloud Volumes ONTAP, será necessário obter o ARN dessa chave.

   Você precisa fornecer o ARN ao Console ao criar o sistema Cloud Volumes ONTAP .

3. Adicione a função do IAM da instância à lista de usuários principais de uma CMK.

   Isso dá ao Console permissões para usar o CMK com o Cloud Volumes ONTAP.

Etapa 4: instalar o agente do Console e configurar o Console

Antes de começar a usar o Console para implantar o Cloud Volumes ONTAP na AWS, você deve instalar e configurar o agente do Console. Ele permite que o Console gerencie recursos e processos dentro do seu ambiente de nuvem pública (isso inclui o Cloud Volumes ONTAP).

Passos

1. Obtenha um certificado raiz assinado por uma autoridade de certificação (CA) no formato X.509 codificado em Privacy Enhanced Mail (PEM) Base-64. Consulte as políticas e procedimentos da sua organização para obter o certificado.

   > Para regiões do AWS Secret Cloud, você deve fazer upload do `NSS Root CA 2` certificado e para Top Secret Cloud, o `Amazon Root CA 4` certificado. Certifique-se de carregar apenas esses certificados e não a cadeia inteira. O arquivo da cadeia de certificados é grande e o upload pode falhar. Se você tiver certificados adicionais, poderá enviá-los mais tarde, conforme descrito na próxima etapa.

   Você precisa carregar o certificado durante o processo de configuração. O Console usa o certificado confiável ao enviar solicitações para a AWS via HTTPS.

2. Inicie a instância do agente do Console:
   a. Acesse a página do AWS Intelligence Community Marketplace para o Console.
   b. Na guia Inicialização personalizada, escolha a opção para iniciar a instância no console do EC2.
   c. Siga as instruções para configurar a instância.

      Observe o seguinte ao configurar a instância:

      - Recomendamos t3.xlarge.
      - Você deve escolher a função do IAM que criou ao configurar as permissões.
      - Você deve manter as opções de armazenamento padrão.
      - Os métodos de conexão necessários para o agente do Console são os seguintes: SSH, HTTP e HTTPS.
3. Configure o Console a partir de um host que tenha uma conexão com a instância:
   a. Abra um navegador da web e digite https://ipaddress onde ipaddress é o endereço IP do host Linux onde você instalou o agente do Console.
   b. Especifique um servidor proxy para conectividade com serviços da AWS.
   c. Carregue o certificado que você obteve na etapa 1.
   d. Siga as instruções para configurar um novo sistema.
      - **Detalhes do sistema**: insira um nome para o agente do Console e o nome da sua empresa.
      - **Criar usuário administrador**: Crie o usuário administrador do sistema.

        Esta conta de usuário é executada localmente no sistema. Não há conexão com o serviço auth0

disponível através do Console.

- **Revisar**: revise os detalhes, aceite o contrato de licença e selecione **Configurar**.

e. Para concluir a instalação do certificado assinado pela CA, reinicie a instância do agente do Console no console do EC2.

4. Após a reinicialização do agente do Console, efetue login usando a conta de usuário administrador que você criou no assistente de configuração.

Etapa 5: (opcional) Instalar um certificado de modo privado

Esta etapa é opcional para as regiões AWS Secret Cloud e Top Secret Cloud e é necessária somente se você tiver certificados adicionais além dos certificados raiz que instalou na etapa anterior.

Passos

1. Listar certificados instalados existentes.
   a. Para coletar o ID do docker do contêiner occm (nome identificado “ds-occm-1”), execute o seguinte comando:

```
docker ps
```

   b. Para entrar no contêiner occm, execute o seguinte comando:

```
docker exec -it <docker-id> /bin/sh
```

   c. Para coletar a senha da variável de ambiente “TRUST_STORE_PASSWORD”, execute o seguinte comando:

```
env
```

   d. Para listar todos os certificados instalados no truststore, execute o seguinte comando e use a senha coletada na etapa anterior:

```
keytool -list -v -keystore occm.truststore
```

2. Adicionar um certificado.
   a. Para coletar o ID do docker do contêiner occm (nome identificado “ds-occm-1”), execute o seguinte comando:

```
docker ps
```

   b. Para entrar no contêiner occm, execute o seguinte comando:

```
docker exec -it <docker-id> /bin/sh
```

Salve o novo arquivo de certificado dentro.

c. Para coletar a senha da variável de ambiente “TRUST_STORE_PASSWORD”, execute o seguinte comando:

```
env
```

d. Para adicionar o certificado ao truststore, execute o seguinte comando e use a senha da etapa anterior:

```
keytool -import -alias <alias-name> -file <certificate-file-name>
-keystore occm.truststore
```

e. Para verificar se o certificado foi instalado, execute o seguinte comando:

```
keytool -list -v -keystore occm.truststore -alias <alias-name>
```

f. Para sair do contêiner occm, execute o seguinte comando:

```
exit
```

g. Para redefinir o contêiner occm, execute o seguinte comando:

```
docker restart <docker-id>
```

Etapa 6: Adicionar uma licença ao Console

Se você comprou uma licença da NetApp, precisará adicioná-la ao Console para poder selecionar a licença ao criar um novo sistema Cloud Volumes ONTAP . Essas licenças permanecem não atribuídas até que você as associe a um novo sistema Cloud Volumes ONTAP .

Passos

1. No menu de navegação à esquerda, selecione * Licenses and subscriptions*.
2. No painel * Cloud Volumes ONTAP*, selecione **Exibir**.
3. Na guia * Cloud Volumes ONTAP*, selecione **Licenças > Licenças baseadas em nós**.
4. Clique em **Não atribuído**.
5. Clique em **Adicionar licenças não atribuídas**.
6. Digite o número de série da licença ou carregue o arquivo de licença.

7. Se você ainda não tiver o arquivo de licença, precisará carregá-lo manualmente em netapp.com.
   a. Vá para o"Gerador de arquivo de licença NetApp" e faça login usando suas credenciais do site de suporte da NetApp .
   b. Digite sua senha, escolha seu produto, insira o número de série, confirme que você leu e aceitou a política de privacidade e clique em **Enviar**.
   c. Escolha se deseja receber o arquivo JSON serialnumber.NLF por e-mail ou download direto.
8. Clique em **Adicionar licença**.

Resultado

O Console adiciona a licença como não atribuída até que você a associe a um novo sistema Cloud Volumes ONTAP . Você pode ver a licença no menu de navegação à esquerda em * Licenses and subscriptions > Cloud Volumes ONTAP > Exibir > Licenças*.

Etapa 7: Inicie o Cloud Volumes ONTAP no console

Você pode iniciar instâncias do Cloud Volumes ONTAP no AWS Secret Cloud e Top Secret Cloud criando novos sistemas no Console.

Antes de começar

Para pares HA, um par de chaves é necessário para habilitar a autenticação SSH baseada em chave para o mediador HA.

Passos

1. Na página **Sistemas**, clique em **Adicionar Sistema**.
2. Em **Criar**, selecione Cloud Volumes ONTAP.

   Para HA: em **Criar**, selecione Cloud Volumes ONTAP ou Cloud Volumes ONTAP HA.

3. Conclua as etapas do assistente para iniciar o sistema Cloud Volumes ONTAP .

> Ao fazer seleções por meio do assistente, não selecione **Data Sense & Compliance** e **Backup to Cloud** em **Serviços**. Em **Pacotes pré-configurados**, selecione apenas **Alterar configuração** e certifique-se de não ter selecionado nenhuma outra opção. Pacotes pré-configurados não são suportados nas regiões AWS Secret Cloud e Top Secret Cloud e, se selecionados, sua implantação falhará.

Observações para implantação do Cloud Volumes ONTAP HA em várias zonas de disponibilidade

Observe o seguinte ao concluir o assistente para pares HA.

- Você deve configurar um gateway de trânsito ao implantar o Cloud Volumes ONTAP HA em várias Zonas de Disponibilidade (AZs). Para obter instruções, consulte"Configurar um gateway de trânsito da AWS" .
- Implante a configuração da seguinte forma porque apenas duas AZs estavam disponíveis no AWS Top Secret Cloud no momento da publicação:
  - Nó 1: Zona de disponibilidade A
  - Nó 2: Zona de disponibilidade B
  - Mediador: Zona de disponibilidade A ou B

Observações para implantação do Cloud Volumes ONTAP em nós únicos e de alta disponibilidade

Observe o seguinte ao concluir o assistente:

- Você deve deixar a opção padrão para usar um grupo de segurança gerado.

  O grupo de segurança predefinido inclui as regras que o Cloud Volumes ONTAP precisa para operar com sucesso. Se você precisar usar o seu próprio, consulte a seção de grupo de segurança abaixo.

- Você deve escolher a função do IAM que criou ao preparar seu ambiente da AWS.
- O tipo de disco AWS subjacente é para o volume inicial do Cloud Volumes ONTAP .

  Você pode escolher um tipo de disco diferente para volumes subsequentes.

- O desempenho dos discos da AWS está vinculado ao tamanho do disco.

  Você deve escolher o tamanho do disco que lhe dará o desempenho sustentado que você precisa. Consulte a documentação da AWS para obter mais detalhes sobre o desempenho do EBS.

- O tamanho do disco é o tamanho padrão para todos os discos no sistema.

  Se precisar de um tamanho diferente posteriormente, você pode usar a opção Alocação avançada para criar um agregado que use discos de um tamanho específico.

Resultado

A instância do Cloud Volumes ONTAP é iniciada. Você pode acompanhar o progresso na página **Auditoria**.

Etapa 8: instalar certificados de segurança para camadas de dados

Você precisa instalar manualmente os certificados de segurança para habilitar a hierarquização de dados nas regiões AWS Secret Cloud e Top Secret Cloud.

Antes de começar

1. Crie buckets S3.

   Certifique-se de que os nomes dos buckets sejam prefixados com `fabric-pool-`. Por exemplo `fabric-pool-testbucket` .

2. Mantenha os certificados raiz que você instalou em `step 4` útil.

Passos

1. Copie o texto dos certificados raiz que você instalou em `step 4` .
2. Conecte-se com segurança ao sistema Cloud Volumes ONTAP usando a CLI.
3. Instale os certificados raiz. Pode ser necessário pressionar o `ENTER` tecla várias vezes:

   ```
   security certificate install -type server-ca -cert-name <certificate-
   name>
   ```

4. Quando solicitado, insira todo o texto copiado, incluindo e de `----- BEGIN CERTIFICATE -----` para `----- END CERTIFICATE -----` .

5. Guarde uma cópia do certificado digital assinado pela CA para referência futura.
6. Guarde o nome da CA e o número de série do certificado.
7. Configure o armazenamento de objetos para as regiões AWS Secret Cloud e Top Secret Cloud: `set -privilege advanced -confirmations off`
8. Execute este comando para configurar o armazenamento de objetos.

> Todos os nomes de recursos da Amazon (ARNs) devem ser sufixados com `-iso-b` , como `arn:aws-iso-b` . Por exemplo, se um recurso requer um ARN com uma região, para Top Secret Cloud, use a convenção de nomenclatura como `us-iso-b` para o `-server` bandeira. Para AWS Secret Cloud, use `us-iso-b-1` .

```
storage aggregate object-store config create -object-store-name
<S3Bucket> -provider-type AWS_S3 -auth-type EC2-IAM -server <s3.us-iso-
b-1.server_name> -container-name <fabric-pool-testbucket> -is-ssl
-enabled true -port 443
```

9. Verifique se o armazenamento de objetos foi criado com sucesso: `storage aggregate object-store show -instance`
10. Anexe o armazenamento de objetos ao agregado. Isso deve ser repetido para cada novo agregado: `storage aggregate object-store attach -aggregate <aggr1> -object-store-name <S3Bucket>`

Comece no Microsoft Azure

Saiba mais sobre as opções de implantação do Cloud Volumes ONTAP no Azure

A NetApp oferece duas opções para implantar o Cloud Volumes ONTAP no Azure. O Cloud Volumes ONTAP tradicionalmente depende do NetApp Console para implantação e orquestração. A partir do Cloud Volumes ONTAP 9.16.1, você pode aproveitar a implantação direta do Azure Marketplace, um processo simplificado que fornece acesso a um conjunto limitado, mas ainda poderoso, de recursos e opções do Cloud Volumes ONTAP .

Ao implantar o Cloud Volumes ONTAP diretamente do marketplace do Azure, você não precisa configurar o agente do Console nem atender a outros critérios de segurança e integração necessários para implantar o Cloud Volumes ONTAP por meio do Console. No marketplace do Azure, você pode implantar rapidamente o Cloud Volumes ONTAP em apenas alguns cliques e explorar seus principais recursos e funcionalidades em seu ambiente.

Ao concluir a implantação no marketplace do Azure, você pode descobrir esses sistemas no Console. Após a descoberta, você pode gerenciá-los como sistemas Cloud Volumes ONTAP e aproveitar todos os recursos do Console. Consulte "Descubra os sistemas implantados no Console" .

Aqui está a comparação de recursos entre as duas opções. Observe que os recursos de uma instância autônoma implantada por meio do marketplace do Azure mudam quando ela é descoberta no Console.

	Mercado do Azure	NetApp Console
Integração	Mais curto e fácil, com preparação mínima necessária para implantação direta	Processo de integração mais longo, incluindo a instalação do agente do Console
Tipos de máquinas virtuais (VM) suportados	Tipos de instância Eds_v5 e Ls_v3	Gama completa de tipos de VM.https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-azure.html["Configurações com suporte no Azure"^]
Licença	Licença gratuita	Qualquer licença baseada em capacidade."Licenciamento do Cloud Volumes ONTAP"
* Suporte NetApp *	Não incluído	Disponível, com base no tipo de licença
Capacidade	Até 500 GiB	Expansível por configuração
Modelo de implantação	Implantação do modo de alta disponibilidade (HA) em zona de disponibilidade única (AZ)	Todas as configurações suportadas, incluindo modos de nó único e HA, implantações de AZ únicas e múltiplas
Tipo de disco suportado	Discos gerenciados SSD v2 premium	Suporte mais amplo."Configuração padrão para Cloud Volumes ONTAP"
Velocidade de gravação (modo de gravação rápida)	Não suportado	Suportado, com base na sua configuração. "Saiba mais sobre velocidades de gravação no Cloud Volumes ONTAP" .
Capacidade de orquestração	Não disponível	Disponível por meio do NetApp Console, com base no tipo de licença
Número de VMs de armazenamento suportadas	Um por implantação	Várias VMs de armazenamento, com base na sua configuração."Número suportado de VMs de armazenamento"
Alterando o tipo de instância	Não suportado	Suportado
* Hierarquização do FabricPool *	Não suportado	Suportado

Links relacionados

- Implantação direta do Azure Marketplace:"Implantar o Cloud Volumes ONTAP no marketplace do Azure"
- Implantação por meio do Console:"Início rápido para Cloud Volumes ONTAP no Azure"
- "Documentação do NetApp Console"

Introdução ao NetApp Console

Início rápido para Cloud Volumes ONTAP no Azure

Comece a usar o Cloud Volumes ONTAP para Azure em poucas etapas.

1 Criar um agente de console

Se você não tem um "Agente de console" no entanto, você precisa criar um. "Aprenda a criar um agente de console no Azure"

Observe que se você quiser implantar o Cloud Volumes ONTAP em uma sub-rede onde não há acesso à Internet disponível, será necessário instalar manualmente o agente do Console e acessar o NetApp Console que está em execução nesse agente do Console. "Aprenda a instalar manualmente o agente do Console em um local sem acesso à Internet"

2 Planeje sua configuração

O Console oferece pacotes pré-configurados que correspondem aos seus requisitos de carga de trabalho, ou você pode criar sua própria configuração. Se você escolher sua própria configuração, deverá entender as opções disponíveis. Para obter informações, consulte"Planeje sua configuração do Cloud Volumes ONTAP no Azure" .

3 Configure sua rede

1. Certifique-se de que sua VNet e sub-redes oferecerão suporte à conectividade entre o agente do Console e o Cloud Volumes ONTAP.
2. Habilite o acesso de saída à Internet da VPC de destino para o NetApp AutoSupport.

   Esta etapa não é necessária se você estiver implantando o Cloud Volumes ONTAP em um local onde não há acesso à Internet disponível.

"Saiba mais sobre os requisitos de rede" .

4 Inicie o Cloud Volumes ONTAP

Clique em **Adicionar Sistema**, selecione o tipo de sistema que você gostaria de implantar e conclua as etapas do assistente. "Leia as instruções passo a passo" .

Links relacionados

- "Criando um agente de console a partir do console"
- "Criando um agente de console no Azure Marketplace"
- "Instalando o software do agente do Console em um host Linux"
- "O que o Console faz com as permissões"

Planeje sua configuração do Cloud Volumes ONTAP no Azure

Ao implantar o Cloud Volumes ONTAP no Azure, você pode escolher um sistema pré-configurado que corresponda aos seus requisitos de carga de trabalho ou pode criar sua própria configuração. Se você escolher sua própria configuração, deverá entender as

opções disponíveis.

Escolha uma licença do Cloud Volumes ONTAP

Várias opções de licenciamento estão disponíveis para o Cloud Volumes ONTAP. Cada opção permite que você escolha um modelo de consumo que atenda às suas necessidades.

- "Saiba mais sobre as opções de licenciamento do Cloud Volumes ONTAP"
- "Aprenda como configurar o licenciamento"

Escolha uma região com suporte

O Cloud Volumes ONTAP é compatível com a maioria das regiões do Microsoft Azure. "Veja a lista completa de regiões suportadas" .

Escolha um tipo de VM compatível

O Cloud Volumes ONTAP oferece suporte a vários tipos de VM, dependendo do tipo de licença escolhido.

"Configurações com suporte para Cloud Volumes ONTAP no Azure"

Entenda os limites de armazenamento

O limite de capacidade bruta para um sistema Cloud Volumes ONTAP está vinculado à licença. Limites adicionais afetam o tamanho dos agregados e volumes. Você deve estar ciente desses limites ao planejar sua configuração.

"Limites de armazenamento para Cloud Volumes ONTAP no Azure"

Dimensione seu sistema no Azure

Dimensionar seu sistema Cloud Volumes ONTAP pode ajudar você a atender aos requisitos de desempenho e capacidade. Você deve estar ciente de alguns pontos importantes ao escolher um tipo de VM, tipo de disco e tamanho de disco:

Tipo de máquina virtual

Veja os tipos de máquinas virtuais suportados no "Notas de versão do Cloud Volumes ONTAP" e, em seguida, revise os detalhes sobre cada tipo de VM com suporte. Esteja ciente de que cada tipo de VM suporta um número específico de discos de dados.

- "Documentação do Azure: Tamanhos de máquinas virtuais de uso geral"
- "Documentação do Azure: tamanhos de máquinas virtuais otimizados para memória"

Tipo de disco do Azure com sistemas de nó único

Ao criar volumes para o Cloud Volumes ONTAP, você precisa escolher o armazenamento em nuvem subjacente que o Cloud Volumes ONTAP usa como disco.

Sistemas de nó único podem usar estes tipos de Azure Managed Disks:

- *Discos SSD gerenciados premium* oferecem alto desempenho para cargas de trabalho com uso intensivo de E/S a um custo mais alto.
- *Discos gerenciados SSD v2 Premium* oferecem maior desempenho com menor latência e menor custo, em comparação aos discos gerenciados SSD Premium.

- *Discos gerenciados SSD padrão* fornecem desempenho consistente para cargas de trabalho que exigem IOPS baixo.
- *Discos gerenciados de HDD padrão* são uma boa escolha se você não precisa de IOPS alto e quer reduzir seus custos.

Para obter detalhes adicionais sobre os casos de uso desses discos, consulte "Documentação do Microsoft Azure: Quais tipos de disco estão disponíveis no Azure?" .

Tipo de disco do Azure com pares de alta disponibilidade

Os sistemas HA usam discos gerenciados compartilhados SSD Premium, que fornecem alto desempenho para cargas de trabalho com uso intensivo de E/S a um custo mais alto. Implantações de HA criadas antes do lançamento 9.12.1 usam blobs de páginas Premium.

Tamanho do disco do Azure

Ao iniciar instâncias do Cloud Volumes ONTAP , você deve escolher o tamanho de disco padrão para agregados. O NetApp Console usa esse tamanho de disco para o agregado inicial e para quaisquer agregados adicionais que ele cria quando você usa a opção de provisionamento simples. Você pode criar agregados que usam um tamanho de disco diferente do padrão por"usando a opção de alocação avançada" .

Todos os discos em um agregado devem ter o mesmo tamanho.

Ao escolher o tamanho do disco, você deve levar vários fatores em consideração. O tamanho do disco afeta o quanto você paga pelo armazenamento, o tamanho dos volumes que você pode criar em um agregado, a capacidade total disponível para o Cloud Volumes ONTAP e o desempenho do armazenamento.

O desempenho do Armazenamento Premium do Azure está vinculado ao tamanho do disco. Discos maiores oferecem maior IOPS e taxa de transferência. Por exemplo, escolher discos de 1 TiB pode fornecer melhor desempenho do que discos de 500 GiB, a um custo mais alto.

Não há diferenças de desempenho entre os tamanhos de disco para armazenamento padrão. Você deve escolher o tamanho do disco com base na capacidade necessária.

Consulte o Azure para IOPS e taxa de transferência por tamanho de disco:

- "Microsoft Azure: preços de discos gerenciados"
- "Microsoft Azure: preços de Page Blobs"

Exibir discos de sistema padrão

Além do armazenamento para dados do usuário, o Console também adquire armazenamento em nuvem para dados do sistema Cloud Volumes ONTAP (dados de inicialização, dados raiz, dados principais e NVRAM). Para fins de planejamento, pode ser útil revisar esses detalhes antes de implantar o Cloud Volumes ONTAP.

"Exibir os discos padrão para dados do sistema Cloud Volumes ONTAP no Azure" .

O agente do Console também requer um disco do sistema. "Exibir detalhes sobre a configuração padrão do agente do Console" .

Coletar informações de rede

Ao implantar o Cloud Volumes ONTAP no Azure, você precisa especificar detalhes sobre sua rede virtual. Você pode usar uma planilha para coletar informações do seu administrador.

Informações do Azure	Seu valor
Região	
Rede virtual (VNet)	
Sub-rede	
Grupo de segurança de rede (se estiver usando o seu próprio)	

Escolha uma velocidade de gravação

O Console permite que você escolha uma configuração de velocidade de gravação para o Cloud Volumes ONTAP. Antes de escolher uma velocidade de gravação, você deve entender as diferenças entre as configurações normal e alta, bem como os riscos e recomendações ao usar alta velocidade de gravação. "Saiba mais sobre velocidade de gravação" .

Escolha um perfil de uso de volume

O ONTAP inclui vários recursos de eficiência de armazenamento que podem reduzir a quantidade total de armazenamento necessária. Ao criar um volume no Console, você pode escolher um perfil que habilite esses recursos ou um perfil que os desabilite. Você deve aprender mais sobre esses recursos para ajudar a decidir qual perfil usar.

Os recursos de eficiência de armazenamento da NetApp oferecem os seguintes benefícios:

Provisionamento fino

Apresenta mais armazenamento lógico para hosts ou usuários do que você realmente tem em seu pool de armazenamento físico. Em vez de pré-alocar espaço de armazenamento, o espaço de armazenamento é alocado dinamicamente para cada volume à medida que os dados são gravados.

Desduplicação

Melhora a eficiência localizando blocos idênticos de dados e substituindo-os por referências a um único bloco compartilhado. Essa técnica reduz os requisitos de capacidade de armazenamento eliminando blocos redundantes de dados que residem no mesmo volume.

Compressão

Reduz a capacidade física necessária para armazenar dados compactando dados dentro de um volume no armazenamento primário, secundário e de arquivo.

Configurar a rede do Azure para o Cloud Volumes ONTAP

O NetApp Console gerencia a configuração de componentes de rede para o Cloud Volumes ONTAP, como endereços IP, máscaras de rede e rotas. Você precisa ter certeza de que o acesso de saída à Internet esteja disponível, que endereços IP privados suficientes estejam disponíveis, que as conexões corretas estejam em vigor e muito mais.

Requisitos para o Cloud Volumes ONTAP

Os seguintes requisitos de rede devem ser atendidos no Azure.

Acesso de saída à Internet

Os sistemas Cloud Volumes ONTAP exigem acesso de saída à Internet para acessar endpoints externos para diversas funções. O Cloud Volumes ONTAP não poderá operar corretamente se esses endpoints estiverem bloqueados em ambientes com requisitos de segurança rigorosos.

O agente do Console também entra em contato com vários endpoints para operações diárias. Para obter informações sobre pontos de extremidade, consulte "Exibir endpoints contatados pelo agente do Console" e "Preparar a rede para usar o Console" .

Pontos de extremidade Cloud Volumes ONTAP

O Cloud Volumes ONTAP usa esses endpoints para se comunicar com vários serviços.

Pontos finais	Aplicável para	Propósito	Modos de implantação	Impacto se indisponível
\ https://netapp-cloud-account.auth0.com	Autenticação	Usado para autenticação no Console.	Modos padrão e restrito.	A autenticação do usuário falha e os seguintes serviços permanecem indisponíveis: • Serviços Cloud Volumes ONTAP • Serviços ONTAP • Protocolos e serviços de proxy
https://vault.azure.net	Cofre de Chaves	Usado para recuperar chaves secretas do cliente do Azure Key Vault ao usar chaves gerenciadas pelo cliente (CMK).	Modos padrão, restrito e privado.	Os serviços do Cloud Volumes ONTAP não estão disponíveis.
\ https://api.bluexp.netapp.com/tenancy	Arrendamento	Usado para recuperar os recursos Cloud Volumes ONTAP do Console para autorizar recursos e usuários.	Modos padrão e restrito.	Os recursos do Cloud Volumes ONTAP e os usuários não estão autorizados.

Pontos finais	Aplicável para	Propósito	Modos de implantação	Impacto se indisponível
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Usado para enviar dados de telemetria do AutoSupport para o suporte da NetApp .	Modos padrão e restrito.	As informações do AutoSupport continuam não entregues.
\ https://management.azure.com \ https://login.microsoftonline.com \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://core.windows.net	Regiões públicas	Comunicação com serviços do Azure.	Modos padrão, restrito e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço do Azure para executar operações específicas para o Console no Azure.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Região da China	Comunicação com serviços do Azure.	Modos padrão, restrito e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço do Azure para executar operações específicas para o Console no Azure.
\ https://management.microsoftazure.de \ https://login.microsoftonline.de \ https://blob.core.cloudapi.de \ https://core.cloudapi.de	Região da Alemanha	Comunicação com serviços do Azure.	Modos padrão, restrito e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço do Azure para executar operações específicas para o Console no Azure.
\ https://management.usgovcloudapi.net \ https://login.microsoftonline.us \ https://blob.core.usgovcloudapi.net \ https://core.usgovcloudapi.net	Regiões governamentais	Comunicação com serviços do Azure.	Modos padrão, restrito e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço do Azure para executar operações específicas para o Console no Azure.

Pontos finais	Aplicável para	Propósito	Modos de implantação	Impacto se indisponível
\ https://management.azure.microsoft.scloud \ https://login.microsoftonline.microsoft.scloud \ https://blob.core.microsoft.scloud \ https://core.microsoft.scloud	Regiões do DoD do governo	Comunicação com serviços do Azure.	Modos padrão, restrito e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço do Azure para executar operações específicas para o Console no Azure.

Configuração de proxy de rede do agente do NetApp Console

Você pode usar a configuração de servidores proxy do agente do NetApp Console para habilitar o acesso de saída à Internet do Cloud Volumes ONTAP. O Console suporta dois tipos de proxies:

- **Proxy explícito**: O tráfego de saída do Cloud Volumes ONTAP usa o endereço HTTP do servidor proxy especificado durante a configuração de proxy do agente do Console. O administrador também pode ter configurado credenciais de usuário e certificados de CA raiz para autenticação adicional. Se um certificado de CA raiz estiver disponível para o proxy explícito, certifique-se de obter e carregar o mesmo certificado para o seu sistema Cloud Volumes ONTAP usando o "ONTAP CLI: instalação do certificado de segurança" comando.
- **Proxy transparente**: A rede está configurada para rotear automaticamente o tráfego de saída do Cloud Volumes ONTAP por meio do proxy para o agente do Console. Ao configurar um proxy transparente, o administrador precisa fornecer apenas um certificado de CA raiz para conectividade do Cloud Volumes ONTAP, não o endereço HTTP do servidor proxy. Certifique-se de obter e carregar o mesmo certificado de CA raiz para o seu sistema Cloud Volumes ONTAP usando o "ONTAP CLI: instalação do certificado de segurança" comando.

Para obter informações sobre como configurar servidores proxy, consulte o "Configurar o agente do Console para usar um servidor proxy" .

Endereços IP

O Console aloca automaticamente o número necessário de endereços IP privados para o Cloud Volumes ONTAP no Azure. Você precisa ter certeza de que sua rede tem endereços IP privados suficientes disponíveis.

O número de LIFs alocados para Cloud Volumes ONTAP depende se você implanta um sistema de nó único ou um par de HA. Uma LIF é um endereço IP associado a uma porta física. Uma LIF de gerenciamento de SVM é necessária para ferramentas de gerenciamento como SnapCenter.

> Um iSCSI LIF fornece acesso de cliente pelo protocolo iSCSI e é usado pelo sistema para outros fluxos de trabalho de rede importantes. Esses LIFs são necessários e não devem ser excluídos.

Endereços IP para um sistema de nó único

O Console aloca 5 ou 6 endereços IP para um sistema de nó único:

- IP de gerenciamento de cluster
- IP de gerenciamento de nó
- IP intercluster para SnapMirror
- IP NFS/CIFS
- IP iSCSI

> O IP iSCSI fornece acesso do cliente através do protocolo iSCSI. Ele também é usado pelo sistema para outros fluxos de trabalho de rede importantes. Este LIF é necessário e não deve ser excluído.

- Gerenciamento de SVM (opcional - não configurado por padrão)

Endereços IP para pares HA

O Console aloca endereços IP para 4 NICs (por nó) durante a implantação.

Observe que o Console cria uma LIF de gerenciamento de SVM em pares de HA, mas não em sistemas de nó único no Azure.

NIC0

- IP de gerenciamento de nó
- IP intercluster
- IP iSCSI

> O IP iSCSI fornece acesso do cliente através do protocolo iSCSI. Ele também é usado pelo sistema para outros fluxos de trabalho de rede importantes. Este LIF é necessário e não deve ser excluído.

NIC1

- IP de rede de cluster

NIC2

- IP de interconexão de cluster (HA IC)

NIC3

- IP da placa de rede Pageblob (acesso ao disco)

> O NIC3 só é aplicável a implantações de HA que usam armazenamento de blobs de páginas.

Os endereços IP acima não migram em eventos de failover.

Além disso, 4 IPs de front-end (FIPs) são configurados para migrar em eventos de failover. Esses IPs de front-end residem no balanceador de carga.

- IP de gerenciamento de cluster
- IP de dados do NodeA (NFS/CIFS)

- IP de dados do NodeB (NFS/CIFS)
- IP de gerenciamento SVM

Conexões seguras com serviços do Azure

Por padrão, o Console habilita um Link Privado do Azure para conexões entre o Cloud Volumes ONTAP e contas de armazenamento de blobs de páginas do Azure.

Na maioria dos casos, não há nada que você precise fazer: o Console gerencia o Azure Private Link para você. Mas se você usar o DNS Privado do Azure, precisará editar um arquivo de configuração. Você também deve estar ciente de um requisito para a localização do agente do Console no Azure.

Você também pode desabilitar a conexão Private Link, se necessário, de acordo com as necessidades do seu negócio. Se você desabilitar o link, o Console configurará o Cloud Volumes ONTAP para usar um ponto de extremidade de serviço.

"Saiba mais sobre como usar o Azure Private Links ou pontos de extremidade de serviço com o Cloud Volumes ONTAP" .

Rede para criptografia do Azure VNet

Cloud Volumes ONTAP oferece suporte "Criptografia da Azure Virtual Network (VNet)"à criptografia do tráfego entre máquinas virtuais (VMs) dentro de uma VNet ou entre VNets emparelhadas. Esse recurso é configurado na camada VNet do Azure e é independente da topologia do Cloud Volumes ONTAP (nó único ou HA).

Você só precisa garantir que a Rede Acelerada esteja habilitada nas NICs da VM e revisar os requisitos e limitações de criptografia da VNet do Azure antes de habilitar o recurso. Você não deve modificar os objetos do balanceador de carga gerenciado pela NetApp.

"Documentação do Azure: criptografia VNet e Accelerated Networking".

Conexões com outros sistemas ONTAP

Para replicar dados entre um sistema Cloud Volumes ONTAP no Azure e sistemas ONTAP em outras redes, você deve ter uma conexão VPN entre a VNet do Azure e a outra rede, por exemplo, sua rede corporativa.

Para obter instruções, consulte o "Documentação do Microsoft Azure: Criar uma conexão site a site no portal do Azure" .

Porta para a interconexão HA

Um par de HA do Cloud Volumes ONTAP inclui uma interconexão de HA, que permite que cada nó verifique continuamente se seu parceiro está funcionando e espelhe dados de log para a memória não volátil do outro. A interconexão HA usa a porta TCP 10006 para comunicação.

Por padrão, a comunicação entre os LIFs de interconexão HA é aberta e não há regras de grupo de segurança para esta porta. Mas se você criar um firewall entre os LIFs de interconexão HA, precisará garantir que o tráfego TCP esteja aberto para a porta 10006 para que o par HA possa operar corretamente.

Apenas um par de HA em um grupo de recursos do Azure

Você deve usar um grupo de recursos *dedicado* para cada par de Cloud Volumes ONTAP HA implantado no Azure. Somente um par de HA é suportado em um grupo de recursos.

O Console terá problemas de conexão se você tentar implantar um segundo par de Cloud Volumes ONTAP HA em um grupo de recursos do Azure.

Regras do grupo de segurança

O Console cria grupos de segurança do Azure que incluem as regras de entrada e saída para que o Cloud Volumes ONTAP opere com sucesso. "Exibir regras de grupo de segurança para o agente do Console" .

Os grupos de segurança do Azure para o Cloud Volumes ONTAP exigem que as portas apropriadas estejam abertas para comunicação interna entre os nós. "Saiba mais sobre as portas internas do ONTAP" .

Não recomendamos modificar os grupos de segurança predefinidos ou usar grupos de segurança personalizados. No entanto, se necessário, observe que o processo de implantação exige que o sistema Cloud Volumes ONTAP tenha acesso total dentro de sua própria sub-rede. Após a conclusão da implantação, se você decidir modificar o grupo de segurança de rede, certifique-se de manter as portas do cluster e as portas de rede HA abertas. Isso garante uma comunicação perfeita dentro do cluster Cloud Volumes ONTAP (comunicação de qualquer para qualquer entre os nós).

Regras de entrada para sistemas de nó único

Ao adicionar um sistema Cloud Volumes ONTAP e escolher um grupo de segurança predefinido, você pode optar por permitir o tráfego dentro de um dos seguintes:

- **Somente VNet selecionada**: A origem do tráfego de entrada é o intervalo de sub-redes da VNet para o sistema Cloud Volumes ONTAP e o intervalo de sub-redes da VNet onde o agente do Console reside. Esta é a opção recomendada.
- **Todas as VNets**: A origem do tráfego de entrada é o intervalo de IP 0.0.0.0/0.
- **Desativado**: esta opção restringe o acesso da rede pública à sua conta de armazenamento e desabilita a hierarquização de dados para sistemas Cloud Volumes ONTAP . Esta é uma opção recomendada se seus endereços IP privados não devem ser expostos, mesmo dentro da mesma VNet, devido a regulamentações e políticas de segurança.

Prioridade e nome	Porta e protocolo	Origem e destino	Descrição
1000 entrada_ssh	22 TCP	Qualquer para Qualquer	Acesso SSH ao endereço IP do LIF de gerenciamento de cluster ou de um LIF de gerenciamento de nó
1001 entrada_http	80 TCP	Qualquer para Qualquer	Acesso HTTP ao console da web do ONTAP System Manager usando o endereço IP do LIF de gerenciamento do cluster
1002 entrada_111_tcp	111 TCP	Qualquer para Qualquer	Chamada de procedimento remoto para NFS
1003 entrada_111_udp	111 UDP	Qualquer para Qualquer	Chamada de procedimento remoto para NFS

Prioridade e nome	Porta e protocolo	Origem e destino	Descrição
1004 entrada_139	139 TCP	Qualquer para Qualquer	Sessão de serviço NetBIOS para CIFS
1005 entrada_161-162 _tcp	161-162 TCP	Qualquer para Qualquer	Protocolo simples de gerenciamento de rede
1006 entrada_161-162 _udp	161-162 UDP	Qualquer para Qualquer	Protocolo simples de gerenciamento de rede
1007 entrada_443	443 TCP	Qualquer para Qualquer	Conectividade com o agente do Console e acesso HTTPS ao console da Web do ONTAP System Manager usando o endereço IP do LIF de gerenciamento do cluster
1008 entrada_445	445 TCP	Qualquer para Qualquer	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
1009 entrada_635_tcp	635 TCP	Qualquer para Qualquer	Montagem NFS
1010 entrada_635_udp	635 UDP	Qualquer para Qualquer	Montagem NFS
1011 entrada_749	749 TCP	Qualquer para Qualquer	Kerberos
1012 entrada_2049_tcp	2049 TCP	Qualquer para Qualquer	Daemon do servidor NFS
1013 entrada_2049_udp	2049 UDP	Qualquer para Qualquer	Daemon do servidor NFS
1014 entrada_3260	3260 TCP	Qualquer para Qualquer	Acesso iSCSI através do LIF de dados iSCSI
1015 entrada_4045-4046_tcp	4045-4046 TCP	Qualquer para Qualquer	Daemon de bloqueio NFS e monitor de status de rede
1016 entrada_4045-4046_udp	4045-4046 UDP	Qualquer para Qualquer	Daemon de bloqueio NFS e monitor de status de rede
1017 entrada_10000	10000 TCP	Qualquer para Qualquer	Backup usando NDMP
1018 entrada_11104-11105	11104-11105 TCP	Qualquer para Qualquer	Transferência de dados do SnapMirror
3000 negação de entrada _todos_tcp	Qualquer porta TCP	Qualquer para Qualquer	Bloquear todo o outro tráfego de entrada TCP
3001 negação de entrada _todos_udp	Qualquer porta UDP	Qualquer para Qualquer	Bloquear todo o outro tráfego de entrada UDP
65000 Permitir entrada de Vnet	Qualquer porta Qualquer protocolo	Rede Virtual para Rede Virtual	Tráfego de entrada de dentro da VNet
65001 Permitir entrada do balanceador de carga do Azure	Qualquer porta Qualquer protocolo	AzureLoadBalancer para qualquer	Tráfego de dados do Azure Standard Load Balancer

Prioridade e nome	Porta e protocolo	Origem e destino	Descrição
65500 NegarAllInBound	Qualquer porta Qualquer protocolo	Qualquer para Qualquer	Bloqueie todo o outro tráfego de entrada

Regras de entrada para sistemas HA

Ao adicionar um sistema Cloud Volumes ONTAP e escolher um grupo de segurança predefinido, você pode optar por permitir o tráfego dentro de um dos seguintes:

- **Somente VNet selecionada**: A origem do tráfego de entrada é o intervalo de sub-redes da VNet para o sistema Cloud Volumes ONTAP e o intervalo de sub-redes da VNet onde o agente do Console reside. Esta é a opção recomendada.
- **Todas as VNets**: A origem do tráfego de entrada é o intervalo de IP 0.0.0.0/0.

Os sistemas de alta disponibilidade (par de HA) têm menos regras de entrada do que os sistemas de nó único porque o tráfego de dados de entrada passa pelo Azure Standard Load Balancer. Por causa disso, o tráfego do Load Balancer deve ser aberto, conforme mostrado na regra "AllowAzureLoadBalancerInBound".

- **Desativado**: esta opção restringe o acesso da rede pública à sua conta de armazenamento e desabilita a hierarquização de dados para sistemas Cloud Volumes ONTAP . Esta é uma opção recomendada se seus endereços IP privados não devem ser expostos, mesmo dentro da mesma VNet, devido a regulamentações e políticas de segurança.

Prioridade e nome	Porta e protocolo	Origem e destino	Descrição
100 entrada_443	443 Qualquer protocolo	Qualquer para Qualquer	Conectividade com o agente do Console e acesso HTTPS ao console da Web do ONTAP System Manager usando o endereço IP do LIF de gerenciamento do cluster
101 entrada_111_tcp	111 Qualquer protocolo	Qualquer para Qualquer	Chamada de procedimento remoto para NFS
102 entrada_2049_tcp	2049 Qualquer protocolo	Qualquer para Qualquer	Daemon do servidor NFS
111 entrada_ssh	22 Qualquer protocolo	Qualquer para Qualquer	Acesso SSH ao endereço IP do LIF de gerenciamento de cluster ou de um LIF de gerenciamento de nó
121 entrada_53	53 Qualquer protocolo	Qualquer para Qualquer	DNS e CIFS
65000 Permitir entrada de Vnet	Qualquer porta Qualquer protocolo	Rede Virtual para Rede Virtual	Tráfego de entrada de dentro da VNet
65001 Permitir entrada do balanceador de carga do Azure	Qualquer porta Qualquer protocolo	AzureLoadBalancer para qualquer	Tráfego de dados do Azure Standard Load Balancer

Prioridade e nome	Porta e protocolo	Origem e destino	Descrição
65500 NegarAllInBound	Qualquer porta Qualquer protocolo	Qualquer para Qualquer	Bloqueie todo o outro tráfego de entrada

Regras de saída

O grupo de segurança predefinido para o Cloud Volumes ONTAP abre todo o tráfego de saída. Se isso for aceitável, siga as regras básicas de saída. Se precisar de regras mais rígidas, use as regras de saída avançadas.

Regras básicas de saída

O grupo de segurança predefinido para o Cloud Volumes ONTAP inclui as seguintes regras de saída.

Porta	Protocolo	Propósito
Todos	Todos os TCP	Todo o tráfego de saída
Todos	Todos os UDP	Todo o tráfego de saída

Regras avançadas de saída

Se precisar de regras rígidas para o tráfego de saída, você pode usar as seguintes informações para abrir apenas as portas necessárias para a comunicação de saída pelo Cloud Volumes ONTAP.

A origem é a interface (endereço IP) no sistema Cloud Volumes ONTAP .

Serviço	Porta	Protocolo	Fonte	Destino	Propósito
Diretório ativo	88	TCP	Gerenciamento de nós LIF	Floresta do Active Directory	Autenticação Kerberos V
	137	UDP	Gerenciamento de nós LIF	Floresta do Active Directory	Serviço de nomes NetBIOS
	138	UDP	Gerenciamento de nós LIF	Floresta do Active Directory	Serviço de datagrama NetBIOS
	139	TCP	Gerenciamento de nós LIF	Floresta do Active Directory	Sessão de serviço NetBIOS
	389	TCP e UDP	Gerenciamento de nós LIF	Floresta do Active Directory	LDAP
	445	TCP	Gerenciamento de nós LIF	Floresta do Active Directory	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
	464	TCP	Gerenciamento de nós LIF	Floresta do Active Directory	Alteração e definição de senha do Kerberos V (SET_CHANGE)
	464	UDP	Gerenciamento de nós LIF	Floresta do Active Directory	Administração de chaves Kerberos
	749	TCP	Gerenciamento de nós LIF	Floresta do Active Directory	Kerberos V alterar e definir senha (RPCSEC_GSS)
	88	TCP	Dados LIF (NFS, CIFS, iSCSI)	Floresta do Active Directory	Autenticação Kerberos V
	137	UDP	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Serviço de nomes NetBIOS
	138	UDP	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Serviço de datagrama NetBIOS
	139	TCP	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Sessão de serviço NetBIOS
	389	TCP e UDP	Dados LIF (NFS, CIFS)	Floresta do Active Directory	LDAP
	445	TCP	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
	464	TCP	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Alteração e definição de senha do Kerberos V (SET_CHANGE)
	464	UDP	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Administração de chaves Kerberos
	749	TCP	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Alterar e definir senha do Kerberos V (RPCSEC_GSS)

Serviço	Porta	Protocolo	Fonte	Destino	Propósito
AutoSupport	HTTPS	443	Gerenciamento de nós LIF	meusuporte.netapp.com	AutoSupport (HTTPS é o padrão)
	HTTP	80	Gerenciamento de nós LIF	meusuporte.netapp.com	AutoSupport (somente se o protocolo de transporte for alterado de HTTPS para HTTP)
	TCP	3128	Gerenciamento de nós LIF	Agente de console	Envio de mensagens do AutoSupport por meio de um servidor proxy no agente do Console, se uma conexão de saída com a Internet não estiver disponível
Backups de configuração	HTTP	80	Gerenciamento de nós LIF	http://<endereço-IP-do-agente-do-console>/occm/offboxconfig	Envie backups de configuração para o agente do Console. "Documentação do ONTAP" .
DHCP	68	UDP	Gerenciamento de nós LIF	DHCP	Cliente DHCP para configuração inicial
DHCPS	67	UDP	Gerenciamento de nós LIF	DHCP	Servidor DHCP
DNS	53	UDP	Gerenciamento de nós LIF e dados LIF (NFS, CIFS)	DNS	DNS
NDMP	18600–18699	TCP	Gerenciamento de nós LIF	Servidores de destino	Cópia do NDMP
SMTP	25	TCP	Gerenciamento de nós LIF	Servidor de e-mail	Alertas SMTP podem ser usados para AutoSupport
SNMP	161	TCP	Gerenciamento de nós LIF	Servidor de monitoramento	Monitoramento por armadilhas SNMP
	161	UDP	Gerenciamento de nós LIF	Servidor de monitoramento	Monitoramento por armadilhas SNMP
	162	TCP	Gerenciamento de nós LIF	Servidor de monitoramento	Monitoramento por armadilhas SNMP
	162	UDP	Gerenciamento de nós LIF	Servidor de monitoramento	Monitoramento por armadilhas SNMP
SnapMirror	11104	TCP	LIF interaglomerado	LIFs interaglomerados ONTAP	Gerenciamento de sessões de comunicação entre clusters para SnapMirror
	11105	TCP	LIF interaglomerado	LIFs interaglomerados ONTAP	Transferência de dados do SnapMirror

Serviço	Porta	Protocolo	Fonte	Destino	Propósito
Log de sistema	514	UDP	Gerenciamento de nós LIF	Servidor Syslog	Mensagens de encaminhamento do Syslog

Requisitos para o agente do console

Se você ainda não criou um agente do Console, revise também os requisitos de rede para o agente do Console.

- "Exibir requisitos de rede para o agente do Console"
- "Regras de grupo de segurança no Azure"

Tópicos relacionados

- "Verifique a configuração do AutoSupport para o Cloud Volumes ONTAP"
- "Saiba mais sobre as portas internas do ONTAP" .

Configurar o Cloud Volumes ONTAP para usar uma chave gerenciada pelo cliente no Azure

Os dados são criptografados automaticamente no Cloud Volumes ONTAP no Azure usando o Azure Storage Service Encryption com uma chave gerenciada pela Microsoft. Mas você pode usar sua própria chave de criptografia seguindo os passos nesta página.

Visão geral da criptografia de dados

Os dados do Cloud Volumes ONTAP são criptografados automaticamente no Azure usando "Criptografia do Serviço de Armazenamento do Azure" . A implementação padrão usa uma chave gerenciada pela Microsoft. Nenhuma configuração é necessária.

Se você quiser usar uma chave gerenciada pelo cliente com o Cloud Volumes ONTAP, precisará concluir as seguintes etapas:

1. No Azure, crie um cofre de chaves e depois gere uma chave nesse cofre.
2. No NetApp Console, use a API para criar um sistema Cloud Volumes ONTAP que usa a chave.

Como os dados são criptografados

O Console usa um conjunto de criptografia de disco, que permite o gerenciamento de chaves de criptografia com discos gerenciados, não blobs de páginas. Todos os novos discos de dados também usam o mesmo conjunto de criptografia de disco. Versões anteriores usarão a chave gerenciada pela Microsoft, em vez da chave gerenciada pelo cliente.

Depois de criar um sistema Cloud Volumes ONTAP configurado para usar uma chave gerenciada pelo cliente, os dados do Cloud Volumes ONTAP são criptografados da seguinte maneira.

Configuração do Cloud Volumes ONTAP	Discos do sistema usados para criptografia de chaves	Discos de dados usados para criptografia de chaves
Nó único	• Bota • Essencial • NVRAM	• Raiz • Dados
Zona de disponibilidade única do Azure HA com blobs de página	• Bota • Essencial • NVRAM	Nenhum
Zona de disponibilidade única do Azure HA com discos gerenciados compartilhados	• Bota • Essencial • NVRAM	• Raiz • Dados
Várias zonas de disponibilidade do Azure HA com discos gerenciados compartilhados	• Bota • Essencial • NVRAM	• Raiz • Dados

Todas as contas de armazenamento do Azure para o Cloud Volumes ONTAP são criptografadas usando uma chave gerenciada pelo cliente. Se quiser criptografar suas contas de armazenamento durante sua criação, você deverá criar e fornecer o ID do recurso na solicitação de criação do Cloud Volumes ONTAP . Isso se aplica a todos os tipos de implantações. Se você não fornecer, as contas de armazenamento ainda serão criptografadas, mas o Console primeiro cria as contas de armazenamento com criptografia de chave gerenciada pela Microsoft e depois atualiza as contas de armazenamento para usar a chave gerenciada pelo cliente.

Rotação de chaves no Cloud Volumes ONTAP

Ao configurar suas chaves de criptografia, você deve usar o portal do Azure para configurar e habilitar a rotação automática de chaves. Criar e habilitar uma nova versão de chaves de criptografia garante que o Cloud Volumes ONTAP possa detectar e usar automaticamente a versão mais recente da chave para criptografia, garantindo que seus dados permaneçam seguros sem a necessidade de intervenção manual.

Para obter informações sobre como configurar suas chaves e definir a rotação de chaves, consulte os seguintes tópicos de documentação do Microsoft Azure:

- "Configurar a rotação automática da chave criptográfica no Azure Key Vault"
- "Azure PowerShell - Habilitar chaves gerenciadas pelo cliente"

> Após configurar as chaves, certifique-se de ter selecionado "*Ativar rotação automática*" , para que o Cloud Volumes ONTAP possa usar as novas chaves quando as chaves anteriores expirarem. Se você não habilitar essa opção no portal do Azure, o Cloud Volumes ONTAP não poderá detectar automaticamente as novas chaves, o que pode causar problemas com o provisionamento de armazenamento.

Crie uma identidade gerenciada atribuída pelo usuário

Você tem a opção de criar um recurso chamado identidade gerenciada atribuída pelo usuário. Isso permite que você criptografe suas contas de armazenamento ao criar um sistema Cloud Volumes ONTAP . Recomendamos criar este recurso antes de criar um cofre de chaves e gerar uma chave.

O recurso tem o seguinte ID: `userassignedidentity` .

Passos

1. No Azure, acesse Serviços do Azure e selecione **Identidades Gerenciadas**.
2. Clique em **Criar**.
3. Forneça os seguintes detalhes:
   - **Assinatura**: Escolha uma assinatura. Recomendamos escolher a mesma assinatura do agente do Console.
   - **Grupo de recursos**: use um grupo de recursos existente ou crie um novo.
   - **Região**: Opcionalmente, selecione a mesma região do agente do Console.
   - **Nome**: Digite um nome para o recurso.
4. Opcionalmente, adicione tags.
5. Clique em **Criar**.

Crie um cofre de chaves e gere uma chave

O cofre de chaves deve residir na mesma assinatura e região do Azure em que você planeja criar o sistema Cloud Volumes ONTAP .

Se vocêcriou uma identidade gerenciada atribuída pelo usuário , ao criar o cofre de chaves, você também deve criar uma política de acesso para o cofre de chaves.

Passos

1. "Crie um cofre de chaves na sua assinatura do Azure" .

   Observe os seguintes requisitos para o cofre de chaves:

   - O cofre de chaves deve residir na mesma região que o sistema Cloud Volumes ONTAP .
   - As seguintes opções devem ser habilitadas:
     - **Exclusão suave** (esta opção é habilitada por padrão, mas *não* deve ser desabilitada)
     - **Proteção contra purga**
     - **Azure Disk Encryption para criptografia de volumes** (para sistemas de nó único, pares de HA em várias zonas e implantações de par de HA em uma única zona de disponibilidade)

       O uso de chaves de criptografia gerenciadas pelo cliente do Azure depende da habilitação da criptografia do Azure Disk para o cofre de chaves.

   - A seguinte opção deve ser habilitada se você criou uma identidade gerenciada atribuída pelo usuário:
     - **Política de acesso ao cofre**
2. Se você selecionou a política de acesso ao cofre, clique em Criar para criar uma política de acesso para o cofre de chaves. Caso contrário, pule para a etapa 3.

a. Selecione as seguintes permissões:
   - pegar
   - lista
   - decifrar
   - criptografar
   - desembrulhar chave
   - chave de envoltório
   - verificar
   - sinal

b. Selecione a identidade gerenciada atribuída pelo usuário (recurso) como principal.

c. Revise e crie a política de acesso.

3. "Gerar uma chave no cofre de chaves" .

   Observe os seguintes requisitos para a chave:

   - O tipo de chave deve ser **RSA**.
   - O tamanho de chave RSA recomendado é **2048**, mas outros tamanhos são suportados.

Crie um sistema que use a chave de criptografia

Depois de criar o cofre de chaves e gerar uma chave de criptografia, você pode criar um novo sistema Cloud Volumes ONTAP configurado para usar a chave. Essas etapas são suportadas pelo uso da API.

Permissões necessárias

Se você quiser usar uma chave gerenciada pelo cliente com um sistema Cloud Volumes ONTAP de nó único, certifique-se de que o agente do Console tenha as seguintes permissões:

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/diskEncryptionSets/write",
"Microsoft.Compute/diskEncryptionSets/delete"
"Microsoft.KeyVault/vaults/deploy/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

"Veja a lista mais recente de permissões"

Passos

1. Obtenha a lista de cofres de chaves na sua assinatura do Azure usando a seguinte chamada de API.

   Para um par HA: `GET /azure/ha/metadata/vaults`

   Para nó único: `GET /azure/vsa/metadata/vaults`

   Anote o **nome** e o **resourceGroup**. Você precisará especificar esses valores na próxima etapa.

"Saiba mais sobre esta chamada de API" .

2. Obtenha a lista de chaves dentro do cofre usando a seguinte chamada de API.

   Para um par HA: `GET /azure/ha/metadata/keys-vault`

   Para nó único: `GET /azure/vsa/metadata/keys-vault`

   Anote o **keyName**. Você precisará especificar esse valor (junto com o nome do cofre) na próxima etapa.

   "Saiba mais sobre esta chamada de API" .

3. Crie um sistema Cloud Volumes ONTAP usando a seguinte chamada de API.

   a. Para um par HA:

      `POST /azure/ha/working-environments`

      O corpo da solicitação deve incluir os seguintes campos:

```
"azureEncryptionParameters": {
                "key": "keyName",
                "vaultName": "vaultName"
}
```

      Incluir o `"userAssignedIdentity": " userAssignedIdentityId"` campo se você criou este recurso para ser usado para criptografia de conta de armazenamento.

      "Saiba mais sobre esta chamada de API" .

   b. Para um sistema de nó único:

      `POST /azure/vsa/working-environments`

      O corpo da solicitação deve incluir os seguintes campos:

```
"azureEncryptionParameters": {
                "key": "keyName",
                "vaultName": "vaultName"
}
```

      Incluir o `"userAssignedIdentity": " userAssignedIdentityId"` campo se você criou este recurso para ser usado para criptografia de conta de armazenamento.

   "Saiba mais sobre esta chamada de API" .

Resultado

Você tem um novo sistema Cloud Volumes ONTAP configurado para usar sua chave gerenciada pelo cliente

para criptografia de dados.

Configurar o licenciamento do Cloud Volumes ONTAP no Azure

Depois de decidir qual opção de licenciamento você deseja usar com o Cloud Volumes ONTAP, algumas etapas são necessárias antes que você possa escolher essa opção de licenciamento ao criar um novo sistema.

Freemium

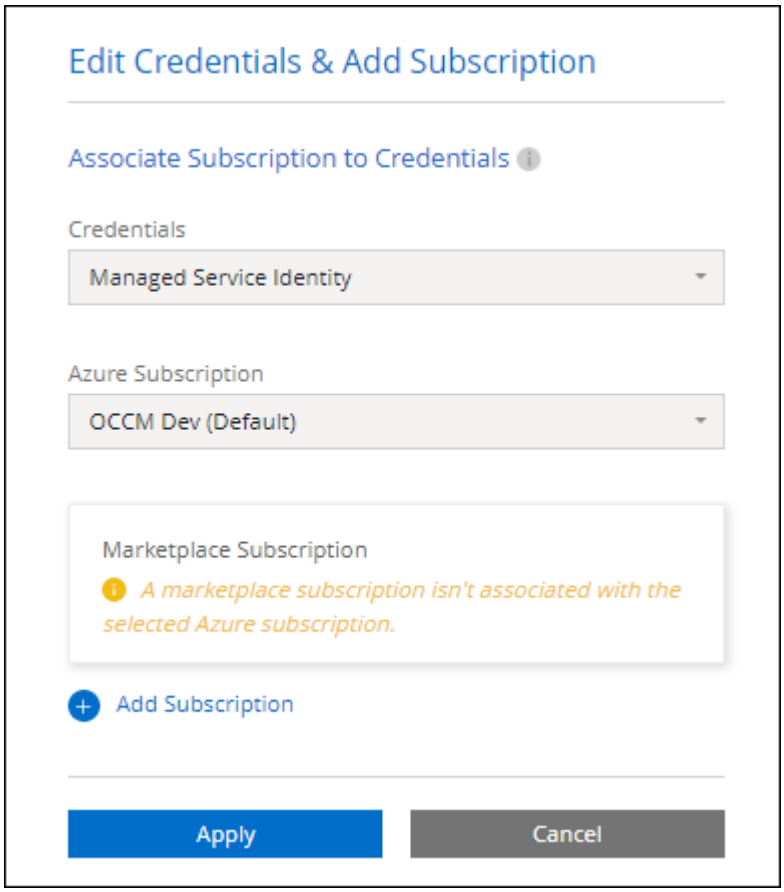
Selecione a oferta Freemium para usar o Cloud Volumes ONTAP gratuitamente com até 500 GiB de capacidade provisionada. "Saiba mais sobre a oferta Freemium" .

Passos

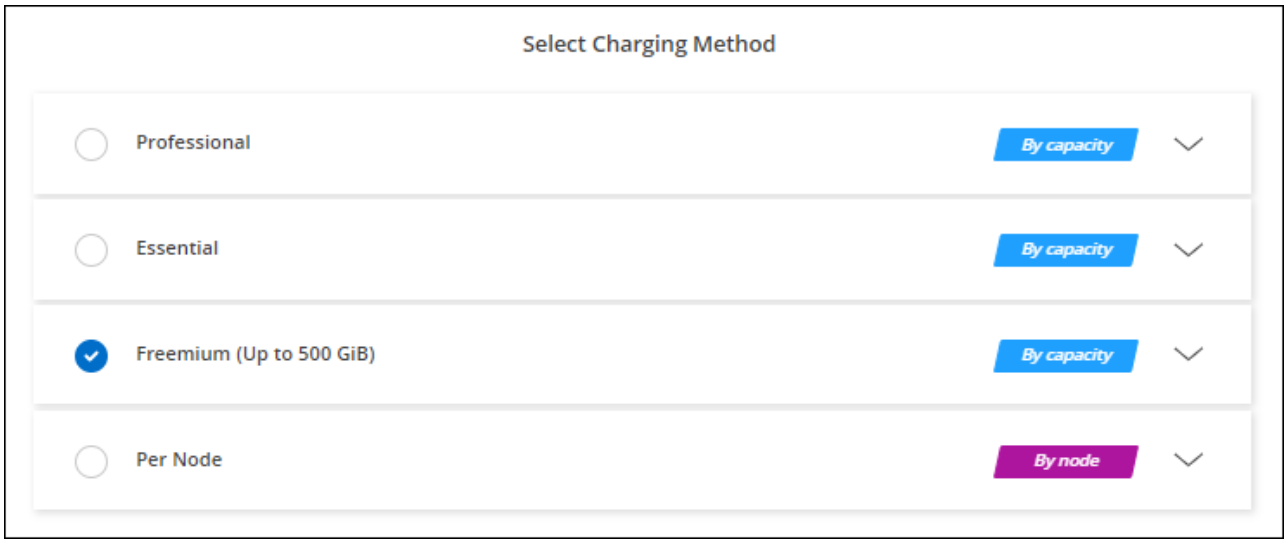
1. No menu de navegação esquerdo do NetApp Console, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas.

    a. Na página **Detalhes e credenciais**, clique em **Editar credenciais > Adicionar assinatura** e siga as instruções para assinar a oferta de pagamento conforme o uso no Azure Marketplace.

    Você não será cobrado pela assinatura do marketplace, a menos que exceda 500 GiB de capacidade provisionada, momento em que o sistema será automaticamente convertido para o"Pacote Essentials" .



    a. Após retornar ao Console, selecione **Freemium** quando chegar à página de métodos de cobrança.



"Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP no Azure" .

Licença baseada em capacidade

O licenciamento baseado em capacidade permite que você pague pelo Cloud Volumes ONTAP por TiB de capacidade. O licenciamento baseado em capacidade está disponível na forma de um *pacote*: o pacote Essentials ou o pacote Professional.

Os pacotes Essentials e Professional estão disponíveis nos seguintes modelos de consumo ou opções de compra:

- Uma licença (traga sua própria licença (BYOL)) adquirida da NetApp
- Uma assinatura por hora, paga conforme o uso (PAYGO) do Azure Marketplace
- Um contrato anual

"Saiba mais sobre licenciamento baseado em capacidade" .

As seções a seguir descrevem como começar a usar cada um desses modelos de consumo.

Traga sua própria bebida

Pague antecipadamente comprando uma licença (BYOL) da NetApp para implantar sistemas Cloud Volumes ONTAP em qualquer provedor de nuvem.

A NetApp restringiu a compra, extensão e renovação de licenças BYOL. Para obter mais informações, consulte "Disponibilidade restrita de licenciamento BYOL para Cloud Volumes ONTAP" .

Passos

1. "Entre em contato com a equipe de vendas da NetApp para obter uma licença"
2. "Adicione sua conta do site de suporte da NetApp ao console"

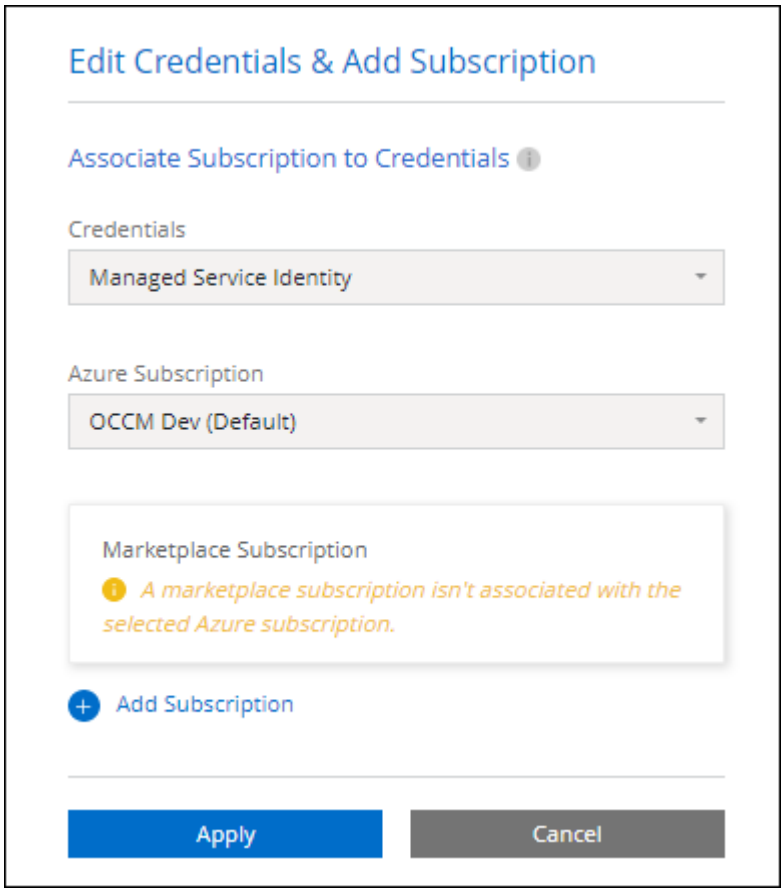
   O Console consulta automaticamente o serviço de licenciamento da NetApp para obter detalhes sobre as licenças associadas à sua conta do Site de Suporte da NetApp . Se não houver erros, o Console adicionará automaticamente as licenças ao Console.

Sua licença deve estar disponível no Console antes que você possa usá-la com o Cloud Volumes ONTAP. Se necessário, você pode"adicione manualmente a licença ao Console" .

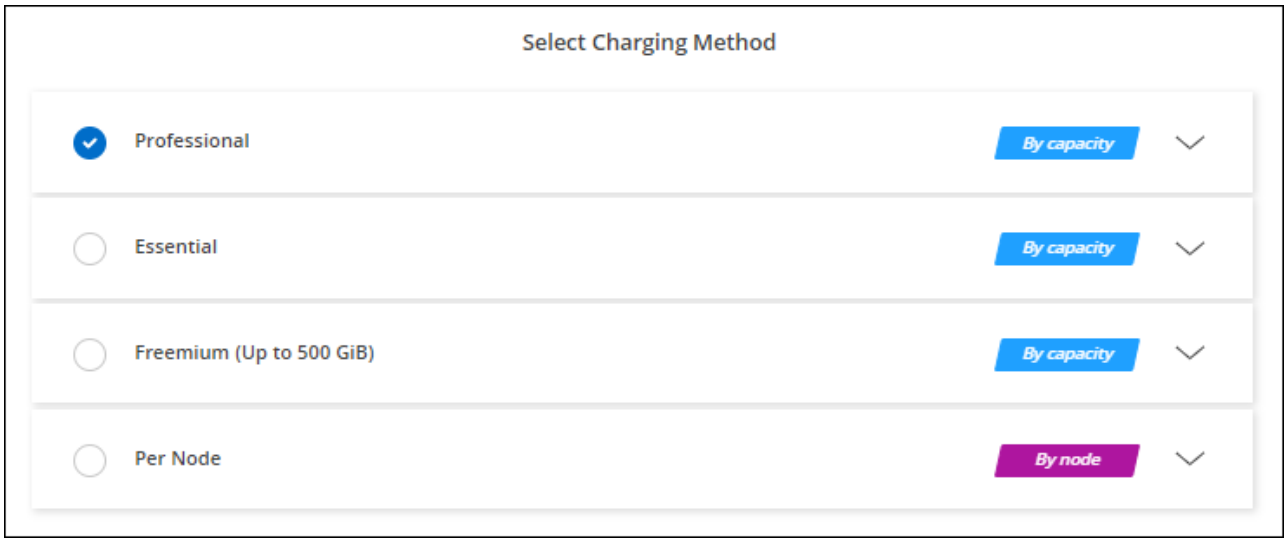
3. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas.

   a. Na página **Detalhes e credenciais**, clique em **Editar credenciais > Adicionar assinatura** e siga as instruções para assinar a oferta de pagamento conforme o uso no Azure Marketplace.

      A licença que você comprou da NetApp é sempre cobrada primeiro, mas você será cobrado pela taxa horária no mercado se exceder sua capacidade licenciada ou se o prazo de sua licença expirar.



   a. Após retornar ao Console, selecione um pacote baseado em capacidade quando chegar à página de métodos de cobrança.



"Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP no Azure" .

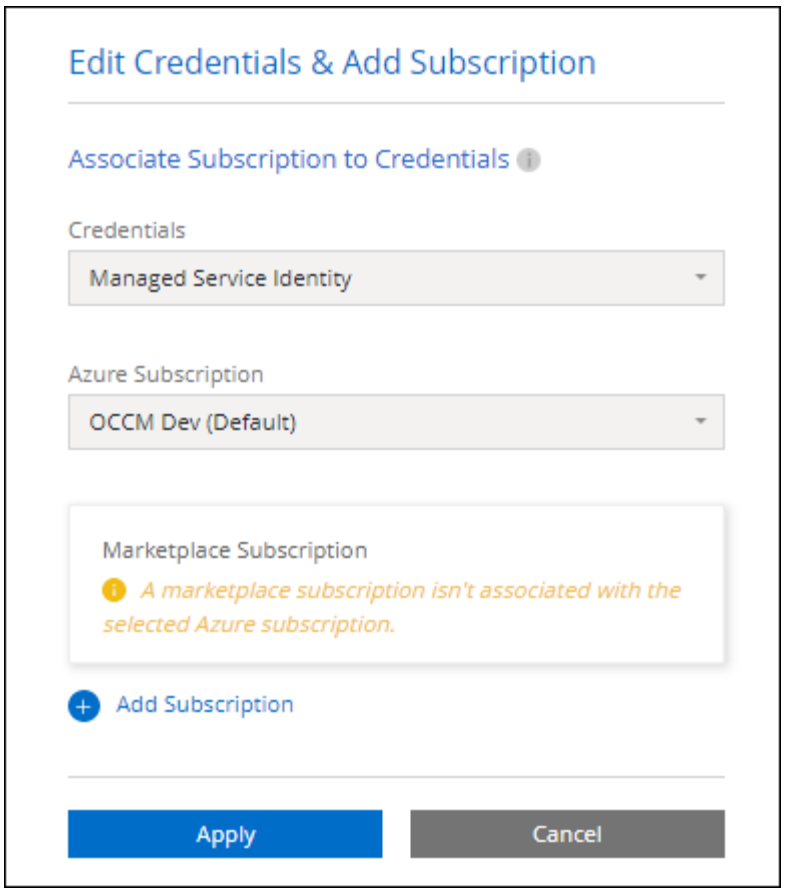
Assinatura PAYGO

Pague por hora assinando a oferta do marketplace do seu provedor de nuvem.

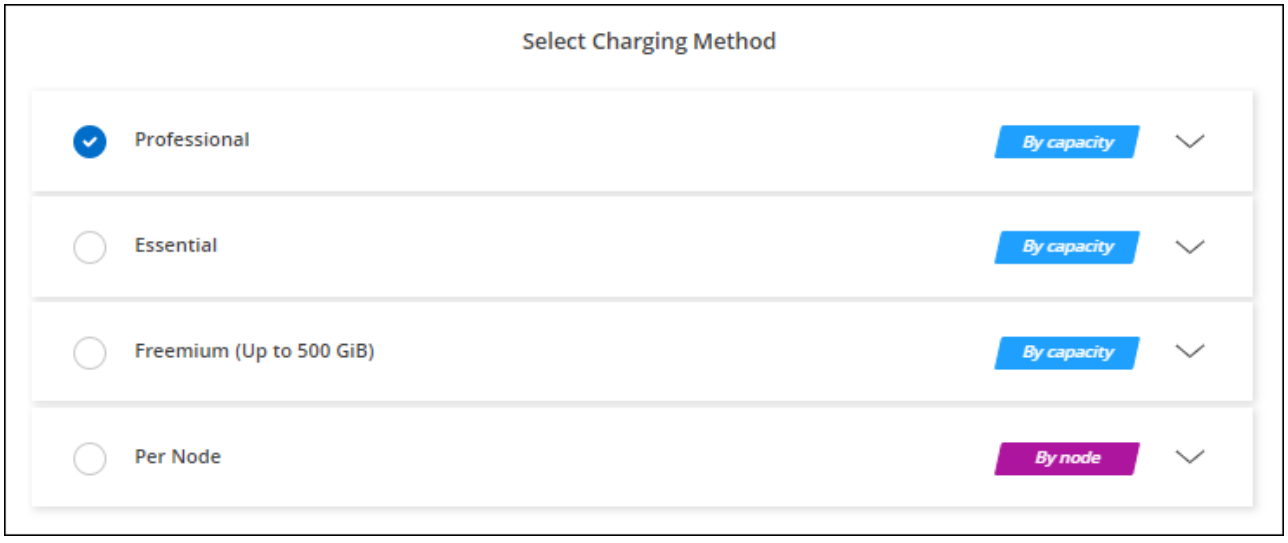
Ao criar um sistema Cloud Volumes ONTAP , o Console solicita que você assine o contrato disponível no Azure Marketplace. Essa assinatura é então associada ao sistema de cobrança. Você pode usar a mesma assinatura para sistemas adicionais.

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas.
   a. Na página **Detalhes e credenciais**, clique em **Editar credenciais > Adicionar assinatura** e siga as instruções para assinar a oferta de pagamento conforme o uso no Azure Marketplace.



b. Após retornar ao Console, selecione um pacote baseado em capacidade quando chegar à página de métodos de cobrança.



"Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP no Azure" .

Você pode gerenciar as assinaturas do Azure Marketplace associadas às suas contas do Azure na página Configurações > Credenciais. "Aprenda a gerenciar suas contas e assinaturas do Azure"

Contrato anual

Pague pelo Cloud Volumes ONTAP anualmente comprando um contrato anual.

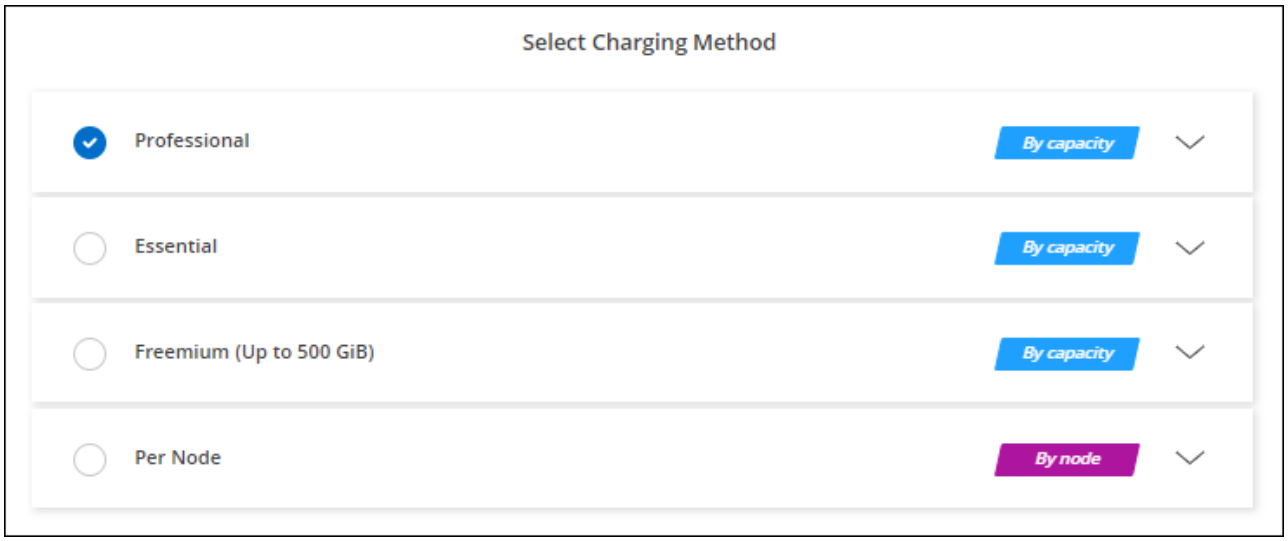
Passos

1. Entre em contato com seu representante de vendas da NetApp para adquirir um contrato anual.

   O contrato está disponível como uma oferta *privada* no Azure Marketplace.

   Depois que a NetApp compartilhar a oferta privada com você, você poderá selecionar o plano anual ao assinar o Azure Marketplace durante a criação do sistema.

2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas.
   a. Na página **Detalhes e credenciais**, clique em **Editar credenciais > Adicionar assinatura > Continuar**.
   b. No portal do Azure, selecione o plano anual que foi compartilhado com sua conta do Azure e clique em **Assinar**.
   c. Após retornar ao Console, selecione um pacote baseado em capacidade quando chegar à página de métodos de cobrança.



"Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP no Azure" .

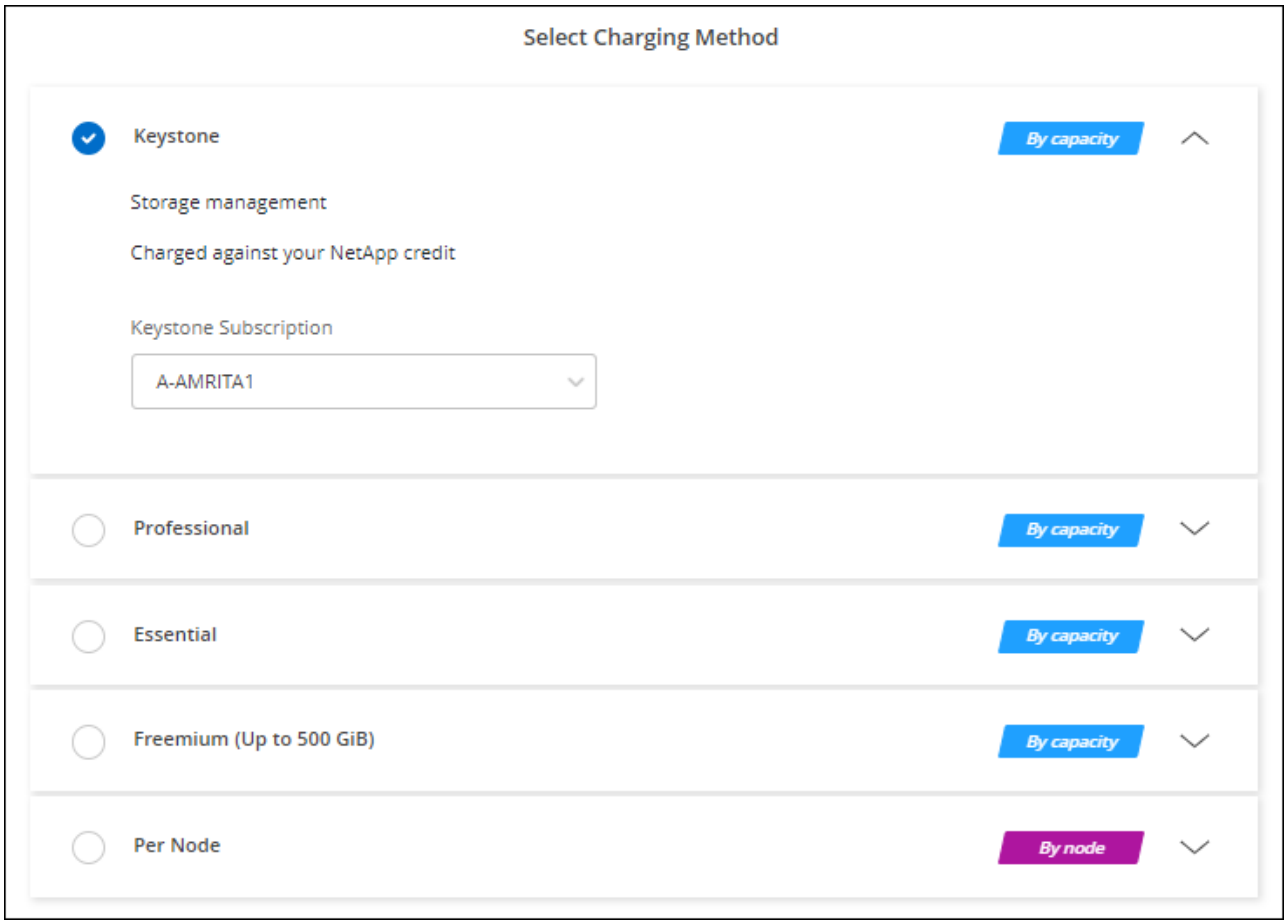
Assinatura Keystone

Uma assinatura Keystone é um serviço baseado em assinatura com pagamento conforme o crescimento. "Saiba mais sobre as assinaturas do NetApp Keystone" .

Passos

1. Se você ainda não tem uma assinatura, "entre em contato com a NetApp"
2. Entre em contato com a NetApp para autorizar sua conta de usuário no Console com uma ou mais assinaturas do Keystone .
3. Depois que a NetApp autorizar sua conta,"vincule suas assinaturas para uso com o Cloud Volumes ONTAP" .
4. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas.

a. Selecione o método de cobrança da Assinatura Keystone quando solicitado a escolher um método de cobrança.



"Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP no Azure" .

Licença baseada em nó

Uma licença baseada em nó é a licença da geração anterior para o Cloud Volumes ONTAP. Uma licença baseada em nó pode ser adquirida da NetApp (BYOL) e está disponível para renovações de licença apenas em casos específicos. Para obter informações, consulte:

- "Fim da disponibilidade de licenças baseadas em nós"
- "Fim da disponibilidade de licenças baseadas em nós"
- "Converter uma licença baseada em nós para uma licença baseada em capacidade."

Habilitar o modo de alta disponibilidade para o Cloud Volumes ONTAP no Azure

Você deve habilitar o modo de alta disponibilidade (HA) do Microsoft Azure para reduzir os tempos de failover não planejados e habilitar o suporte a NFSv4 para Cloud Volumes ONTAP. Se você habilitar esse modo, seus nós HA do Cloud Volumes ONTAP poderão atingir um baixo tempo de recuperação (RTO) de 60 segundos durante failovers não planejados em clientes CIFS e NFSv4.

A partir do Cloud Volumes ONTAP 9.10.1, reduzimos o tempo de failover não planejado para pares de HA do

Cloud Volumes ONTAP em execução no Microsoft Azure e adicionamos suporte para NFSv4. Para disponibilizar esses aprimoramentos no Cloud Volumes ONTAP, você precisa habilitar o recurso de alta disponibilidade na sua assinatura do Azure.

Sobre esta tarefa

NetApp Console solicita esses detalhes quando o recurso precisa ser habilitado em uma assinatura do Azure. Observe o seguinte:

- Não há problemas com a alta disponibilidade do seu par Cloud Volumes ONTAP HA. Este recurso do Azure funciona em conjunto com o ONTAP para reduzir o tempo de interrupção do aplicativo observado pelo cliente para protocolos NFS que resultam de eventos de failover não planejados.
- A ativação desse recurso não causa interrupções nos pares de HA do Cloud Volumes ONTAP .
- Habilitar esse recurso na sua assinatura do Azure não causa problemas para outras VMs.
- O Cloud Volumes ONTAP usa um balanceador de carga interno do Azure durante failovers de LIFs de gerenciamento de cluster e SVM em clientes CIFS e NFS.
- Quando o modo HA está habilitado, o Console verifica o sistema a cada 12 horas para atualizar as regras internas do Balanceador de Carga do Azure.

Passos

Um usuário do Azure com privilégios de *Proprietário* pode habilitar o recurso a partir do Azure CLI.

1. "Acesse o Azure Cloud Shell pelo Portal do Azure"
2. Registre o recurso de modo de alta disponibilidade:

```
az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
az feature register --name EnableHighAvailabilityMode --namespace
Microsoft.Network
az provider register -n Microsoft.Network
```

3. Opcionalmente, verifique se o recurso agora está registrado:

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

   A CLI do Azure deve retornar um resultado semelhante ao seguinte:

```
{
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Features/providers/Microsoft.Network/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

Links relacionados

1. "Microsoft Azure documentação: Visão geral das portas de alta disponibilidade"
2. "Microsoft Azure documentação: introdução à CLI do Azure"

Habilitar VMOrchestratorZonalMultiFD para Cloud Volumes ONTAP no Azure

Para implantar instâncias de VM em zonas de disponibilidade única (AZ) de armazenamento localmente redundante (LRS), você deve ativar o Microsoft `Microsoft.Compute/VMOrchestratorZonalMultiFD` recurso para suas assinaturas. Em um modo de alta disponibilidade (HA), esse recurso facilita a implantação de nós em domínios de falhas separados na mesma zona de disponibilidade.

A menos que você ative esse recurso, a implantação zonal não ocorrerá, e a implantação não zonal anterior do LRS entrará em vigor.

Para obter informações sobre a implantação de VM em uma única zona de disponibilidade, consulte"Pares de alta disponibilidade no Azure" .

Execute estas etapas como um usuário com privilégios de "Proprietário":

Passos

1. Acesse o Azure Cloud Shell pelo portal do Azure. Para obter informações, consulte o "Documentação do Microsoft Azure: Introdução ao Azure Cloud Shell" .
2. Registre-se para o `Microsoft.Compute/VMOrchestratorZonalMultiFD` recurso executando este comando:

   az account set -s <*Nome_ou_ID_da_assinatura_do_Azure*> az feature register --name VMOrchestratorZonalMultiFD --namespace Microsoft.Compute

3. Verifique o status do registro e a amostra de saída:

az feature show -n VMOrchestratorZonalMultiFD --namespace Microsoft.Compute { "id": "/subscriptions/<*ID*>/providers/Microsoft.Features/providers/Microsoft.Compute/features/VMOrchestratorZonalMultiFD", "name": "Microsoft.Compute/VMOrchestratorZonalMultiFD", "properties": { "state": "Registered" }, "type": "Microsoft.Features/providers/features" }

Inicie o Cloud Volumes ONTAP no Azure

Você pode iniciar um sistema de nó único ou um par de HA no Azure criando um sistema Cloud Volumes ONTAP no NetApp Console.

Antes de começar

Você precisa do seguinte antes de começar.

- Um agente do Console que está ativo e em execução.
  - Você deveria ter um "Agente de console associado ao seu sistema" .
  - "Você deve estar preparado para deixar o agente do Console em execução o tempo todo" .
- Uma compreensão da configuração que você deseja usar.

  Você deve ter uma configuração planejada e os detalhes necessários da rede do Azure fornecidos pelo seu administrador. Para mais informações, consulte "Planejando sua configuração do Cloud Volumes ONTAP" .
- Uma compreensão do que é necessário para configurar o licenciamento do Cloud Volumes ONTAP.

  "Aprenda como configurar o licenciamento" .

Sobre esta tarefa

Quando o Console cria um sistema Cloud Volumes ONTAP no Azure, ele cria vários objetos do Azure, como um grupo de recursos, interfaces de rede e contas de armazenamento. Você pode revisar um resumo dos recursos no final do assistente.

> **Potencial de perda de dados**
>
> A prática recomendada é usar um novo grupo de recursos dedicado para cada sistema Cloud Volumes ONTAP .
>
> Não é recomendado implantar o Cloud Volumes ONTAP em um grupo de recursos compartilhados existente devido ao risco de perda de dados. Embora o Console possa remover recursos do Cloud Volumes ONTAP de um grupo de recursos compartilhados em caso de falha de implantação ou exclusão, um usuário do Azure pode excluir acidentalmente recursos do Cloud Volumes ONTAP de um grupo de recursos compartilhados.

Inicie um sistema Cloud Volumes ONTAP de nó único no Azure

Se você deseja iniciar um sistema Cloud Volumes ONTAP de nó único no Azure, precisa criar um sistema de nó único no Console.

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.

2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as instruções.
3. **Escolha um local**: Selecione **Microsoft Azure** e * Cloud Volumes ONTAP Single Node*.
4. Se você for solicitado, "criar um agente de console" .
5. **Detalhes e credenciais**: Opcionalmente, altere as credenciais e a assinatura do Azure, especifique um nome de cluster, adicione tags, se necessário, e especifique as credenciais.

   A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Nome do sistema	O Console usa o nome do sistema para nomear o sistema Cloud Volumes ONTAP e a máquina virtual do Azure. Ele também usa o nome como prefixo para o grupo de segurança predefinido, se você selecionar essa opção.
Tags de grupos de recursos	Tags são metadados para seus recursos do Azure. Quando você insere tags neste campo, o Console as adiciona ao grupo de recursos associado ao sistema Cloud Volumes ONTAP . Você pode adicionar até quatro tags da interface do usuário ao criar um sistema e depois adicionar mais depois que ele for criado. Observe que a API não limita você a quatro tags ao criar um sistema. Para obter informações sobre etiquetas, consulte o "Documentação do Microsoft Azure: Usando tags para organizar seus recursos do Azure" .
Nome de usuário e senha	Estas são as credenciais para a conta de administrador do cluster Cloud Volumes ONTAP . Você pode usar essas credenciais para se conectar ao Cloud Volumes ONTAP por meio do ONTAP System Manager ou do ONTAP CLI. Mantenha o nome de usuário padrão *admin* ou altere-o para um nome de usuário personalizado.
Editar credenciais	Você pode escolher diferentes credenciais do Azure e uma assinatura diferente do Azure para usar com este sistema Cloud Volumes ONTAP . Você precisa associar uma assinatura do Azure Marketplace à assinatura do Azure selecionada para implantar um sistema Cloud Volumes ONTAP pago conforme o uso. "Aprenda como adicionar credenciais" .

6. **Serviços**: habilite ou desabilite os serviços individuais que você deseja ou não usar com o Cloud Volumes ONTAP.
   - "Saiba mais sobre a NetApp Data Classification"
   - "Saiba mais sobre o NetApp Backup and Recovery"

   Se você quiser utilizar WORM e camadas de dados, desabilite o Backup e Recuperação e implante um sistema Cloud Volumes ONTAP com versão 9.8 ou superior.

7. **Localização**: selecione uma região, zona de disponibilidade, VNet e sub-rede e, em seguida, marque a caixa de seleção para confirmar a conectividade de rede entre o agente do Console e o local de destino.

   Para regiões da China, implantações de nó único são suportadas apenas no Cloud Volumes ONTAP 9.12.1 GA e 9.13.0 GA. Você pode atualizar essas versões para patches e lançamentos posteriores do Cloud Volumes ONTAP como"suportado no Azure" . Se você quiser implantar versões posteriores do Cloud Volumes ONTAP em regiões da China, entre em contato com o Suporte da NetApp . Somente licenças compradas diretamente da NetApp são suportadas nas regiões da China; assinaturas do marketplace não estão disponíveis.

8. **Conectividade**: Escolha um grupo de recursos novo ou existente e, em seguida, escolha se deseja usar o grupo de segurança predefinido ou usar o seu próprio.

   A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Grupo de Recursos	Crie um novo grupo de recursos para o Cloud Volumes ONTAP ou use um grupo de recursos existente. A prática recomendada é usar um novo grupo de recursos dedicado para o Cloud Volumes ONTAP. Embora seja possível implantar o Cloud Volumes ONTAP em um grupo de recursos compartilhados existente, isso não é recomendado devido ao risco de perda de dados. Veja o aviso acima para mais detalhes. Se a conta do Azure que você está usando tiver o "permissões necessárias" , o Console remove os recursos do Cloud Volumes ONTAP de um grupo de recursos, em caso de falha de implantação ou exclusão.
Grupo de segurança gerado	Se você deixar o Console gerar o grupo de segurança para você, precisará escolher como permitirá o tráfego: • Se você escolher **Somente VNet selecionada**, a origem do tráfego de entrada será o intervalo de sub-redes da VNet selecionada e o intervalo de sub-redes da VNet onde o agente do Console reside. Esta é a opção recomendada. • Se você escolher **Todas as VNets**, a origem do tráfego de entrada será o intervalo de IP 0.0.0.0/0.
Use existente	Se você escolher um grupo de segurança existente, ele deverá atender aos requisitos do Cloud Volumes ONTAP . "Exibir o grupo de segurança padrão" .

9. **Métodos de cobrança e conta NSS**: especifique qual opção de cobrança você gostaria de usar com este sistema e, em seguida, especifique uma conta do site de suporte da NetApp .
   - "Saiba mais sobre as opções de licenciamento do Cloud Volumes ONTAP" .
   - "Aprenda como configurar o licenciamento" .
10. **Pacotes pré-configurados**: selecione um dos pacotes para implantar rapidamente um sistema Cloud Volumes ONTAP ou clique em **Criar minha própria configuração**.

    Se você escolher um dos pacotes, precisará apenas especificar um volume e depois revisar e aprovar a configuração.

11. **Licenciamento**: Altere a versão do Cloud Volumes ONTAP , se necessário, e selecione um tipo de máquina virtual.

    Se uma versão mais recente do Release Candidate, Disponibilidade Geral ou patch estiver disponível para a versão selecionada, o BlueXP atualizará o sistema para essa versão ao criar o ambiente de trabalho. Por exemplo, a atualização ocorre se você selecionar Cloud Volumes ONTAP 9.16.1 P3 e 9.16.1 P4 estiver disponível. A atualização não ocorre de uma versão para outra, por exemplo, da 9.15 para a 9.16.

12. **Inscreva-se no Azure Marketplace**: Você verá esta página se o Console não conseguir habilitar implantações programáticas do Cloud Volumes ONTAP. Siga os passos listados na tela. consulte "Implantação programática de produtos do Marketplace" para mais informações.
13. **Recursos de armazenamento subjacentes**: escolha as configurações para o agregado inicial: um tipo de disco, um tamanho para cada disco e se a hierarquização de dados para armazenamento de Blobs deve ser habilitada.

    Observe o seguinte:

    - Se o acesso público à sua conta de armazenamento estiver desabilitado na VNet, você não poderá habilitar a hierarquização de dados no seu sistema Cloud Volumes ONTAP . Para obter informações, consulte"Regras do grupo de segurança" .
    - O tipo de disco é para o volume inicial. Você pode escolher um tipo de disco diferente para volumes subsequentes.
    - O tamanho do disco é para todos os discos no agregado inicial e para quaisquer agregados adicionais que o Console cria quando você usa a opção de provisionamento simples. Você pode criar agregados que usam um tamanho de disco diferente usando a opção de alocação avançada.

      Para obter ajuda na escolha do tipo e tamanho do disco, consulte"Dimensionando seu sistema no Azure" .

    - Você pode escolher uma política específica de níveis de volume ao criar ou editar um volume.
    - Se você desabilitar a hierarquização de dados, poderá habilitá-la em agregações subsequentes.

      "Saiba mais sobre camadas de dados" .

14. **Velocidade de gravação e WORM**:

    a. Escolha a velocidade de gravação **Normal** ou **Alta**, se desejar.

       "Saiba mais sobre velocidade de gravação" .

    b. Ative o armazenamento WORM (escreva uma vez e leia muitas vezes), se desejar.

       Esta opção está disponível apenas para determinados tipos de VM. Para descobrir quais tipos de VM são suportados, consulte"Configurações suportadas por licença para pares HA" .

       O WORM não pode ser habilitado se a hierarquização de dados estiver habilitada para as versões 9.7 e anteriores do Cloud Volumes ONTAP . A reversão ou o downgrade para o Cloud Volumes ONTAP 9.8 é bloqueado após a ativação do WORM e da hierarquização.

    "Saiba mais sobre o armazenamento WORM" .

    a. Se você ativar o armazenamento WORM, selecione o período de retenção.

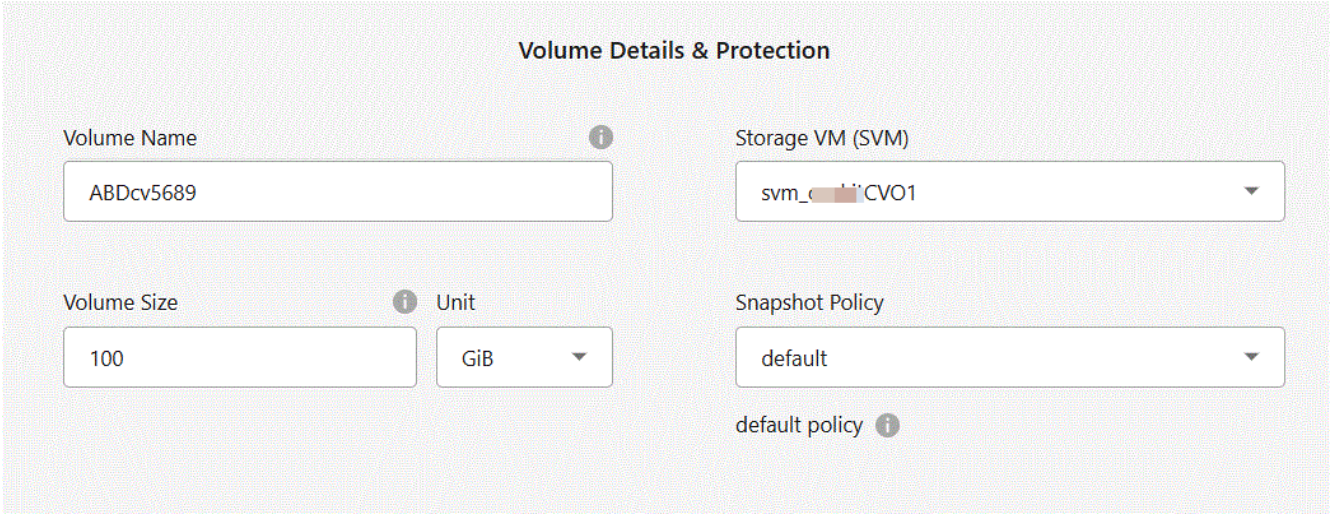
15. **Criar volume**: insira detalhes para o novo volume ou clique em **Ignorar**.

    "Saiba mais sobre os protocolos e versões de clientes suportados" .

    Alguns campos nesta página são autoexplicativos. A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Tamanho	O tamanho máximo que você pode inserir depende muito se você habilita o provisionamento fino, que permite criar um volume maior que o armazenamento físico disponível atualmente.
Controle de acesso (somente para NFS)	Uma política de exportação define os clientes na sub-rede que podem acessar o volume. Por padrão, o Console insere um valor que fornece acesso a todas as instâncias na sub-rede.
Permissões e usuários/grupos (somente para CIFS)	Esses campos permitem que você controle o nível de acesso a um compartilhamento para usuários e grupos (também chamados de listas de controle de acesso ou ACLs). Você pode especificar usuários ou grupos locais ou de domínio do Windows, ou usuários ou grupos do UNIX. Se você especificar um nome de usuário de domínio do Windows, deverá incluir o domínio do usuário usando o formato domínio\nome de usuário.
Política de Snapshot	Uma política de cópia de instantâneo especifica a frequência e o número de cópias de instantâneo do NetApp criadas automaticamente. Uma cópia do NetApp Snapshot é uma imagem do sistema de arquivos de um momento específico que não tem impacto no desempenho e requer armazenamento mínimo. Você pode escolher a política padrão ou nenhuma. Você pode escolher nenhum para dados transitórios: por exemplo, tempdb para Microsoft SQL Server.
Opções avançadas (somente para NFS)	Selecione uma versão do NFS para o volume: NFSv3 ou NFSv4.
Grupo iniciador e IQN (somente para iSCSI)	Os destinos de armazenamento iSCSI são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Os grupos de iniciadores são tabelas de nomes de nós de host iSCSI e controlam quais iniciadores têm acesso a quais LUNs. Os destinos iSCSI se conectam à rede por meio de adaptadores de rede Ethernet padrão (NICs), placas de mecanismo de descarregamento TCP (TOE) com iniciadores de software, adaptadores de rede convergentes (CNAs) ou adaptadores de bust de host dedicados (HBAs) e são identificados por nomes qualificados iSCSI (IQNs). Quando você cria um volume iSCSI, o Console cria automaticamente um LUN para você. Simplificamos criando apenas um LUN por volume, portanto não há gerenciamento envolvido. Depois de criar o volume,"use o IQN para conectar-se ao LUN de seus hosts" .

A imagem a seguir mostra a primeira página do assistente de criação de volume:



16. **Configuração CIFS**: Se você escolher o protocolo CIFS, configure um servidor CIFS.

Campo	Descrição
Endereço IP primário e secundário do DNS	Os endereços IP dos servidores DNS que fornecem resolução de nomes para o servidor CIFS. Os servidores DNS listados devem conter os registros de localização de serviço (SRV) necessários para localizar os servidores LDAP do Active Directory e os controladores de domínio para o domínio ao qual o servidor CIFS se juntará.
Domínio do Active Directory para ingressar	O FQDN do domínio do Active Directory (AD) ao qual você deseja que o servidor CIFS ingresse.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com privilégios suficientes para adicionar computadores à Unidade Organizacional (UO) especificada dentro do domínio do AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio do AD.
Unidade Organizacional	A unidade organizacional dentro do domínio do AD a ser associada ao servidor CIFS. O padrão é CN=Computadores. Para configurar o Azure AD Domain Services como o servidor AD para o Cloud Volumes ONTAP, você deve inserir **OU=AADDC Computers** ou **OU=AADDC Users** neste campo.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentação do Azure: Criar uma Unidade Organizacional (UO) em um domínio gerenciado do Azure AD Domain Services"^]
Domínio DNS	O domínio DNS para a máquina virtual de armazenamento (SVM) do Cloud Volumes ONTAP . Na maioria dos casos, o domínio é o mesmo que o domínio do AD.
Servidor NTP	Selecione **Usar domínio do Active Directory** para configurar um servidor NTP usando o DNS do Active Directory. Se você precisar configurar um servidor NTP usando um endereço diferente, use a API. Consulte o "Documentação de automação do NetApp Console" para mais detalhes. Observe que você só pode configurar um servidor NTP ao criar um servidor CIFS. Não é configurável depois de criar o servidor CIFS.

17. **Perfil de uso, tipo de disco e política de camadas**: escolha se deseja habilitar recursos de eficiência de

armazenamento e alterar a política de camadas de volume, se necessário.

Para mais informações, consulte"Compreendendo os perfis de uso de volume" e"Visão geral da hierarquização de dados" .

18. **Revisar e aprovar**: revise e confirme suas seleções.
    a. Revise os detalhes sobre a configuração.
    b. Clique em **Mais informações** para revisar detalhes sobre o suporte e os recursos do Azure que o Console comprará.
    c. Selecione as caixas de seleção **Eu entendo…**.
    d. Clique em **Ir**.

Resultado

O Console implanta o sistema Cloud Volumes ONTAP . Você pode acompanhar o progresso na página Auditoria.

Se você tiver algum problema ao implantar o sistema Cloud Volumes ONTAP , revise a mensagem de falha. Você também pode selecionar o sistema e clicar em **Recriar ambiente**.

Para obter ajuda adicional, acesse "Suporte NetApp Cloud Volumes ONTAP" .

Após a conclusão do processo de implantação, não modifique as configurações do Cloud Volumes ONTAP geradas pelo sistema no portal do Azure, especialmente as tags do sistema. Quaisquer alterações feitas nessas configurações podem levar a comportamento inesperado ou perda de dados.

Depois que você terminar

- Se você provisionou um compartilhamento CIFS, conceda aos usuários ou grupos permissões para os arquivos e pastas e verifique se esses usuários podem acessar o compartilhamento e criar um arquivo.
- Se você quiser aplicar cotas aos volumes, use o ONTAP System Manager ou o ONTAP CLI.

  As cotas permitem que você restrinja ou rastreie o espaço em disco e o número de arquivos usados por um usuário, grupo ou qtree.

Inicie um par de Cloud Volumes ONTAP HA no Azure

Se você quiser iniciar um par de Cloud Volumes ONTAP HA no Azure, precisará criar um sistema HA no Console.

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as instruções.
3. Se você for solicitado, "criar um agente de console" .
4. **Detalhes e credenciais**: Opcionalmente, altere as credenciais e a assinatura do Azure, especifique um nome de cluster, adicione tags, se necessário, e especifique as credenciais.

   A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Nome do sistema	O Console usa o nome do sistema para nomear o sistema Cloud Volumes ONTAP e a máquina virtual do Azure. Ele também usa o nome como prefixo para o grupo de segurança predefinido, se você selecionar essa opção.
Tags de grupos de recursos	Tags são metadados para seus recursos do Azure. Quando você insere tags neste campo, o Console as adiciona ao grupo de recursos associado ao sistema Cloud Volumes ONTAP . Você pode adicionar até quatro tags da interface do usuário ao criar um sistema e depois adicionar mais depois que ele for criado. Observe que a API não limita você a quatro tags ao criar um sistema. Para obter informações sobre etiquetas, consulte o "Documentação do Microsoft Azure: Usando tags para organizar seus recursos do Azure" .
Nome de usuário e senha	Estas são as credenciais para a conta de administrador do cluster Cloud Volumes ONTAP . Você pode usar essas credenciais para se conectar ao Cloud Volumes ONTAP por meio do ONTAP System Manager ou do ONTAP CLI. Mantenha o nome de usuário padrão *admin* ou altere-o para um nome de usuário personalizado.
Editar credenciais	Você pode escolher diferentes credenciais do Azure e uma assinatura diferente do Azure para usar com este sistema Cloud Volumes ONTAP . Você precisa associar uma assinatura do Azure Marketplace à assinatura do Azure selecionada para implantar um sistema Cloud Volumes ONTAP pago conforme o uso. "Aprenda como adicionar credenciais" .

5. **Serviços**: habilite ou desabilite os serviços individuais com base na sua vontade de usá-los com o Cloud Volumes ONTAP.
   - "Saiba mais sobre a NetApp Data Classification"
   - "Saiba mais sobre o NetApp Backup and Recovery"

   Se você quiser utilizar WORM e camadas de dados, desabilite o Backup e Recuperação e implante um sistema Cloud Volumes ONTAP com versão 9.8 ou superior.

6. **Modelos de implantação de HA**:
   a. Selecione **Zona de disponibilidade única** ou **Zona de disponibilidade múltipla**.
      - Para zonas de disponibilidade únicas, selecione uma região do Azure, uma zona de disponibilidade, uma VNet e uma sub-rede.

        A partir do Cloud Volumes ONTAP 9.15.1, você pode implantar instâncias de máquina virtual (VM) no modo HA em zonas de disponibilidade únicas (AZs) no Azure. Você precisa selecionar uma zona e uma região que suportem esta implantação. Se a zona ou região não suportar implantação zonal, o modo de implantação não zonal anterior para LRS será seguido. Para entender as configurações suportadas para discos gerenciados compartilhados, consulte"Configuração de zona de disponibilidade única de HA com discos gerenciados compartilhados" .

      - Para várias zonas de disponibilidade, selecione uma região, VNet, sub-rede, zona para o nó 1 e zona para o nó 2.

   b. Marque a caixa de seleção **Verifiquei a conectividade de rede…**.
7. **Conectividade**: Escolha um grupo de recursos novo ou existente e, em seguida, escolha se deseja usar o grupo de segurança predefinido ou usar o seu próprio.

A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Grupo de Recursos	Crie um novo grupo de recursos para o Cloud Volumes ONTAP ou use um grupo de recursos existente. A prática recomendada é usar um novo grupo de recursos dedicado para o Cloud Volumes ONTAP. Embora seja possível implantar o Cloud Volumes ONTAP em um grupo de recursos compartilhados existente, isso não é recomendado devido ao risco de perda de dados. Veja o aviso acima para mais detalhes. Você deve usar um grupo de recursos dedicado para cada par de Cloud Volumes ONTAP HA implantado no Azure. Somente um par de HA é suportado em um grupo de recursos. O Console terá problemas de conexão se você tentar implantar um segundo par de Cloud Volumes ONTAP HA em um grupo de recursos do Azure. Se a conta do Azure que você está usando tiver o "permissões necessárias" , o Console remove os recursos do Cloud Volumes ONTAP de um grupo de recursos, em caso de falha de implantação ou exclusão.
Grupo de segurança gerado	Se você deixar o Console gerar o grupo de segurança para você, precisará escolher como permitirá o tráfego: • Se você escolher **Somente VNet selecionada**, a origem do tráfego de entrada será o intervalo de sub-redes da VNet selecionada e o intervalo de sub-redes da VNet onde o agente do Console reside. Esta é a opção recomendada. • Se você escolher **Todas as VNets**, a origem do tráfego de entrada será o intervalo de IP 0.0.0.0/0.
Use existente	Se você escolher um grupo de segurança existente, ele deverá atender aos requisitos do Cloud Volumes ONTAP . "Exibir o grupo de segurança padrão" .

8. **Métodos de cobrança e conta NSS**: especifique qual opção de cobrança você gostaria de usar com este sistema e, em seguida, especifique uma conta do site de suporte da NetApp .
   - "Saiba mais sobre as opções de licenciamento do Cloud Volumes ONTAP" .
   - "Aprenda como configurar o licenciamento" .
9. **Pacotes pré-configurados**: selecione um dos pacotes para implantar rapidamente um sistema Cloud Volumes ONTAP ou clique em **Alterar configuração**.

   Se você escolher um dos pacotes, precisará apenas especificar um volume e depois revisar e aprovar a configuração.
10. **Licenciamento**: Altere a versão do Cloud Volumes ONTAP conforme necessário e selecione um tipo de máquina virtual.

Se uma versão mais recente de Release Candidate, Disponibilidade Geral ou patch estiver disponível para a versão selecionada, o Console atualizará o sistema para essa versão ao criá-la. Por exemplo, a atualização ocorre se você selecionar Cloud Volumes ONTAP 9.13.1 e 9.13.1 P4 estiver disponível. A atualização não ocorre de uma versão para outra — por exemplo, da 9.13 para a 9.14.

11. **Inscreva-se no Azure Marketplace**: siga as etapas se o Console não conseguir habilitar implantações programáticas do Cloud Volumes ONTAP.
12. **Recursos de armazenamento subjacentes**: escolha as configurações para o agregado inicial: um tipo de disco, um tamanho para cada disco e se a hierarquização de dados para armazenamento de Blobs deve ser habilitada.

    Observe o seguinte:

    - O tamanho do disco é para todos os discos no agregado inicial e para quaisquer agregados adicionais que o Console cria quando você usa a opção de provisionamento simples. Você pode criar agregados que usam um tamanho de disco diferente usando a opção de alocação avançada.

      Para obter ajuda na escolha do tamanho do disco, consulte"Dimensione seu sistema no Azure" .

    - Se o acesso público à sua conta de armazenamento estiver desabilitado na VNet, você não poderá habilitar a hierarquização de dados no seu sistema Cloud Volumes ONTAP . Para obter informações, consulte"Regras do grupo de segurança" .
    - Você pode escolher uma política específica de níveis de volume ao criar ou editar um volume.
    - Se você desabilitar a hierarquização de dados, poderá habilitá-la em agregações subsequentes.

      "Saiba mais sobre camadas de dados" .

    - A partir do Cloud Volumes ONTAP 9.15.0P1, os blobs de páginas do Azure não têm mais suporte para novas implantações de pares de alta disponibilidade. Se você atualmente usa blobs de páginas do Azure em implantações de pares de alta disponibilidade existentes, pode migrar para tipos de instância de VM mais recentes nas VMs das séries Edsv4 e Edsv5.

      "Saiba mais sobre as configurações com suporte no Azure" .

13. **Velocidade de gravação e WORM**:

    a. Escolha a velocidade de gravação **Normal** ou **Alta**, se desejar.

       "Saiba mais sobre velocidade de gravação" .

    b. Ative o armazenamento WORM (escreva uma vez e leia muitas vezes), se desejar.

       Esta opção está disponível apenas para determinados tipos de VM. Para descobrir quais tipos de VM são suportados, consulte"Configurações suportadas por licença para pares HA" .

       O WORM não pode ser habilitado se a hierarquização de dados estiver habilitada para as versões 9.7 e anteriores do Cloud Volumes ONTAP . A reversão ou o downgrade para o Cloud Volumes ONTAP 9.8 é bloqueado após a ativação do WORM e da hierarquização.

    "Saiba mais sobre o armazenamento WORM" .

    a. Se você ativar o armazenamento WORM, selecione o período de retenção.

14. **Comunicação segura com armazenamento e WORM**: escolha se deseja habilitar uma conexão HTTPS com contas de armazenamento do Azure e ative o armazenamento WORM (gravação única e leitura múltipla), se desejar.

    A conexão HTTPS é de um par de HA do Cloud Volumes ONTAP 9.7 para contas de armazenamento de blobs de páginas do Azure. Observe que habilitar esta opção pode afetar o desempenho da gravação. Você não pode alterar a configuração depois de criar o sistema.

    "Saiba mais sobre o armazenamento WORM" .

    O WORM não pode ser habilitado se a hierarquização de dados estiver habilitada.

    "Saiba mais sobre o armazenamento WORM" .

15. **Criar volume**: insira detalhes para o novo volume ou clique em **Ignorar**.

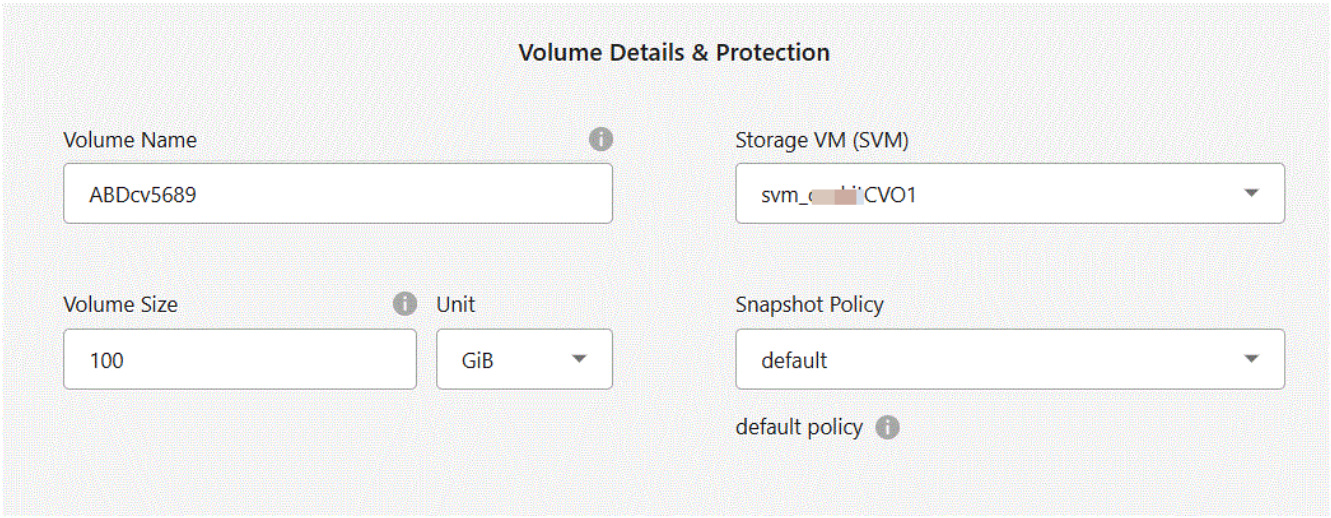
    "Saiba mais sobre os protocolos e versões de clientes suportados" .

    Alguns campos nesta página são autoexplicativos. A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Tamanho	O tamanho máximo que você pode inserir depende muito se você habilita o provisionamento fino, que permite criar um volume maior que o armazenamento físico disponível atualmente.
Controle de acesso (somente para NFS)	Uma política de exportação define os clientes na sub-rede que podem acessar o volume. Por padrão, o Console insere um valor que fornece acesso a todas as instâncias na sub-rede.
Permissões e usuários/grupos (somente para CIFS)	Esses campos permitem que você controle o nível de acesso a um compartilhamento para usuários e grupos (também chamados de listas de controle de acesso ou ACLs). Você pode especificar usuários ou grupos locais ou de domínio do Windows, ou usuários ou grupos do UNIX. Se você especificar um nome de usuário de domínio do Windows, deverá incluir o domínio do usuário usando o formato domínio\nome de usuário.
Política de Snapshot	Uma política de cópia de instantâneo especifica a frequência e o número de cópias de instantâneo do NetApp criadas automaticamente. Uma cópia do NetApp Snapshot é uma imagem do sistema de arquivos de um momento específico que não tem impacto no desempenho e requer armazenamento mínimo. Você pode escolher a política padrão ou nenhuma. Você pode escolher nenhum para dados transitórios: por exemplo, tempdb para Microsoft SQL Server.
Opções avançadas (somente para NFS)	Selecione uma versão do NFS para o volume: NFSv3 ou NFSv4.

Campo	Descrição
Grupo iniciador e IQN (somente para iSCSI)	Os destinos de armazenamento iSCSI são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Os grupos de iniciadores são tabelas de nomes de nós de host iSCSI e controlam quais iniciadores têm acesso a quais LUNs. Os destinos iSCSI se conectam à rede por meio de adaptadores de rede Ethernet padrão (NICs), placas de mecanismo de descarregamento TCP (TOE) com iniciadores de software, adaptadores de rede convergentes (CNAs) ou adaptadores de bust de host dedicados (HBAs) e são identificados por nomes qualificados iSCSI (IQNs). Quando você cria um volume iSCSI, o Console cria automaticamente um LUN para você. Simplificamos criando apenas um LUN por volume, portanto não há gerenciamento envolvido. Depois de criar o volume,"use o IQN para conectar-se ao LUN de seus hosts" .

A imagem a seguir mostra a primeira página do assistente de criação de volume:



16. **Configuração CIFS**: Se você escolher o protocolo CIFS, configure um servidor CIFS.

Campo	Descrição
Endereço IP primário e secundário do DNS	Os endereços IP dos servidores DNS que fornecem resolução de nomes para o servidor CIFS. Os servidores DNS listados devem conter os registros de localização de serviço (SRV) necessários para localizar os servidores LDAP do Active Directory e os controladores de domínio para o domínio ao qual o servidor CIFS se juntará.
Domínio do Active Directory para ingressar	O FQDN do domínio do Active Directory (AD) ao qual você deseja que o servidor CIFS ingresse.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com privilégios suficientes para adicionar computadores à Unidade Organizacional (UO) especificada dentro do domínio do AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio do AD.

Campo	Descrição
Unidade Organizacional	A unidade organizacional dentro do domínio do AD a ser associada ao servidor CIFS. O padrão é CN=Computadores. Para configurar o Azure AD Domain Services como o servidor AD para o Cloud Volumes ONTAP, você deve inserir **OU=AADDC Computers** ou **OU=AADDC Users** neste campo.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentação do Azure: Criar uma Unidade Organizacional (UO) em um domínio gerenciado do Azure AD Domain Services"^]
Domínio DNS	O domínio DNS para a máquina virtual de armazenamento (SVM) do Cloud Volumes ONTAP . Na maioria dos casos, o domínio é o mesmo que o domínio do AD.
Servidor NTP	Selecione **Usar domínio do Active Directory** para configurar um servidor NTP usando o DNS do Active Directory. Se você precisar configurar um servidor NTP usando um endereço diferente, use a API. Consulte o "Documentação de automação do NetApp Console" para mais detalhes. Observe que você só pode configurar um servidor NTP ao criar um servidor CIFS. Não é configurável depois de criar o servidor CIFS.

17. **Perfil de uso, tipo de disco e política de camadas**: escolha se deseja habilitar recursos de eficiência de armazenamento e alterar a política de camadas de volume, se necessário.

    Para mais informações, consulte"Escolha um perfil de uso de volume" ,"Visão geral da hierarquização de dados" , e "KB: Quais recursos de eficiência de armazenamento em linha são suportados pelo CVO?"

18. **Revisar e aprovar**: revise e confirme suas seleções.
    a. Revise os detalhes sobre a configuração.
    b. Clique em **Mais informações** para revisar detalhes sobre o suporte e os recursos do Azure que o Console comprará.
    c. Selecione as caixas de seleção **Eu entendo…**.
    d. Clique em **Ir**.

Resultado

O Console implanta o sistema Cloud Volumes ONTAP . Você pode acompanhar o progresso na página Auditoria.

Se você tiver algum problema ao implantar o sistema Cloud Volumes ONTAP , revise a mensagem de falha. Você também pode selecionar o sistema e clicar em **Recriar ambiente**.

Para obter ajuda adicional, acesse "Suporte NetApp Cloud Volumes ONTAP" .

Depois que você terminar

- Se você provisionou um compartilhamento CIFS, conceda aos usuários ou grupos permissões para os arquivos e pastas e verifique se esses usuários podem acessar o compartilhamento e criar um arquivo.
- Se você quiser aplicar cotas aos volumes, use o ONTAP System Manager ou o ONTAP CLI.

  As cotas permitem que você restrinja ou rastreie o espaço em disco e o número de arquivos usados por um usuário, grupo ou qtree.

Após a conclusão do processo de implantação, não modifique as configurações do Cloud Volumes ONTAP geradas pelo sistema no portal do Azure, especialmente as tags do sistema. Quaisquer alterações feitas nessas configurações podem levar a comportamento inesperado ou perda de dados.

Links relacionados

*"Planejando sua configuração do Cloud Volumes ONTAP no Azure" *"Implantar o Cloud Volumes ONTAP no Azure a partir do Azure Marketplace"

Verificar imagem da plataforma Azure

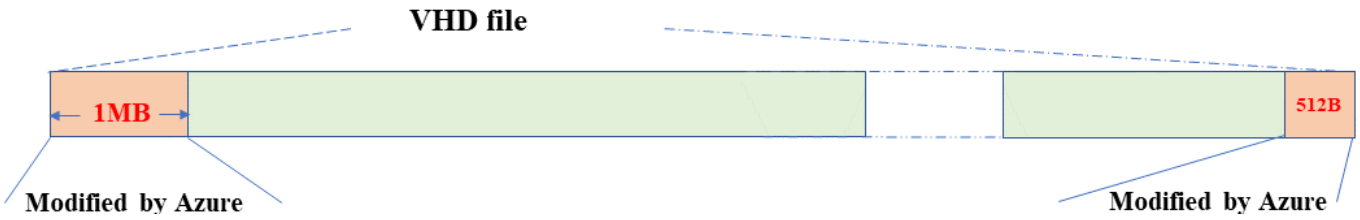
Verificação de imagem do Azure Marketplace para Cloud Volumes ONTAP

A verificação de imagem do Azure está em conformidade com os requisitos de segurança aprimorados da NetApp . Verificar um arquivo de imagem é um processo simples. No entanto, a verificação da assinatura da imagem do Azure requer considerações específicas para o arquivo de imagem VHD do Azure porque ele é alterado no marketplace do Azure.

A verificação de imagem do Azure é compatível com o Cloud Volumes ONTAP 9.15.0 e posteriores.

Alteração de arquivos VHD publicados pelo Azure

O 1 MB (1048576 bytes) no início e 512 bytes no final do arquivo VHD são modificados pelo Azure. O NetApp assina o arquivo VHD restante.



No exemplo, o arquivo VHD tem 10 GB. A parte que a NetApp assinou está marcada em verde (10 GB - 1 MB - 512 bytes).

Links relacionados

- "Blog de falhas de página: como assinar e verificar usando OpenSSL"
- "Use a imagem do Azure Marketplace para criar uma imagem de VM para sua GPU Azure Stack Edge Pro | Microsoft Learn"
- "Exportar/Copiar um disco gerenciado para uma conta de armazenamento usando a CLI do Azure | Microsoft Learn"
- "Início rápido do Azure Cloud Shell - Bash | Microsoft Learn"
- "Como instalar o Azure CLI | Microsoft Learn"
- "cópia do blob de armazenamento az | Microsoft Learn"
- "Sign in com a CLI do Azure — Login e Autenticação | Microsoft Learn"

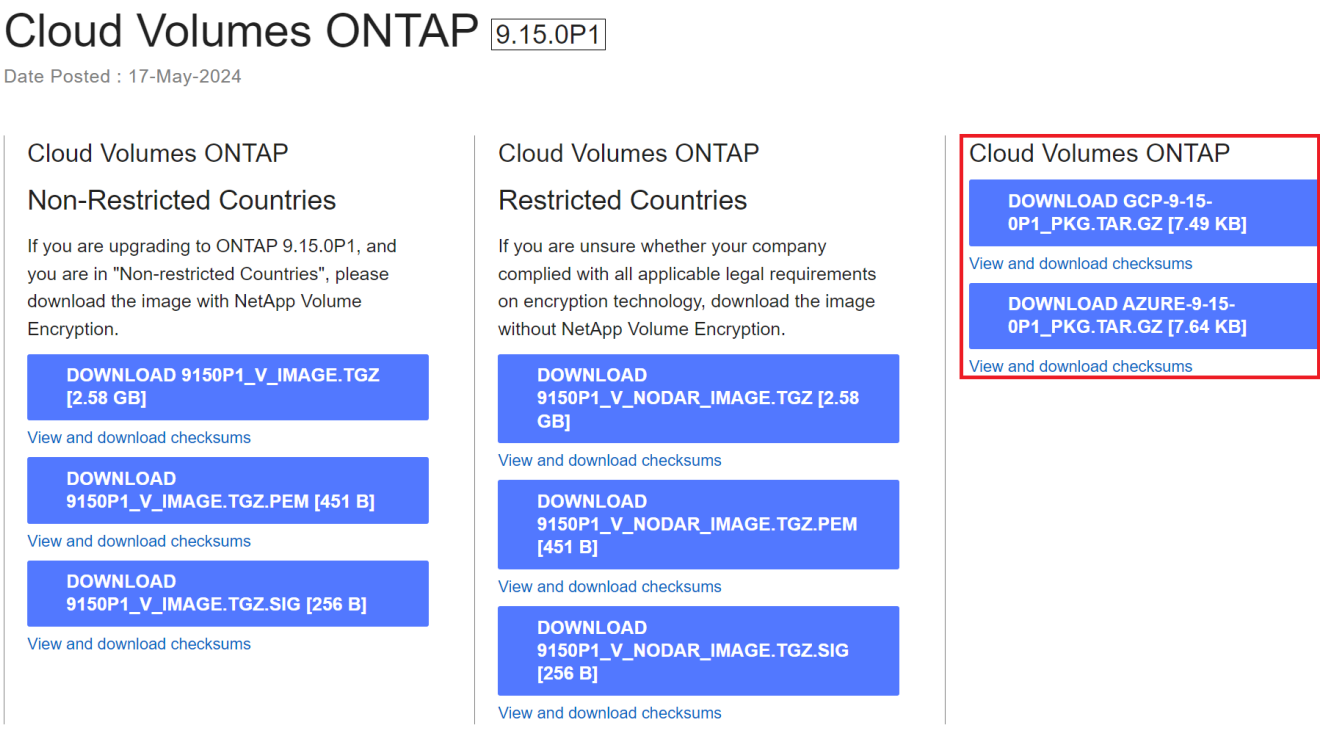
Baixe o arquivo de imagem do Azure para o Cloud Volumes ONTAP

Você pode baixar o arquivo de imagem do Azure em "Site de suporte da NetApp" .

O arquivo *tar.gz* contém os arquivos necessários para verificação da assinatura da imagem. Junto com o arquivo *tar.gz*, você também deve baixar o arquivo *checksum* da imagem. O arquivo de soma de verificação contém o `md5` e `sha256` somas de verificação do arquivo *tar.gz*.

Passos

1. Vá para o "Página do produto Cloud Volumes ONTAP no site de suporte da NetApp" e baixe a versão do software necessária na seção **Downloads**.
2. Na página de download do Cloud Volumes ONTAP , clique no arquivo para download da imagem do Azure e baixe o arquivo *tar.gz*.



3. No Linux, execute `md5sum AZURE-<version>_PKG.TAR.GZ` .

   No macOS, execute `sha256sum AZURE-<version>_PKG.TAR.GZ` .

4. Verifique se o `md5sum` e `sha256sum` os valores correspondem aos da imagem do Azure baixada.
5. No Linux e macOS, extraia o arquivo *tar.gz* usando o `tar -xzf` comando.

   O arquivo *tar.gz* extraído contém o arquivo de resumo (*.sig*), o arquivo de certificado de chave pública (*.pem*) e o arquivo de certificado de cadeia (*.pem*).

   Exemplo de saída após extrair o arquivo tar.gz:

```
$ ls cert/ -l
-rw-r----- 1 netapp netapp  384 May  13 13:00 9.15.0P1_azure_digest.sig
-rw-r----- 1 netapp netapp 2365 May  13 13:00 Certificate-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 Certificate-Chain-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 version_readme
```

Exportar imagens VHD para o Cloud Volumes ONTAP do marketplace do Azure

Depois que a imagem VHD é publicada na nuvem do Azure, ela não é mais gerenciada pelo NetApp. Em vez disso, a imagem publicada é colocada no marketplace do Azure. Quando a imagem é preparada e publicada no marketplace do Azure, o Azure modifica 1 MB no início e 512 bytes no final do VHD. Para verificar a assinatura do arquivo VHD, você precisa exportar a imagem VHD modificada pelo Azure do marketplace do Azure.

Antes de começar

Certifique-se de que a CLI do Azure esteja instalada no seu sistema ou que o Azure Cloud Shell esteja disponível no portal do Azure. Para obter mais informações sobre como instalar o Azure CLI, consulte o "Documentação da Microsoft: Como instalar o Azure CLI" .

Passos

1. Mapeie a versão do Cloud Volumes ONTAP no seu sistema para a versão da imagem do Azure Marketplace usando o conteúdo do arquivo *version_readme*. A versão Cloud Volumes ONTAP é representada por `buildname` e a versão da imagem do marketplace do Azure é representada por `version` nos mapeamentos de versão.

   No exemplo a seguir, a versão do Cloud Volumes ONTAP `9.15.0P1` é mapeado para a versão da imagem do Azure Marketplace `9150.01000024.05090105` . Esta versão da imagem do Azure Marketplace é usada posteriormente para definir o URN da imagem.

   ```
   [
    "buildname": "9.15.0P1",
       "publisher": "netapp",
        "version": "9150.01000024.05090105"

   ]
   ```

2. Identifique a região onde você deseja criar as VMs. O nome da região é usado como valor para o `locName` variável ao definir a URN da imagem do marketplace. Para listar as regiões disponíveis, execute este comando:

   ```
   az account list-locations -o table
   ```

   Nesta tabela, o nome da região aparece no `Name` campo.

```
$ az account list-locations -o table
DisplayName               Name                 RegionalDisplayName
------------------------  -------------------
-----------------------------------
East US                   eastus               (US) East US
East US 2                 eastus2              (US) East US 2
South Central US          southcentralus       (US) South Central US
...
```

3. Revise os nomes de SKU para as versões correspondentes do Cloud Volumes ONTAP e os tipos de implantação de VM na tabela abaixo. O nome do SKU é usado como valor para o `skuName` variável ao definir o URN da imagem do marketplace.

   Por exemplo, todas as implantações de nó único com Cloud Volumes ONTAP 9.15.0 devem usar `ontap_cloud_byol` como o nome do SKU.

* Versão Cloud Volumes ONTAP *	**Implantação de VM por meio de**	**Nome do SKU**
9.17.1 e posterior	O mercado do Azure	ontap_cloud_direct_gen2
9.17.1 e posterior	O NetApp Console	ontap_cloud_gen2
9.16.1	O mercado do Azure	ontap_cloud_direct
9.16.1	O Console	ontap_cloud
9.15.1	O Console	ontap_cloud
9.15.0	O Console, implantações de nó único	ontap_cloud_byol
9.15.0	O Console, implantações de alta disponibilidade (HA)	ontap_cloud_byol_ha

4. Após mapear a versão do ONTAP e a imagem do Azure Marketplace, exporte o arquivo VHD do Azure Marketplace usando o Azure Cloud Shell ou o Azure CLI.

Exportar arquivo VHD usando o Azure Cloud Shell no Linux

No Azure Cloud Shell, exporte a imagem do marketplace para o arquivo VHD (por exemplo, *9150.01000024.05090105.vhd*) e baixe-a para o seu sistema Linux local. Execute estas etapas para obter a imagem VHD do marketplace do Azure.

Passos

1. Defina o URN e outros parâmetros da imagem do marketplace. O formato URN é `<publisher>:<offer>:<sku>:<version>` . Opcionalmente, você pode listar imagens do NetApp Marketplace para confirmar a versão correta da imagem.

```
PS /home/user1> $urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
PS /home/user1> $locName="eastus2"
PS /home/user1> $pubName="netapp"
PS /home/user1> $offerName="netapp-ontap-cloud"
PS /home/user1> $skuName="ontap_cloud_byol"
PS /home/user1> Get-AzVMImage -Location $locName -PublisherName $pubName
-Offer $offerName -Sku $skuName |select version
...
141.20231128
9.141.20240131
9.150.20240213
9150.01000024.05090105
...
```

2. Crie um novo disco gerenciado a partir da imagem do marketplace com a versão da imagem correspondente:

```
PS /home/user1> $diskName = “9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = “fnf1”
PS /home/user1> az disk create -g $diskRG -n $diskName --image-reference
$urn
PS /home/user1> $sas = az disk grant-access --duration-in-seconds 3600
--access-level Read --name $diskName --resource-group $diskRG
PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-Json)[0].accessSas
```

3. Exporte o arquivo VHD do disco gerenciado para o Armazenamento do Azure. Crie um contêiner com o nível de acesso apropriado. Neste exemplo, usamos um contêiner chamado `vm-images` com `Container` nível de acesso. Obtenha a chave de acesso da conta de armazenamento no portal do Azure: **Contas de armazenamento > *examplesaname* > Chave de acesso > *key1* > *key* > Mostrar > <*cópia*>**

```
PS /home/user1> $storageAccountName = “examplesaname”
PS /home/user1> $containerName = “vm-images”
PS /home/user1> $storageAccountKey = "<replace with the above access
key>"
PS /home/user1> $destBlobName = “9150.01000024.05090105.vhd”
PS /home/user1> $destContext = New-AzureStorageContext
-StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri $diskAccessSAS
-DestContainer $containerName -DestContext $destContext -DestBlob
$destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState –Container $containerName
–Context $destContext -Blob $destBlobName
```

4. Baixe a imagem gerada para o seu sistema Linux. Use o `wget` comando para baixar o arquivo VHD:

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

O URL segue um formato padrão. Para automação, você pode derivar a sequência de URL conforme mostrado abaixo. Como alternativa, você pode usar o Azure CLI `az` comando para obter a URL. URL de exemplo:https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

5. Limpe o disco gerenciado

```
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName
$diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

Exportar arquivo VHD usando a CLI do Azure no Linux

Exporte a imagem do marketplace para um arquivo VHD usando a CLI do Azure de um sistema Linux local.

Passos

1. Efetue login na CLI do Azure e liste as imagens do marketplace:

```
% az login --use-device-code
```

2. Para fazer login, use um navegador da web para abrir a página https://microsoft.com/devicelogin e digite o código de autenticação.

```
% az vm image list --all --publisher netapp --offer netapp-ontap-cloud
--sku ontap_cloud_byol
...
{
"architecture": "x64",
"offer": "netapp-ontap-cloud",
"publisher": "netapp",
"sku": "ontap_cloud_byol",
"urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
"version": "9150.01000024.05090105"
},
...
```

3. Crie um novo disco gerenciado a partir da imagem do marketplace com a versão da imagem correspondente.

```
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level Read
--name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
```

Para automatizar o processo, o SAS precisa ser extraído da saída padrão. Consulte os documentos apropriados para obter orientação.

4. Exporte o arquivo VHD do disco gerenciado.

   a. Crie um contêiner com o nível de acesso apropriado. Neste exemplo, um contêiner chamado `vm-images` com `Container` nível de acesso é usado.

   b. Obtenha a chave de acesso da conta de armazenamento no portal do Azure: **Contas de armazenamento > *examplesaname* > Chave de acesso > *key1* > *key* > Mostrar > <*cópia*>**

      Você também pode usar o `az` comando para esta etapa.

```
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS --destination
-container $containerName --account-name $storageAccountName --account
-key $storageAccountKey --destination-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

5. Verifique o status da cópia do blob.

```
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
    "copy": {
      "completionTime": null,
      "destinationSnapshot": null,
      "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxx",
      "incrementalCopy": null,
      "progress": "10737418752/10737418752",
      "source": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
    },
....
```

6. Baixe a imagem gerada para o seu servidor Linux.

```
wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>
```

O URL segue um formato padrão. Para automação, você pode derivar a sequência de URL conforme mostrado abaixo. Como alternativa, você pode usar o Azure CLI `az` comando para obter a URL. URL de exemplo:https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

7. Limpe o disco gerenciado

```
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

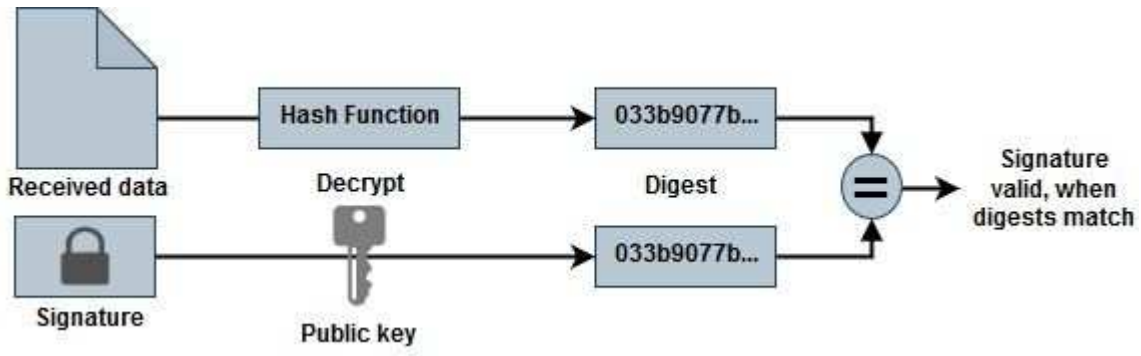
Verificar assinatura do arquivo

Verificação de assinatura de imagem do Azure Marketplace para Cloud Volumes ONTAP

O processo de verificação de imagem do Azure gera um arquivo de resumo a partir do arquivo VHD, retirando 1 MB no início e 512 bytes no final e, em seguida, aplicando uma função de hash. Para corresponder ao procedimento de assinatura, *sha256* é usado para hash.

Resumo do fluxo de trabalho de verificação de assinatura de arquivo

A seguir, uma visão geral do processo de fluxo de trabalho de verificação de assinatura de arquivo.



- Baixando a imagem do Azure do "Site de suporte da NetApp" e extrair o arquivo digest (.sig), o arquivo de certificado de chave pública (.pem) e o arquivo de certificado de cadeia (.pem). Consulte "Baixe o arquivo de resumo da imagem do Azure" para maiores informações.
- Verificação da cadeia de confiança.
- Extraindo a chave pública (.pub) do certificado de chave pública (.pem).
- Descriptografando o arquivo de resumo usando a chave pública extraída.
- Comparando o resultado com um resumo recém-gerado de um arquivo temporário criado a partir do arquivo de imagem após remover 1 MB no início e 512 bytes no final. Esta etapa é realizada usando a ferramenta de linha de comando OpenSSL. A ferramenta OpenSSL CLI exibe mensagens apropriadas sobre sucesso ou falha na correspondência dos arquivos.

```
openssl dgst -verify <public_key> -keyform <form> <hash_function>
-signature <digest_file> -binary <temporary_file>
```

Verificar assinatura de imagem do Azure Marketplace para Cloud Volumes ONTAP no Linux

A verificação da assinatura de um arquivo VHD exportado no Linux inclui a validação da cadeia de confiança, a edição do arquivo e a verificação da assinatura.

Passos

1. Baixe o arquivo de imagem do Azure em "Site de suporte da NetApp" e extraia o arquivo digest (.sig), o arquivo de certificado de chave pública (.pem) e o arquivo de certificado de cadeia (.pem).

   Consulte "Baixe o arquivo de resumo da imagem do Azure" para maiores informações.

2. Verifique a cadeia de confiança.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. Remova 1 MB (1.048.576 bytes) no início e 512 bytes no final do arquivo VHD. Ao usar `tail` , o `-c +K` opção gera bytes a partir do K-ésimo byte do arquivo. Portanto, ele passa 1048577 para `tail -c` .

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. Use o OpenSSL para extrair a chave pública do certificado e verificar o arquivo removido (sign.tmp) com o arquivo de assinatura e a chave pública.

   O prompt de comando exibe mensagens indicando sucesso ou falha com base na verificação.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verification OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. Limpe o espaço de trabalho.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Verificar assinatura de imagem do Azure Marketplace para Cloud Volumes ONTAP no macOS

A verificação da assinatura de um arquivo VHD exportado no Linux inclui a validação da cadeia de confiança, a edição do arquivo e a verificação da assinatura.

Passos

1. Baixe o arquivo de imagem do Azure em "Site de suporte da NetApp" e extraia o arquivo digest (.sig), o arquivo de certificado de chave pública (.pem) e o arquivo de certificado de cadeia (.pem).

   Consulte "Baixe o arquivo de resumo da imagem do Azure" para maiores informações.

2. Verifique a cadeia de confiança.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. Remova 1 MB (1.048.576 bytes) no início e 512 bytes no final do arquivo VHD. Ao usar `tail` , o `-c +K` opção gera bytes a partir do K-ésimo byte do arquivo. Portanto, ele passa 1048577 para `tail -c` . Observe que no macOS, o comando tail pode levar cerca de dez minutos para ser concluído.

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. Use o OpenSSL para extrair a chave pública do certificado e verificar o arquivo removido (sign.tmp) com o arquivo de assinatura e a chave pública. O prompt de comando exibe mensagens indicando sucesso ou falha com base na verificação.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. Limpe o espaço de trabalho.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Implantar o Cloud Volumes ONTAP no marketplace do Azure

Você pode usar a implantação direta do Azure Marketplace para implantar o Cloud Volumes ONTAP de forma rápida e fácil. No marketplace do Azure, você pode implantar rapidamente o Cloud Volumes ONTAP em apenas alguns cliques e explorar seus principais recursos e funcionalidades em seu ambiente.

Para mais informações sobre esta oferta, consulte"Saiba mais sobre as ofertas do Cloud Volumes ONTAP no NetApp Console e no marketplace" .

Sobre esta tarefa

O sistema Cloud Volumes ONTAP implantado usando a implantação direta do Azure Marketplace tem essas propriedades. Observe que os recursos de uma instância autônoma implantada por meio do marketplace do Azure mudam quando ela é descoberta no NetApp Console.

- A versão mais recente do Cloud Volumes ONTAP (9.16.1 ou posterior).
- Uma licença gratuita para o Cloud Volumes ONTAP limitada a 500 GiB de capacidade provisionada. Esta licença não inclui suporte NetApp e não tem data de expiração.
- Dois nós configurados em modo de alta disponibilidade (HA) em uma única zona de disponibilidade (AZ), provisionados com números de série padrão. As máquinas virtuais de armazenamento (VMs de armazenamento) são implantadas em um"modo de orquestração flexível" .
- Um agregado para a instância criada por padrão.
- Um disco gerenciado SSD v2 Premium com capacidade provisionada de 500 GiB, além de um disco raiz e um disco de dados.
- Uma VM de armazenamento de dados implantada, com serviços de dados NFS, CIFS, iSCSI e NVMe/TCP. Não é possível adicionar nenhuma VM de armazenamento de dados adicional.
- Licenças instaladas para NFS, CIFS (SMB), iSCSI, Autonomous Ransomware Protection (ARP), SnapLock e SnapMirror.
- "Eficiência de armazenamento sensível à temperatura (TSSE) ONTAP", criptografia de volume e gerenciamento de chaves externas habilitados por padrão.
- Os seguintes recursos não são suportados:
  - Hierarquização do FabricPool
  - Alterando o tipo de VM de armazenamento
  - Modo de gravação rápida

Antes de começar

- Certifique-se de ter uma assinatura válida do Azure Marketplace.
- Certifique-se de atender aos requisitos de rede para um"Implantação de HA em uma única AZ" no Azure. Consulte "Configurar a rede do Azure para o Cloud Volumes ONTAP" .

- Você precisa ter uma destas funções do Azure atribuídas para implantar o Cloud Volumes ONTAP:
  - O `contributor` função com as permissões padrão. Para mais informações, consulte o "Documentação do Microsoft Azure: funções integradas do Azure" .
  - Uma função RBAC personalizada com as seguintes permissões. Para mais informações, consulte o "Documentação do Azure: Funções personalizadas do Azure" .

```
"permissões": [ { "ações": [ "Microsoft.AAD/register/action",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Network/loadBalancers/write", "Microsoft.ClassicCompute/virtualMachines/write",
"Microsoft.Compute/capacityReservationGroups/deploy/action",
"Microsoft.ClassicCompute/virtualMachines/networkInterfaces/associatedNetworkSecurityGroups/
write", "Microsoft.Network/networkInterfaces/write", "Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Network/virtualNetworks/write", "Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/read", "Microsoft.Compute/disks/write",
"Microsoft.Compute/virtualMachineScaleSets/write", "Microsoft.Resources/deployments/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/subnets/write" ], "notActions": [], "dataActions": [],
"notDataActions": [] } ]
```

> Se você registrou o provedor de recursos "Microsoft.storage" em sua assinatura, não precisará do `Microsoft.AAD/register/action` permissão. Para mais informações, consulte o "Documentação do Azure: Permissões do Azure para Armazenamento" .

Passos

1. No site do marketplace do Azure, pesquise por produtos NetApp .
2. Selecione * NetApp Cloud Volumes ONTAP direct*.
3. Clique em **Criar** para iniciar o assistente de implantação.
4. Selecione um plano. A lista **Plano** normalmente exibe as versões mais recentes do Cloud Volumes ONTAP.
5. Na aba **Básico**, forneça estes detalhes:
   - **Assinatura**: Selecione uma assinatura. A implantação será vinculada ao número de assinatura.
   - **Grupo de recursos**: use um grupo de recursos existente ou crie um novo. Os grupos de recursos ajudam a alocar todos os recursos, como discos e VMs de armazenamento, dentro de um único grupo para um sistema Cloud Volumes ONTAP .
   - **Região**: selecione uma região que ofereça suporte à implantação de HA do Azure em uma única AZ. Você vê apenas as regiões disponíveis na lista.
   - **Tamanho**: Selecione um tamanho de VM de armazenamento para o Disco gerenciado Premium SSD v2 compatível.
   - **Zona**: Selecione uma zona para a região selecionada.
   - **Senha do administrador**: Defina uma senha. Use esta senha de administrador para efetuar login no sistema após a implantação.

- **Confirmar senha**: Digite novamente a mesma senha para confirmação.
  - Na aba **Rede**, adicione uma rede virtual e uma sub-rede ou selecione-as nas listas.

    Para cumprir com as restrições do Microsoft Azure, você deve criar uma nova sub-rede ao configurar uma nova rede virtual. Da mesma forma, se você escolher uma rede existente, deverá selecionar uma sub-rede existente.

  - Para selecionar um grupo de segurança de rede predefinido, selecione **Sim**. Selecione **Não** para atribuir um grupo de segurança de rede predefinido do Azure com as regras de tráfego necessárias. Para mais informações, consulte "Regras de grupo de segurança para o Azure" .
  - Na guia **Avançado**, confirme se os dois recursos do Azure necessários para esta implantação foram definidos. Consulte"Habilitar um recurso do Azure para implantações de AZ únicas do Cloud Volumes ONTAP" e"Habilitar o modo de alta disponibilidade para o Cloud Volumes ONTAP no Azure" .
  - Você pode definir pares de nomes e valores para os recursos ou grupos de recursos na guia **Tags**.
  - Na aba **Revisar + criar**, revise os detalhes e inicie a implantação.

Depois que você terminar

Selecione o ícone de notificação para visualizar o progresso da sua implantação. Após a implantação do Cloud Volumes ONTAP , você pode visualizar a VM de armazenamento listada para operações.

Uma vez acessível, use o ONTAP System Manager ou o ONTAP CLI para efetuar login na VM de armazenamento com as credenciais de administrador que você definiu. Depois disso, você pode criar volumes, LUNs ou compartilhamentos e começar a utilizar os recursos de armazenamento do Cloud Volumes ONTAP.

Solucionar problemas de implantação

Os sistemas Cloud Volumes ONTAP implantados diretamente pelo marketplace do Azure não incluem suporte da NetApp. Caso surjam problemas durante a implantação, você pode solucioná-los e resolvê-los de forma independente.

Passos

1. No site do marketplace do Azure, acesse **Diagnóstico de inicialização > Log serial**.
2. Baixe e investigue os logs seriais.
3. Consulte a documentação do produto e os artigos da base de conhecimento (KB) para solução de problemas.
   - "Documentação do marketplace do Azure"
   - "Documentação da NetApp"
   - "Artigos da base de conhecimento da NetApp"

Descubra os sistemas implantados no Console

Você pode descobrir os sistemas Cloud Volumes ONTAP que você implantou usando a implantação direta do Azure Marketplace e gerenciá-los na página **Sistemas** no Console. O agente do Console descobre os sistemas, os adiciona e aplica as licenças necessárias, além de desbloqueia todos os recursos do Console para esses sistemas. A configuração HA original em uma única AZ com discos gerenciados PSSD v2 é mantida, e o sistema é registrado na mesma assinatura do Azure e no mesmo grupo de recursos da implantação original.

Sobre esta tarefa

Ao descobrir os sistemas Cloud Volumes ONTAP implantados usando a implantação direta do Azure Marketplace, o agente do Console executa estas tarefas:

- Substitui as licenças gratuitas dos sistemas descobertos como licenças regulares baseadas em capacidade"Licenças Freemium" .
- Mantém os recursos existentes dos sistemas implantados e adiciona recursos adicionais do Console, como proteção de dados, gerenciamento de dados e recursos de segurança.
- Substitui as licenças instaladas nos nós por novas licenças ONTAP para NFS, CIFS (SMB), iSCSI, ARP, SnapLock e SnapMirror.
- Converte os números de série dos nós genéricos em números de série exclusivos.
- Atribui novas tags de sistema aos recursos, conforme necessário.
- Converte os endereços IP dinâmicos da instância em endereços IP estáticos.
- Habilita as funcionalidades de"Hierarquização do FabricPool" ,"AutoSupport" , e"escrever uma vez e ler muitas vezes" (WORM) armazenamento nos sistemas implantados. Você pode ativar esses recursos no Console quando precisar deles.
- Registra as instâncias nas contas NSS usadas para descobri-las.
- Habilita recursos de gerenciamento de capacidade em"modos automático e manual" para os sistemas descobertos.

Antes de começar

Certifique-se de que a implantação esteja concluída no marketplace do Azure. O agente do Console pode descobrir os sistemas somente quando a implantação estiver concluída e eles estiverem disponíveis para descoberta.

Passos

No Console, você segue o procedimento padrão para descobrir sistemas existentes. Consulte "Adicionar um sistema Cloud Volumes ONTAP existente ao Console" .

> Durante a descoberta, você poderá ver mensagens de falha, mas pode ignorá-las até que o processo de descoberta seja concluído. Não modifique as configurações do Cloud Volumes ONTAP geradas pelo sistema no portal do marketplace do Azure durante a descoberta, especialmente as tags do sistema. Quaisquer alterações feitas nessas configurações podem levar a um comportamento inesperado do sistema.

Depois que você terminar

Após a conclusão da descoberta, você poderá visualizar os sistemas listados na página **Sistemas** no Console. Você pode executar várias tarefas de gerenciamento, como"expandindo o agregado" ,"adicionando volumes" ,"provisionamento de VMs de armazenamento adicionais" , e"alterando os tipos de instância" .

Links relacionados

Consulte a documentação do ONTAP para obter mais informações sobre como criar armazenamento:

- "Criar volumes para NFS"
- "Criar LUNs para iSCSI"
- "Criar compartilhamentos para CIFS"

Comece a usar o Google Cloud

Início rápido para o Cloud Volumes ONTAP no Google Cloud

Comece a usar o Cloud Volumes ONTAP no Google Cloud em poucas etapas.

1 Criar um agente de console

Se você não tiver um "Agente de console" No entanto, você precisa criar um. "Aprenda a criar um agente de console no Google Cloud"

Observe que se você quiser implantar o Cloud Volumes ONTAP em uma sub-rede onde não há acesso à Internet disponível, será necessário instalar manualmente o agente do Console e acessar o NetApp Console que está em execução nesse agente do Console. "Aprenda a instalar manualmente o agente do Console em um local sem acesso à Internet"

2 Planeje sua configuração

O Console oferece pacotes pré-configurados que correspondem aos seus requisitos de carga de trabalho, ou você pode criar sua própria configuração. Se você escolher sua própria configuração, deverá entender as opções disponíveis.

"Saiba mais sobre o planejamento de sua configuração" .

3 Configure sua rede

1. Certifique-se de que sua VPC e sub-redes oferecerão suporte à conectividade entre o agente do Console e o Cloud Volumes ONTAP.
2. Se você planeja habilitar a hierarquização de dados, "configurar a sub-rede Cloud Volumes ONTAP para acesso privado do Google" .
3. Se você estiver implantando um par de HA, certifique-se de ter quatro VPCs, cada uma com sua própria sub-rede.
4. Se você estiver usando uma VPC compartilhada, forneça a função *Usuário da rede de computação* à conta de serviço do agente do console.
5. Habilite o acesso de saída à Internet da VPC de destino para o NetApp AutoSupport.

   Esta etapa não é necessária se você estiver implantando o Cloud Volumes ONTAP em um local onde não há acesso à Internet disponível.

"Saiba mais sobre os requisitos de rede" .

4 Configurar uma conta de serviço

O Cloud Volumes ONTAP requer uma conta de serviço do Google Cloud para duas finalidades. A primeira é quando você habilita"hierarquização de dados" para hierarquizar dados frios para armazenamento de objetos de baixo custo no Google Cloud. A segunda é quando você habilita o "NetApp Backup and Recovery" para fazer backup de volumes em armazenamento de objetos de baixo custo.

Você pode configurar uma conta de serviço e usá-la para ambas as finalidades. A conta de serviço deve ter a função **Administrador de armazenamento**.

"Leia as instruções passo a passo" .

5 Habilitar APIs do Google Cloud

"Habilite as seguintes APIs do Google Cloud no seu projeto" . Essas APIs são necessárias para implantar o agente do Console e o Cloud Volumes ONTAP.

- API do Gerenciador de Implantação em Nuvem V2
- API de registro em nuvem
- API do Gerenciador de Recursos de Nuvem
- API do mecanismo de computação
- API de gerenciamento de identidade e acesso (IAM)

6 Inicie o Cloud Volumes ONTAP usando o Console

Clique em **Adicionar Sistema**, selecione o tipo de sistema que você gostaria de implantar e conclua as etapas do assistente. "Leia as instruções passo a passo" .

Links relacionados

- "Criando um agente de console"
- "Instalando o software do agente do Console em um host Linux"
- "Permissões do Google Cloud para o agente do Console"

Planeje sua configuração do Cloud Volumes ONTAP no Google Cloud

Ao implantar o Cloud Volumes ONTAP no Google Cloud, você pode escolher um sistema pré-configurado que corresponda aos seus requisitos de carga de trabalho ou pode criar sua própria configuração. Se você escolher sua própria configuração, deverá entender as opções disponíveis.

Escolha uma licença do Cloud Volumes ONTAP

Várias opções de licenciamento estão disponíveis para o Cloud Volumes ONTAP. Cada opção permite que você escolha um modelo de consumo que atenda às suas necessidades.

- "Saiba mais sobre as opções de licenciamento do Cloud Volumes ONTAP"
- "Aprenda como configurar o licenciamento"

Escolha uma região com suporte

O Cloud Volumes ONTAP é compatível com a maioria das regiões do Google Cloud. "Veja a lista completa de regiões suportadas" .

Escolha um tipo de máquina compatível

O Cloud Volumes ONTAP oferece suporte a vários tipos de máquinas, dependendo do tipo de licença escolhido.

"Configurações suportadas para Cloud Volumes ONTAP no Google Cloud"

Entenda os limites de armazenamento

O limite de capacidade bruta para um sistema Cloud Volumes ONTAP está vinculado à licença. Limites adicionais afetam o tamanho dos agregados e volumes. Você deve estar ciente desses limites ao planejar sua configuração.

"Limites de armazenamento para Cloud Volumes ONTAP no Google Cloud"

Dimensione seu sistema no Google Cloud

Dimensionar seu sistema Cloud Volumes ONTAP pode ajudar você a atender aos requisitos de desempenho e capacidade. Você deve estar ciente de alguns pontos-chave ao escolher um tipo de máquina, tipo de disco e tamanho de disco:

Tipo de máquina

Veja os tipos de máquinas suportados em "Notas de versão do Cloud Volumes ONTAP" Em seguida, consulte os detalhes do Google sobre cada tipo de máquina compatível. Adapte seus requisitos de carga de trabalho ao número de vCPUs e memória para o tipo de máquina. Observe que cada núcleo da CPU aumenta o desempenho da rede.

Consulte o seguinte para mais detalhes:

- "Documentação do Google Cloud: tipos de máquinas padrão N1"
- "Documentação do Google Cloud: Desempenho"

Tipos de disco

Ao criar volumes para o Cloud Volumes ONTAP, você precisa escolher o armazenamento em nuvem subjacente que o Cloud Volumes ONTAP usa para um disco. O tipo de disco pode ser qualquer um dos seguintes:

- *Discos persistentes SSD zonais*: discos persistentes SSD são melhores para cargas de trabalho que exigem altas taxas de IOPS aleatórios.
- *Discos persistentes zonais balanceados*: Esses SSDs equilibram desempenho e custo ao fornecer IOPS mais baixos por GB.
- *Discos persistentes padrão zonais*: os discos persistentes padrão são econômicos e podem lidar com operações sequenciais de leitura/gravação.

  Para mais detalhes, consulte o "Documentação do Google Cloud: Discos permanentes zonais (padrão e SSD)" .

Tamanho do disco

Você precisa escolher um tamanho de disco inicial ao implantar um sistema Cloud Volumes ONTAP . Depois disso, você pode deixar que o NetApp Console gerencie a capacidade de um sistema para você, mas se quiser criar agregados sozinho, esteja ciente do seguinte:

- Todos os discos em um agregado devem ter o mesmo tamanho.
- Determine o espaço que você precisa, levando em consideração o desempenho.
- O desempenho dos discos persistentes é dimensionado automaticamente com o tamanho do disco e o número de vCPUs disponíveis para o sistema.

  Consulte o seguinte para mais detalhes:

  - "Documentação do Google Cloud: Discos permanentes zonais (padrão e SSD)"
  - "Documentação do Google Cloud: Otimizando o desempenho do disco permanente e do SSD local"

Exibir discos de sistema padrão

Além do armazenamento para dados do usuário, o Console também adquire armazenamento em nuvem para dados do sistema Cloud Volumes ONTAP (dados de inicialização, dados raiz, dados principais e NVRAM). Para fins de planejamento, pode ser útil revisar esses detalhes antes de implantar o Cloud Volumes ONTAP.

- "Visualize os discos padrão para dados do sistema Cloud Volumes ONTAP no Google Cloud" .
- "Documentação do Google Cloud: Visão geral das quotas de nuvem"

  O Google Cloud Compute Engine impõe cotas no uso de recursos, portanto, você deve garantir que não atingiu seu limite antes de implantar o Cloud Volumes ONTAP.

O agente do Console também requer um disco do sistema. "Exibir detalhes sobre a configuração padrão do agente do Console" .

Coletar informações de rede

Ao implantar Cloud Volumes ONTAP no Google Cloud, você precisa especificar detalhes sobre sua rede virtual. Você pode usar uma planilha para coletar informações do seu administrador.

Informações de rede para um sistema de nó único

Informações do Google Cloud	Seu valor
Região	
Zona	
Rede VPC	
Sub-rede	
Política de firewall (se estiver usando a sua própria)	

Informações de rede para um par HA em várias zonas

Informações do Google Cloud	Seu valor
Região	
Zona para Nó 1	

Informações do Google Cloud	Seu valor
Zona para o Nó 2	
Zona para o mediador	
VPC-0 e sub-rede	
VPC-1 e sub-rede	
VPC-2 e sub-rede	
VPC-3 e sub-rede	
Política de firewall (se estiver usando a sua própria)	

Informações de rede para um par HA em uma única zona

Informações do Google Cloud	Seu valor
Região	
Zona	
VPC-0 e sub-rede	
VPC-1 e sub-rede	
VPC-2 e sub-rede	
VPC-3 e sub-rede	
Política de firewall (se estiver usando a sua própria)	

Escolha uma velocidade de gravação

O Console permite que você escolha uma configuração de velocidade de gravação para o Cloud Volumes ONTAP, exceto para pares de alta disponibilidade (HA) no Google Cloud. Antes de escolher uma velocidade de gravação, você deve entender as diferenças entre as configurações normal e alta, bem como os riscos e recomendações ao usar alta velocidade de gravação. "Saiba mais sobre velocidade de gravação" .

Escolha um perfil de uso de volume

O ONTAP inclui vários recursos de eficiência de armazenamento que podem reduzir a quantidade total de armazenamento necessária. Ao criar um volume no Console, você pode escolher um perfil que habilite esses recursos ou um perfil que os desabilite. Você deve aprender mais sobre esses recursos para ajudar a decidir qual perfil usar.

Os recursos de eficiência de armazenamento da NetApp oferecem os seguintes benefícios:

Provisionamento fino

Apresenta mais armazenamento lógico para hosts ou usuários do que você realmente tem em seu pool de armazenamento físico. Em vez de pré-alocar espaço de armazenamento, o espaço de armazenamento é alocado dinamicamente para cada volume à medida que os dados são gravados.

Desduplicação

Melhora a eficiência localizando blocos idênticos de dados e substituindo-os por referências a um único bloco compartilhado. Essa técnica reduz os requisitos de capacidade de armazenamento eliminando blocos redundantes de dados que residem no mesmo volume.

Compressão

Reduz a capacidade física necessária para armazenar dados compactando dados dentro de um volume no armazenamento primário, secundário e de arquivo.

Configurar a rede do Google Cloud para o Cloud Volumes ONTAP

O NetApp Console gerencia a configuração de componentes de rede para o Cloud Volumes ONTAP, como endereços IP, máscaras de rede e rotas. Você precisa ter certeza de que o acesso de saída à Internet esteja disponível, que endereços IP privados suficientes estejam disponíveis, que as conexões corretas estejam em vigor e muito mais.

Se você deseja implantar um par de HA, você deve"saiba como os pares de HA funcionam no Google Cloud" .

Requisitos para o Cloud Volumes ONTAP

Os seguintes requisitos devem ser atendidos no Google Cloud.

Requisitos específicos para sistemas de nó único

Se você deseja implantar um sistema de nó único, certifique-se de que sua rede atenda aos seguintes requisitos.

Uma VPC

É necessária uma Virtual Private Cloud (VPC) para um sistema de nó único.

Endereços IP privados

Para um sistema de nó único no Google Cloud, o Console aloca endereços IP privados para o seguinte:

- Nó
- Conjunto
- VM de armazenamento
- Dados NAS LIF
- Dados iSCSI LIF

Você pode pular a criação do LIF de gerenciamento da VM de armazenamento (SVM) se implantar o Cloud Volumes ONTAP usando a API e especificar o seguinte sinalizador:

```
skipSvmManagementLif: true
```

Um LIF é um endereço IP associado a uma porta física. Um LIF de gerenciamento de VM de armazenamento (SVM) é necessário para ferramentas de gerenciamento como o SnapCenter.

Requisitos específicos para pares HA

Se você quiser implantar um par HA, certifique-se de que sua rede atenda aos seguintes requisitos.

Uma ou várias zonas

Você pode garantir a alta disponibilidade dos seus dados implantando uma configuração de HA em várias zonas ou em uma única zona. O Console solicita que você escolha várias zonas ou uma única zona ao criar o par HA.

- Várias zonas (recomendado)

  A implantação de uma configuração de HA em três zonas garante disponibilidade contínua de dados caso ocorra uma falha em uma zona. Observe que o desempenho de gravação é um pouco menor quando comparado ao uso de uma única zona, mas é mínimo.

- Zona única

  Quando implantada em uma única zona, uma configuração do Cloud Volumes ONTAP HA usa uma política de posicionamento espalhado. Esta política garante que uma configuração de HA seja protegida de um único ponto de falha dentro da zona, sem precisar usar zonas separadas para obter isolamento de falhas.

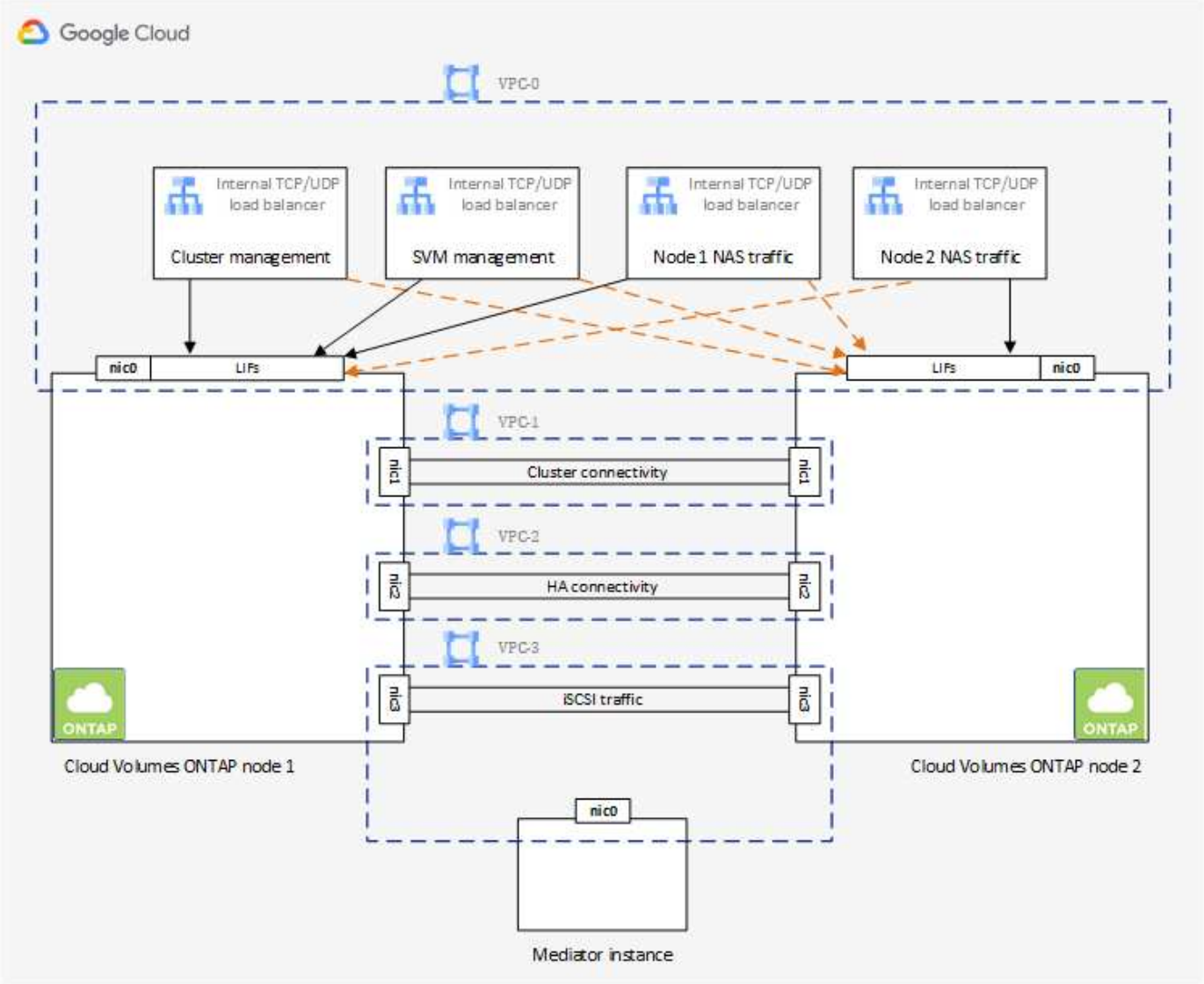
  Este modelo de implantação reduz seus custos porque não há cobranças de saída de dados entre zonas.

Quatro Nuvens Privadas Virtuais

Quatro Nuvens Privadas Virtuais (VPCs) são necessárias para uma configuração de HA. Quatro VPCs são necessárias porque o Google Cloud exige que cada interface de rede resida em uma rede VPC separada.

O Console solicita que você escolha quatro VPCs ao criar o par HA:

- VPC-0 para conexões de entrada aos dados e nós
- VPC-1, VPC-2 e VPC-3 para comunicação interna entre os nós e o mediador HA



Sub-redes

Uma sub-rede privada é necessária para cada VPC.

Se você colocar o agente do Console no VPC-0, precisará habilitar o Private Google Access na sub-rede para acessar as APIs e habilitar a hierarquização de dados.

As sub-redes nessas VPCs devem ter intervalos CIDR distintos. Eles não podem ter intervalos CIDR sobrepostos.

Endereços IP privados

O Console aloca automaticamente o número necessário de endereços IP privados para o Cloud Volumes ONTAP no Google Cloud. Você precisa ter certeza de que sua rede tem endereços privados suficientes disponíveis.

O número de LIFs alocados para Cloud Volumes ONTAP depende se você implanta um sistema de nó único ou um par de HA. Uma LIF é um endereço IP associado a uma porta física. Uma LIF de gerenciamento de SVM é necessária para ferramentas de gerenciamento como SnapCenter.

- **Nó único** O Console aloca 4 endereços IP para um sistema de nó único:

- Gerenciamento de nós LIF
- Gerenciamento de cluster LIF
- Dados iSCSI LIF

> Um iSCSI LIF fornece acesso de cliente pelo protocolo iSCSI e é usado pelo sistema para outros fluxos de trabalho de rede importantes. Esses LIFs são necessários e não devem ser excluídos.

- NAS LIF

  Você pode pular a criação do LIF de gerenciamento da VM de armazenamento (SVM) se implantar o Cloud Volumes ONTAP usando a API e especificar o seguinte sinalizador:

```
skipSvmManagementLif: true
```

- **Par HA** O Console aloca 12-13 endereços IP para um par HA:
  - 2 LIFs de gerenciamento de nós (e0a)
  - 1 Gerenciamento de cluster LIF (e0a)
  - 2 iSCSI LIFs (e0a)

> Um iSCSI LIF fornece acesso de cliente pelo protocolo iSCSI e é usado pelo sistema para outros fluxos de trabalho de rede importantes. Esses LIFs são necessários e não devem ser excluídos.

  - 1 ou 2 NAS LIFs (e0a)
  - 2 LIFs de cluster (e0b)
  - 2 endereços IP de interconexão HA (e0c)
  - 2 endereços IP iSCSI RSM (e0d)

    Você pode pular a criação do LIF de gerenciamento da VM de armazenamento (SVM) se implantar o Cloud Volumes ONTAP usando a API e especificar o seguinte sinalizador:

```
skipSvmManagementLif: true
```

Balanceadores de carga internos

O Console cria quatro balanceadores de carga internos do Google Cloud (TCP/UDP) que gerenciam o tráfego de entrada para o par Cloud Volumes ONTAP HA. Nenhuma configuração é necessária da sua parte. Listamos isso como um requisito simplesmente para informá-lo sobre o tráfego de rede e para atenuar quaisquer preocupações de segurança.

Um balanceador de carga é para gerenciamento de cluster, um é para gerenciamento de VM de armazenamento (SVM), um é para tráfego NAS para o nó 1 e o último é para tráfego NAS para o nó 2.

A configuração para cada balanceador de carga é a seguinte:

- Um endereço IP privado compartilhado
- Um exame de saúde global

Por padrão, as portas usadas pela verificação de integridade são 63001, 63002 e 63003.

- Um serviço regional de backend TCP
- Um serviço regional de backend UDP
- Uma regra de encaminhamento TCP
- Uma regra de encaminhamento UDP
- O acesso global está desabilitado

  Embora o acesso global esteja desabilitado por padrão, há suporte para habilitá-lo após a implantação. Nós o desabilitamos porque o tráfego entre regiões terá latências significativamente maiores. Queríamos garantir que você não tivesse uma experiência negativa devido a montagens acidentais entre regiões. A ativação desta opção é específica para as necessidades do seu negócio.

VPCs compartilhadas

O Cloud Volumes ONTAP e o agente do Console são suportados em uma VPC compartilhada do Google Cloud e também em VPCs autônomas.

Para um sistema de nó único, a VPC pode ser uma VPC compartilhada ou uma VPC independente.

Para um par HA, são necessárias quatro VPCs. Cada uma dessas VPCs pode ser compartilhada ou independente. Por exemplo, VPC-0 pode ser uma VPC compartilhada, enquanto VPC-1, VPC-2 e VPC-3 podem ser VPCs independentes.

Uma VPC compartilhada permite que você configure e gerencie centralmente redes virtuais em vários projetos. Você pode configurar redes VPC compartilhadas no *projeto host* e implantar o agente do Console e as instâncias da máquina virtual Cloud Volumes ONTAP em um *projeto de serviço*.

"Documentação do Google Cloud: Visão geral da VPC compartilhada" .

"Revise as permissões de VPC compartilhadas necessárias abordadas na implantação do agente do Console"

Espelhamento de pacotes em VPCs

"Espelhamento de pacotes"deve ser desabilitado na sub-rede do Google Cloud na qual você implanta o Cloud Volumes ONTAP.

Acesso de saída à Internet

Os sistemas Cloud Volumes ONTAP exigem acesso de saída à Internet para acessar endpoints externos para diversas funções. O Cloud Volumes ONTAP não poderá operar corretamente se esses endpoints estiverem bloqueados em ambientes com requisitos de segurança rigorosos.

O agente do Console também entra em contato com vários endpoints para operações diárias. Para obter informações sobre os pontos de extremidade, consulte "Exibir endpoints contatados pelo agente do Console" e "Preparar a rede para usar o Console" .

Pontos de extremidade Cloud Volumes ONTAP

O Cloud Volumes ONTAP usa esses endpoints para se comunicar com vários serviços.

Pontos finais	Aplicável para	Propósito	Modo de implantação	Impacto se o ponto final não estiver disponível
\ https://netapp-cloud-account.auth0.com	Autenticação	Usado para autenticação no Console.	Modos padrão e restrito.	A autenticação do usuário falha e os seguintes serviços permanecem indisponíveis: • Serviços Cloud Volumes ONTAP • Serviços ONTAP • Protocolos e serviços de proxy
\ https://api.bluexp.netapp.com/tenancy	Arrendamento	Usado para recuperar o recurso Cloud Volumes ONTAP do Console para autorizar recursos e usuários.	Modos padrão e restrito.	Os recursos do Cloud Volumes ONTAP e os usuários não estão autorizados.
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Usado para enviar dados de telemetria do AutoSupport para o suporte da NetApp .	Modos padrão e restrito.	As informações do AutoSupport continuam não entregues.

Pontos finais	Aplicável para	Propósito	Modo de implantação	Impacto se o ponto final não estiver disponível
https://cloudbuild.googleapis.com/v1 (somente para implantações em modo privado) https://cloudkms.googleapis.com/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://compute.googleapis.com/compute/v1 https://www.googleapis.com/compute/beta https://www.googleapis.com/compute/v1/projects/ https://www.googleapis.com/deploymentmanager/v2/projects https://www.googleapis.com/storage/v1 https://www.googleapis.com/upload/storage/v1 https://config.googleapis.com/v1 https://iam.googleapis.com/v1 https://storage.googleapis.com/storage/v1	Google Cloud (uso comercial).	Comunicação com os serviços do Google Cloud.	Modos padrão, restrito e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço Google Cloud para executar operações específicas para o Console no Google Cloud.

Conexões com sistemas ONTAP em outras redes

Para replicar dados entre um sistema Cloud Volumes ONTAP no Google Cloud e sistemas ONTAP em outras redes, você deve ter uma conexão VPN entre a VPC e a outra rede, por exemplo, sua rede corporativa.

"Documentação do Google Cloud: Visão geral do Cloud VPN" .

Regras de firewall

O Console cria regras de firewall do Google Cloud que incluem as regras de entrada e saída que o Cloud Volumes ONTAP precisa para operar com sucesso. Talvez você queira consultar as portas para fins de teste ou, se preferir, usar suas próprias regras de firewall.

As regras de firewall para o Cloud Volumes ONTAP exigem regras de entrada e saída. Se você estiver implantando uma configuração de HA, estas são as regras de firewall para o Cloud Volumes ONTAP no VPC-

0.

Observe que dois conjuntos de regras de firewall são necessários para uma configuração de HA:

- Um conjunto de regras para componentes HA no VPC-0. Essas regras permitem o acesso aos dados do Cloud Volumes ONTAP.
- Outro conjunto de regras para componentes HA em VPC-1, VPC-2 e VPC-3. Essas regras estão abertas para comunicação de entrada e saída entre os componentes do HA. Saber mais .

Procurando informações sobre o agente do Console? "Exibir regras de firewall para o agente do Console"

Regras de entrada

Ao adicionar um sistema Cloud Volumes ONTAP , você pode escolher o filtro de origem para a política de firewall predefinida durante a implantação:

- **Somente VPC selecionada**: o filtro de origem para tráfego de entrada é o intervalo de sub-rede da VPC para o sistema Cloud Volumes ONTAP e o intervalo de sub-rede da VPC onde o agente do Console reside. Esta é a opção recomendada.
- **Todas as VPCs**: o filtro de origem para tráfego de entrada é o intervalo de IP 0.0.0.0/0.

Se você usar sua própria política de firewall, certifique-se de adicionar todas as redes que precisam se comunicar com o Cloud Volumes ONTAP, mas também certifique-se de adicionar ambos os intervalos de endereços para permitir que o Google Load Balancer interno funcione corretamente. Esses endereços são 130.211.0.0/22 e 35.191.0.0/16. Para mais informações, consulte o "Documentação do Google Cloud: Regras de firewall do balanceador de carga" .

Protocolo	Porta	Propósito
Todos os ICMP	Todos	Executando ping na instância
HTTP	80	Acesso HTTP ao console da web do ONTAP System Manager usando o endereço IP do LIF de gerenciamento do cluster
HTTPS	443	Conectividade com o agente do Console e acesso HTTPS ao console da Web do ONTAP System Manager usando o endereço IP do LIF de gerenciamento do cluster
SSH	22	Acesso SSH ao endereço IP do LIF de gerenciamento de cluster ou de um LIF de gerenciamento de nó
TCP	111	Chamada de procedimento remoto para NFS
TCP	139	Sessão de serviço NetBIOS para CIFS
TCP	161-162	Protocolo simples de gerenciamento de rede
TCP	445	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
TCP	635	Montagem NFS
TCP	749	Kerberos
TCP	2049	Daemon do servidor NFS
TCP	3260	Acesso iSCSI através do LIF de dados iSCSI

Protocolo	Porta	Propósito
TCP	4045	Daemon de bloqueio NFS
TCP	4046	Monitor de status de rede para NFS
TCP	10000	Backup usando NDMP
TCP	11104	Gerenciamento de sessões de comunicação entre clusters para SnapMirror
TCP	11105	Transferência de dados do SnapMirror usando LIFs intercluster
TCP	63001-63050	Portas de sondagem de balanceamento de carga para determinar qual nó está íntegro (necessário apenas para pares de HA)
UDP	111	Chamada de procedimento remoto para NFS
UDP	161-162	Protocolo simples de gerenciamento de rede
UDP	635	Montagem NFS
UDP	2049	Daemon do servidor NFS
UDP	4045	Daemon de bloqueio NFS
UDP	4046	Monitor de status de rede para NFS
UDP	4049	Protocolo NFS rquotad

Regras de saída

O grupo de segurança predefinido para o Cloud Volumes ONTAP abre todo o tráfego de saída. Se isso for aceitável, siga as regras básicas de saída. Se precisar de regras mais rígidas, use as regras de saída avançadas.

Regras básicas de saída

O grupo de segurança predefinido para o Cloud Volumes ONTAP inclui as seguintes regras de saída.

Protocolo	Porta	Propósito
Todos os ICMP	Todos	Todo o tráfego de saída
Todos os TCP	Todos	Todo o tráfego de saída
Todos os UDP	Todos	Todo o tráfego de saída

Regras avançadas de saída

Se precisar de regras rígidas para o tráfego de saída, você pode usar as seguintes informações para abrir apenas as portas necessárias para a comunicação de saída pelo Cloud Volumes ONTAP. Os clusters Cloud Volumes ONTAP usam as seguintes portas para regular o tráfego de nós.

A origem é a interface (endereço IP) do sistema Cloud Volumes ONTAP .

Serviço	Protocolo	Porta	Fonte	Destino	Propósito
Diretório ativo	TCP	88	Gerenciamento de nós LIF	Floresta do Active Directory	Autenticação Kerberos V
	UDP	137	Gerenciamento de nós LIF	Floresta do Active Directory	Serviço de nomes NetBIOS
	UDP	138	Gerenciamento de nós LIF	Floresta do Active Directory	Serviço de datagrama NetBIOS
	TCP	139	Gerenciamento de nós LIF	Floresta do Active Directory	Sessão de serviço NetBIOS
	TCP e UDP	389	Gerenciamento de nós LIF	Floresta do Active Directory	LDAP
	TCP	445	Gerenciamento de nós LIF	Floresta do Active Directory	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
	TCP	464	Gerenciamento de nós LIF	Floresta do Active Directory	Alteração e definição de senha do Kerberos V (SET_CHANGE)
	UDP	464	Gerenciamento de nós LIF	Floresta do Active Directory	Administração de chaves Kerberos
	TCP	749	Gerenciamento de nós LIF	Floresta do Active Directory	Kerberos V alterar e definir senha (RPCSEC_GSS)
	TCP	88	Dados LIF (NFS, CIFS, iSCSI)	Floresta do Active Directory	Autenticação Kerberos V
	UDP	137	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Serviço de nomes NetBIOS
	UDP	138	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Serviço de datagrama NetBIOS
	TCP	139	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Sessão de serviço NetBIOS
	TCP e UDP	389	Dados LIF (NFS, CIFS)	Floresta do Active Directory	LDAP
	TCP	445	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
	TCP	464	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Alteração e definição de senha do Kerberos V (SET_CHANGE)
	UDP	464	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Administração de chaves Kerberos
	TCP	749	Dados LIF (NFS, CIFS)	Floresta do Active Directory	Alterar e definir senha do Kerberos V (RPCSEC_GSS)

Serviço	Protocolo	Porta	Fonte	Destino	Propósito
AutoSupport	HTTPS	443	Gerenciamento de nós LIF	meusuporte.netapp.com	AutoSupport (HTTPS é o padrão)
	HTTP	80	Gerenciamento de nós LIF	meusuporte.netapp.com	AutoSupport (somente se o protocolo de transporte for alterado de HTTPS para HTTP)
	TCP	3128	Gerenciamento de nós LIF	Agente de console	Envio de mensagens do AutoSupport por meio de um servidor proxy no agente do Console, se uma conexão de saída com a Internet não estiver disponível
Backups de configuração	HTTP	80	Gerenciamento de nós LIF	http://<endereço-IP-do-agente-do-console>/occm/offboxconfig	Envie backups de configuração para o agente do Console."Documentação do ONTAP"
DHCP	UDP	68	Gerenciamento de nós LIF	DHCP	Cliente DHCP para configuração inicial
DHCPS	UDP	67	Gerenciamento de nós LIF	DHCP	Servidor DHCP
DNS	UDP	53	Gerenciamento de nós LIF e dados LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	Gerenciamento de nós LIF	Servidores de destino	Cópia do NDMP
SMTP	TCP	25	Gerenciamento de nós LIF	Servidor de e-mail	Alertas SMTP podem ser usados para AutoSupport
SNMP	TCP	161	Gerenciamento de nós LIF	Servidor de monitoramento	Monitoramento por armadilhas SNMP
	UDP	161	Gerenciamento de nós LIF	Servidor de monitoramento	Monitoramento por armadilhas SNMP
	TCP	162	Gerenciamento de nós LIF	Servidor de monitoramento	Monitoramento por armadilhas SNMP
	UDP	162	Gerenciamento de nós LIF	Servidor de monitoramento	Monitoramento por armadilhas SNMP
SnapMirror	TCP	11104	LIF interaglomerado	LIFs interaglomerados ONTAP	Gerenciamento de sessões de comunicação entre clusters para SnapMirror
	TCP	11105	LIF interaglomerado	LIFs interaglomerados ONTAP	Transferência de dados do SnapMirror

Serviço	Protocolo	Porta	Fonte	Destino	Propósito
Log de sistema	UDP	514	Gerenciamento de nós LIF	Servidor Syslog	Mensagens de encaminhamento do Syslog

Regras para VPC-1, VPC-2 e VPC-3

No Google Cloud, uma configuração de HA é implantada em quatro VPCs. As regras de firewall necessárias para a configuração de HA no VPC-0 sãolistado acima para Cloud Volumes ONTAP .

Enquanto isso, as regras de firewall predefinidas criadas para as instâncias em VPC-1, VPC-2 e VPC-3 permitem a comunicação de entrada em *todos* os protocolos e portas. Essas regras permitem a comunicação entre nós de HA.

A comunicação dos nós HA com o mediador HA ocorre pela porta 3260 (iSCSI).

> Para habilitar alta velocidade de gravação para novas implantações de pares de HA do Google Cloud, uma unidade máxima de transmissão (MTU) de pelo menos 8.896 bytes é necessária para VPC-1, VPC-2 e VPC-3. Se você optar por atualizar as VPC-1, VPC-2 e VPC-3 existentes para uma MTU de 8.896 bytes, deverá desligar todos os sistemas HA existentes que usam essas VPCs durante o processo de configuração.

Requisitos para o agente do console

Se você ainda não criou um agente do Console, revise os requisitos de rede.

- "Exibir requisitos de rede para o agente do Console"
- "Regras de firewall no Google Cloud"

Configurações de rede para oferecer suporte ao proxy do agente do console

Você pode usar os servidores proxy configurados para o agente do Console para habilitar o acesso de saída à Internet do Cloud Volumes ONTAP. O Console suporta dois tipos de proxies:

- **Proxy explícito**: O tráfego de saída do Cloud Volumes ONTAP usa o endereço HTTP do servidor proxy especificado durante a configuração do proxy do agente do Console. O administrador do agente do Console também pode ter configurado credenciais de usuário e certificados de CA raiz para autenticação adicional. Se um certificado de CA raiz estiver disponível para o proxy explícito, certifique-se de obter e carregar o mesmo certificado para o seu sistema Cloud Volumes ONTAP usando o "ONTAP CLI: instalação do certificado de segurança" comando.
- **Proxy transparente**: A rede está configurada para rotear automaticamente o tráfego de saída do Cloud Volumes ONTAP por meio do proxy do agente do Console. Ao configurar um proxy transparente, o administrador do agente do Console precisa fornecer apenas um certificado de CA raiz para conectividade do Cloud Volumes ONTAP, não o endereço HTTP do servidor proxy. Certifique-se de obter e carregar o mesmo certificado de CA raiz para o seu sistema Cloud Volumes ONTAP usando o "ONTAP CLI: instalação do certificado de segurança" comando.

Para obter informações sobre como configurar servidores proxy para o agente do Console, consulte o "Configurar um agente de console para usar um servidor proxy" .

Configurar tags de rede para o Cloud Volumes ONTAP no Google Cloud

Durante a configuração do proxy transparente do agente do Console, o administrador adiciona uma tag de

rede para o Google Cloud. Você precisa obter e adicionar manualmente a mesma tag de rede para sua configuração do Cloud Volumes ONTAP . Esta tag é necessária para que o servidor proxy funcione corretamente.

1. No Console do Google Cloud, localize seu sistema Cloud Volumes ONTAP.
2. Vá para **Detalhes > Rede > Tags de rede**.
3. Adicione a tag usada para o agente do Console e salve a configuração.

Tópicos relacionados

- "Verifique a configuração do AutoSupport para o Cloud Volumes ONTAP"
- "Saiba mais sobre as portas internas do ONTAP" .

Configurar o VPC Service Controls para implantar o Cloud Volumes ONTAP no Google Cloud

Ao escolher bloquear seu ambiente do Google Cloud com o VPC Service Controls, você deve entender como o NetApp Console e o Cloud Volumes ONTAP interagem com as APIs do Google Cloud, bem como configurar seu perímetro de serviço para implantar o Console e o Cloud Volumes ONTAP.

Os Controles de Serviço VPC permitem que você controle o acesso a serviços gerenciados pelo Google fora de um perímetro confiável, bloqueie o acesso a dados de locais não confiáveis e mitigue riscos de transferência de dados não autorizada. "Saiba mais sobre os controles de serviço VPC do Google Cloud" .

Como os serviços NetApp se comunicam com os VPC Service Controls

O Console se comunica diretamente com as APIs do Google Cloud. Isso é acionado por um endereço IP externo fora do Google Cloud (por exemplo, de api.services.cloud.netapp.com) ou dentro do Google Cloud a partir de um endereço interno atribuído ao agente do Console.

Dependendo do estilo de implantação do agente do Console, certas exceções podem ter que ser feitas para seu perímetro de serviço.

Imagens

Tanto Cloud Volumes ONTAP quanto o Console usam imagens de um projeto no Google Cloud que é gerenciado pela NetApp. Isso pode afetar a implantação do agente do Console e do Cloud Volumes ONTAP, se sua organização tiver uma política que bloqueia o uso de imagens que não estão hospedadas dentro da organização.

Você pode implantar um agente do Console manualmente usando o método de instalação manual, mas o Cloud Volumes ONTAP também precisará extrair imagens do projeto NetApp . Você deve fornecer uma lista permitida para implantar um agente do Console e o Cloud Volumes ONTAP.

Implantando um agente de console

O usuário que implanta um agente do Console precisa ser capaz de referenciar uma imagem hospedada no projectId *netapp-cloudmanager* e no número do projeto *14190056516*.

Implantando o Cloud Volumes ONTAP

- A conta de serviço do Console precisa fazer referência a uma imagem hospedada no projectId *netapp-*

cloudmanager e ao número do projeto *14190056516* do projeto de serviço.

- A conta de serviço do Agente de Serviço de APIs padrão do Google precisa fazer referência a uma imagem hospedada no projectId *netapp-cloudmanager* e ao número do projeto *14190056516* do projeto de serviço.

Exemplos das regras necessárias para extrair essas imagens com o VPC Service Controls são definidos abaixo.

Políticas de perímetro do VPC Service Controls

As políticas permitem exceções aos conjuntos de regras de Controles de Serviço da VPC. Para obter mais informações sobre políticas, visite o "Documentação da política de Service Controls VPC do Google Cloud".

Para definir as políticas exigidas pelo Console, navegue até o Perímetro de Controles de Serviço da VPC na sua organização e adicione as seguintes políticas. Os campos devem corresponder às opções fornecidas na página de política do VPC Service Controls. Observe também que **todas** as regras são obrigatórias e os parâmetros **OU** devem ser usados no conjunto de regras.

Regras de entrada

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Service Project]
    Services =
        Service name: iam.googleapis.com
          Service methods: All actions
        Service name: compute.googleapis.com
          Service methods:All actions
```

OU

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Host Project]
    Services =
        Service name: compute.googleapis.com
          Service methods: All actions
```

OU

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
    Source > All sources allowed
To:
    Projects =
        [Service Project]
        [Host Project]
    Services =
        Service name: compute.googleapis.com
        Service methods: All actions
```

Regras de saída

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
To:
    Projects =
        14190056516
    Service =
        Service name: compute.googleapis.com
        Service methods: All actions
```

O número do projeto descrito acima é o projeto *netapp-cloudmanager* usado pela NetApp para armazenar imagens para o agente do Console e para o Cloud Volumes ONTAP.

Crie uma conta de serviço do Google Cloud para o Cloud Volumes ONTAP

O Cloud Volumes ONTAP requer uma conta de serviço do Google Cloud para duas finalidades. A primeira é quando você habilita"hierarquização de dados" para hierarquizar dados frios para armazenamento de objetos de baixo custo no Google Cloud. A segunda é quando você habilita o "NetApp Backup and Recovery" para fazer backup de volumes em armazenamento de objetos de baixo custo.

O Cloud Volumes ONTAP usa a conta de serviço para acessar e gerenciar um bucket para dados em camadas e outro bucket para backups.

Você pode configurar uma conta de serviço e usá-la para ambas as finalidades. A conta de serviço deve ter a função **Administrador de armazenamento**.

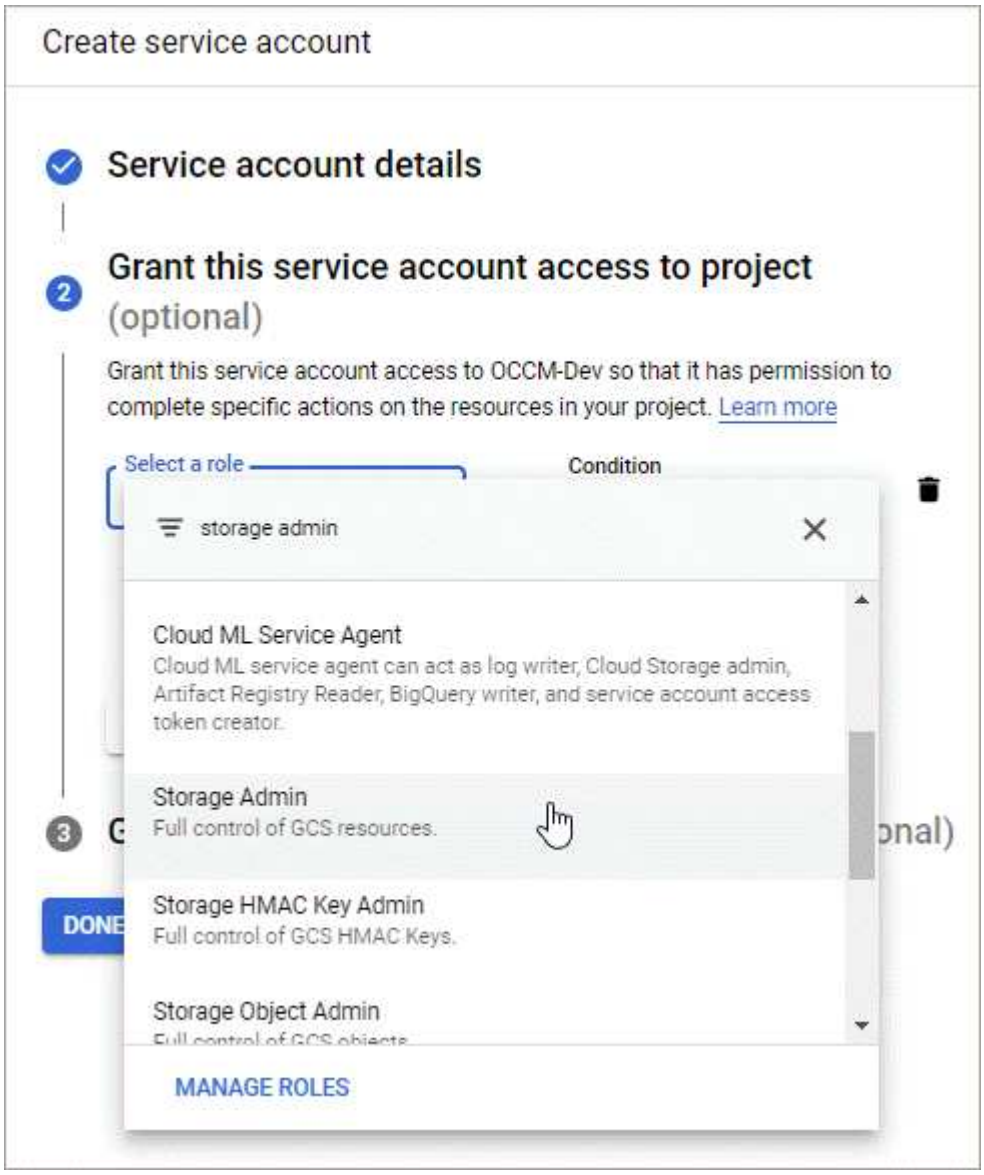
Passos

1. No Console do Google Cloud, "vá para a página de contas de serviço".
2. Selecione seu projeto.

3. Clique em **Criar conta de serviço** e forneça as informações necessárias.

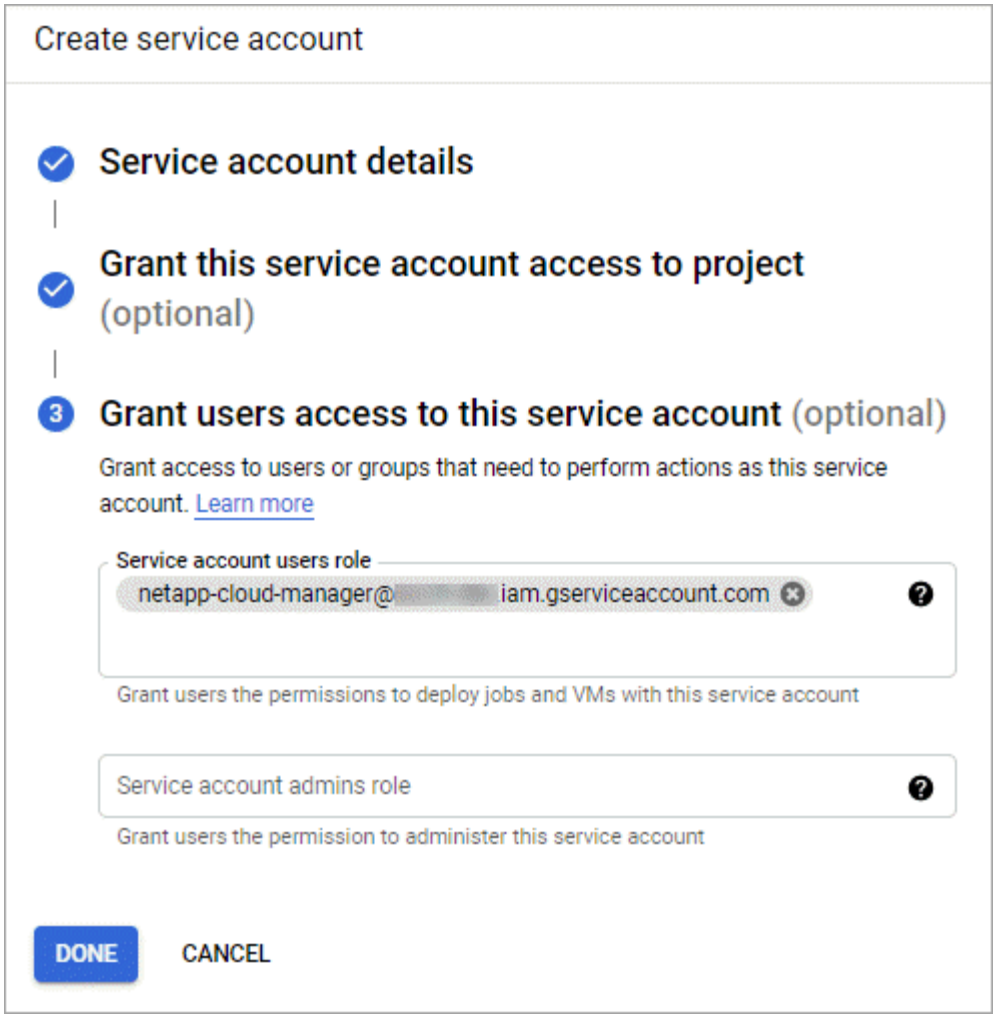
   a. **Detalhes da conta de serviço**: insira um nome e uma descrição.

   b. **Conceder a esta conta de serviço acesso ao projeto**: Selecione a função **Administrador de armazenamento**.



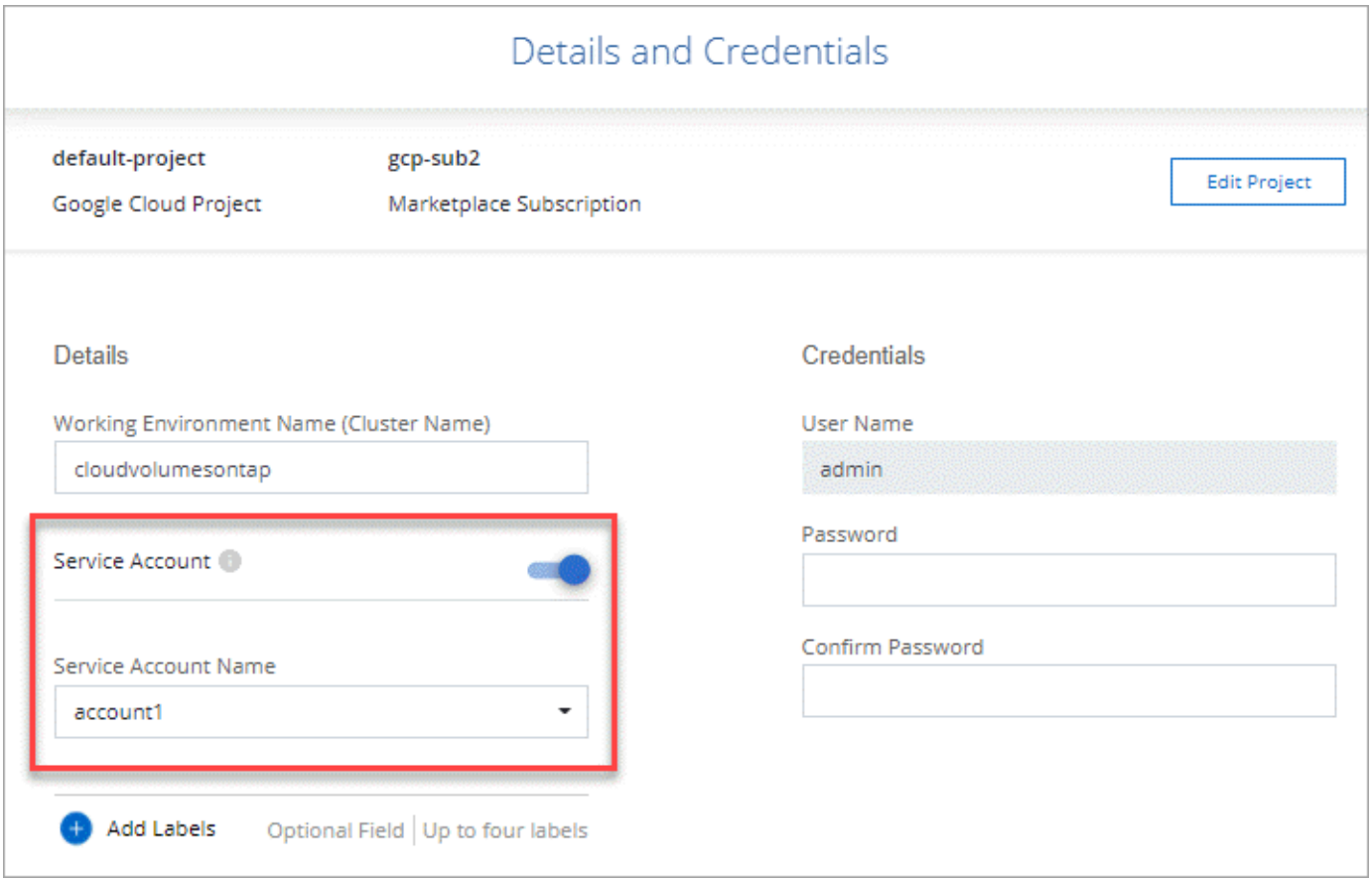
   c. **Conceder aos usuários acesso a esta conta de serviço**: adicione a conta de serviço do agente do Console como um *Usuário da conta de serviço* a esta nova conta de serviço.

      Esta etapa é necessária somente para a hierarquização de dados. Não é necessário para backup e recuperação.



O que vem a seguir?

Você precisará selecionar a conta de serviço mais tarde ao criar um sistema Cloud Volumes ONTAP .



Usando chaves de criptografia gerenciadas pelo cliente com o Cloud Volumes ONTAP

Embora o Google Cloud Storage sempre criptografe seus dados antes de gravá-los no disco, você pode usar as APIs para criar um sistema Cloud Volumes ONTAP que usa *chaves de criptografia gerenciadas pelo cliente*. Essas são chaves que você gera e gerencia no GCP usando o Cloud Key Management Service.

Passos

1. Certifique-se de que a conta de serviço do agente do Console tenha as permissões corretas no nível do projeto, no projeto onde a chave está armazenada.

   As permissões são fornecidas no "as permissões da conta de serviço por padrão" , mas pode não ser aplicável se você usar um projeto alternativo para o Cloud Key Management Service.

   As permissões são as seguintes:

   ```
   - cloudkms.cryptoKeyVersions.useToEncrypt
   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.list
   ```

2. Certifique-se de que a conta de serviço para o "Agente de serviço do Google Compute Engine" tem permissões do Cloud KMS Encrypter/Decrypter na chave.

O nome da conta de serviço usa o seguinte formato: "service-[service_project_number]@compute-system.iam.gserviceaccount.com".

"Documentação do Google Cloud: Usando o IAM com o Cloud KMS - Concedendo funções em um recurso"

3. Obtenha o "id" da chave invocando o comando get para `/gcp/vsa/metadata/gcp-encryption-keys` Chamada de API ou escolhendo "Copiar nome do recurso" na chave no console do GCP.
4. Se estiver usando chaves de criptografia gerenciadas pelo cliente e hierarquizando dados para armazenamento de objetos, o NetApp Console tentará utilizar as mesmas chaves usadas para criptografar os discos persistentes. Mas primeiro você precisa habilitar os buckets do Google Cloud Storage para usar as chaves:

   a. Encontre o agente de serviço do Google Cloud Storage seguindo o "Documentação do Google Cloud: Obtendo o agente de serviço do Cloud Storage" .

   b. Navegue até a chave de criptografia e atribua ao agente de serviço do Google Cloud Storage permissões de Criptografador/Descriptografador do Cloud KMS.

   Para mais informações, consulte "Documentação do Google Cloud: Usando chaves de criptografia gerenciadas pelo cliente"

5. Use o parâmetro ""gcpEncryption"" na sua solicitação de API ao criar um sistema.

   Exemplo

```
"gcpEncryptionParameters": {
    "key": "projects/project-1/locations/us-east4/keyRings/keyring-1/cryptoKeys/generatedkey1"
  }
```

Consulte o "Documentação de automação do NetApp Console" para mais detalhes sobre o uso do parâmetro "GcpEncryption".

Configurar o licenciamento do Cloud Volumes ONTAP no Google Cloud

Depois de decidir qual opção de licenciamento você deseja usar com o Cloud Volumes ONTAP, algumas etapas são necessárias antes que você possa escolher essa opção de licenciamento ao criar um novo sistema.

Freemium

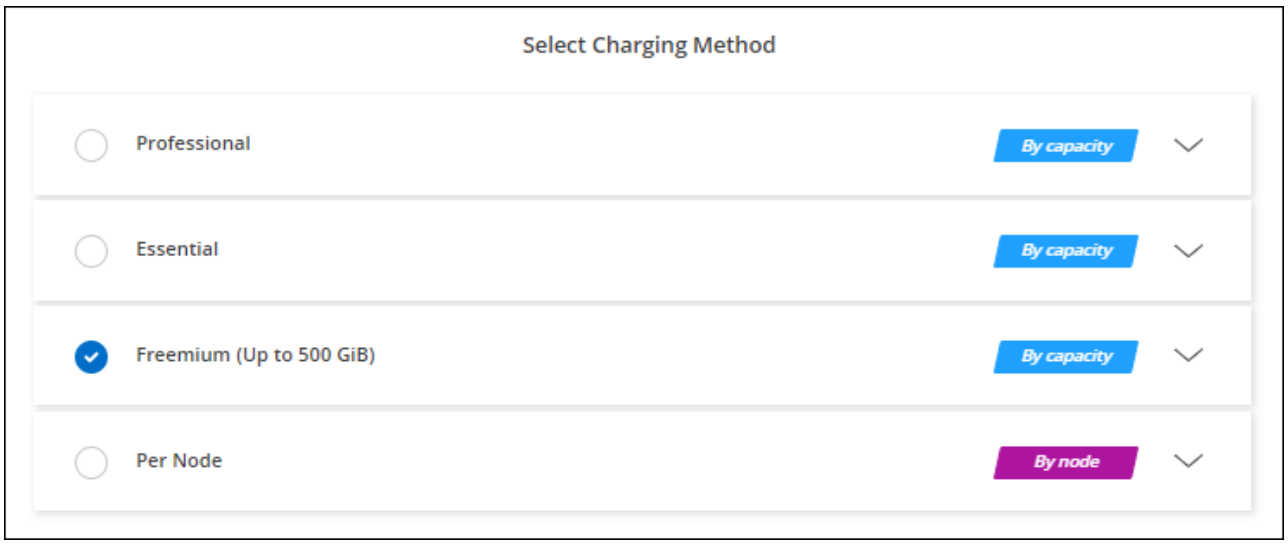
Selecione a oferta Freemium para usar o Cloud Volumes ONTAP gratuitamente com até 500 GiB de capacidade provisionada. "Saiba mais sobre a oferta Freemium" .

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas no NetApp Console.
   a. Na página **Detalhes e credenciais**, clique em **Editar credenciais > Adicionar assinatura** e siga as instruções para assinar a oferta de pagamento conforme o uso no Google Cloud Marketplace.

Você não será cobrado pela assinatura do marketplace, a menos que exceda 500 GiB de capacidade provisionada, momento em que o sistema será automaticamente convertido para o"Pacote Essentials" .

b. Após retornar ao Console, selecione **Freemium** quando chegar à página de métodos de cobrança.



"Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP no Google Cloud" .

Licença baseada em capacidade

O licenciamento baseado em capacidade permite que você pague pelo Cloud Volumes ONTAP por TiB de capacidade. O licenciamento baseado em capacidade está disponível na forma de um *pacote*: o pacote Essentials ou Professional.

Os pacotes Essentials e Professional estão disponíveis nos seguintes modelos de consumo ou opções de compra:

- Uma licença (traga sua própria licença (BYOL)) adquirida da NetApp
- Uma assinatura por hora, paga conforme o uso (PAYGO), do Google Cloud Marketplace
- Um contrato anual

"Saiba mais sobre licenciamento baseado em capacidade" .

As seções a seguir descrevem como começar a usar cada um desses modelos de consumo.

Traga sua própria bebida

Pague antecipadamente comprando uma licença (BYOL) da NetApp para implantar sistemas Cloud Volumes ONTAP em qualquer provedor de nuvem.

A NetApp restringiu a compra, extensão e renovação de licenças BYOL. Para obter mais informações, consulte "Disponibilidade restrita de licenciamento BYOL para Cloud Volumes ONTAP" .

Passos

1. "Entre em contato com a equipe de vendas da NetApp para obter uma licença"

2. "Adicione sua conta do site de suporte da NetApp ao NetApp Console"

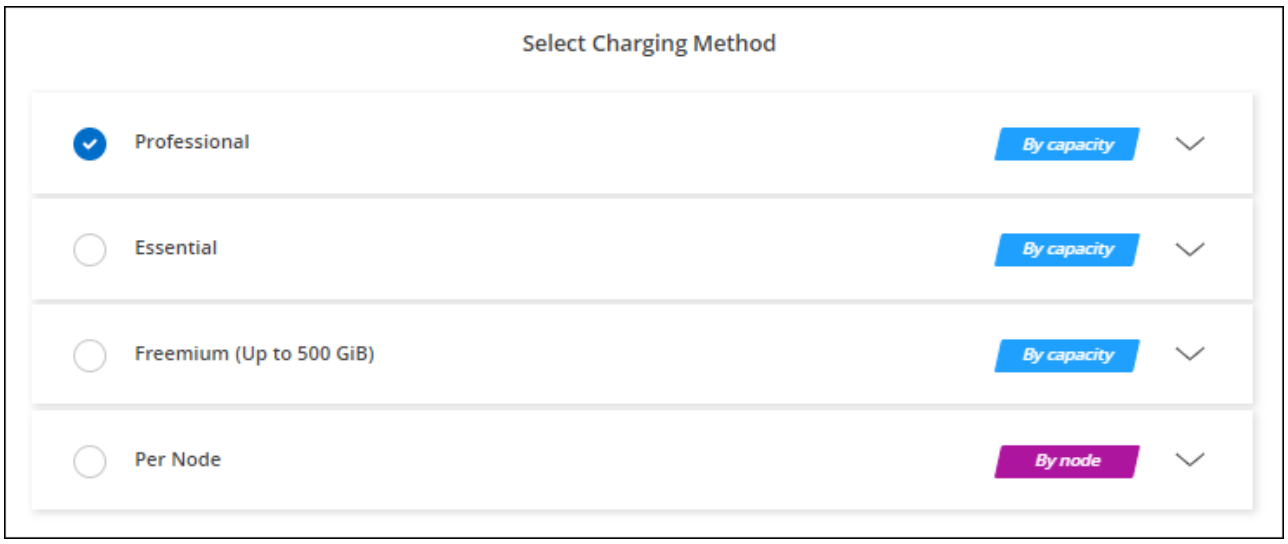
   O Console consulta automaticamente o serviço de licenciamento da NetApp para obter detalhes sobre as licenças associadas à sua conta do Site de Suporte da NetApp . Se não houver erros, o Console adiciona as licenças.

   Sua licença deve estar disponível no Console antes que você possa usá-la com o Cloud Volumes ONTAP. Se necessário, você pode"adicione manualmente a licença ao Console" .

3. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas.
   a. Na página **Detalhes e credenciais**, clique em **Editar credenciais > Adicionar assinatura** e siga as instruções para assinar a oferta de pagamento conforme o uso no Google Cloud Marketplace.

      A licença que você comprou da NetApp é sempre cobrada primeiro, mas você será cobrado pela taxa horária no mercado se exceder sua capacidade licenciada ou se o prazo de sua licença expirar.

   b. Após retornar ao Console, selecione um pacote baseado em capacidade quando chegar à página de métodos de cobrança.



"Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP no Google Cloud" .

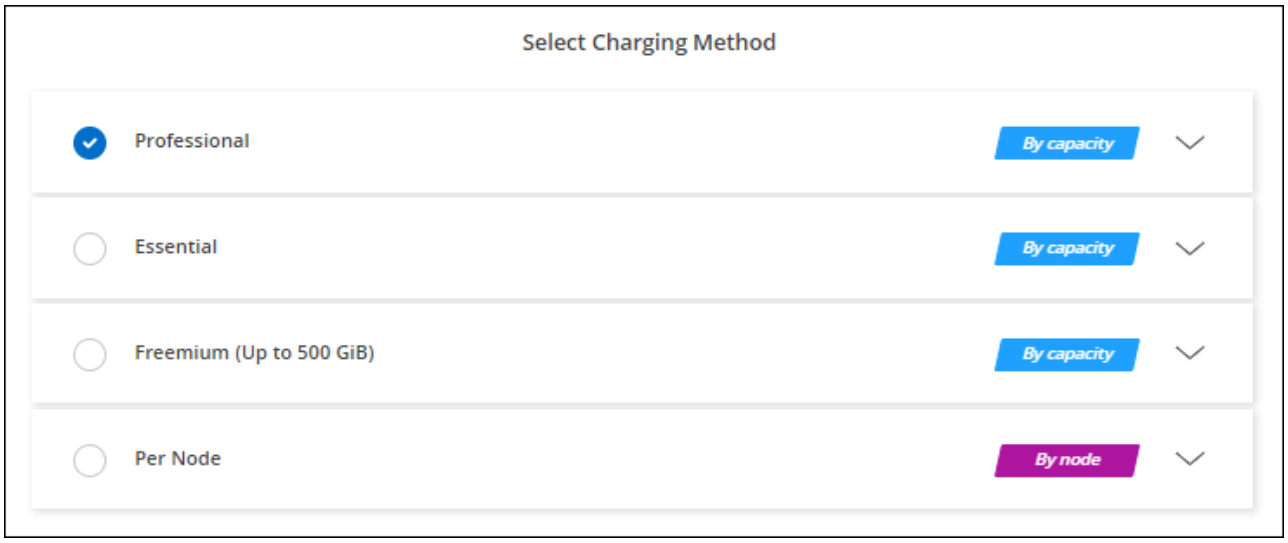
Assinatura PAYGO

Pague por hora assinando a oferta do marketplace do seu provedor de nuvem.

Ao criar um sistema Cloud Volumes ONTAP , o Console solicita que você assine o contrato disponível no Google Cloud Marketplace. Essa assinatura é então associada ao sistema de cobrança. Você pode usar a mesma assinatura para sistemas adicionais.

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas.
   a. Na página **Detalhes e credenciais**, clique em **Editar credenciais > Adicionar assinatura** e siga as instruções para assinar a oferta de pagamento conforme o uso no Google Cloud Marketplace.
   b. Após retornar ao Console, selecione um pacote baseado em capacidade quando chegar à página de métodos de cobrança.



"Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP no Google Cloud" .

Você pode gerenciar as assinaturas do Google Cloud Marketplace associadas às suas contas na página Configurações > Credenciais. "Aprenda a gerenciar suas credenciais e assinaturas do Google Cloud"

Contrato anual

Pague pelo Cloud Volumes ONTAP anualmente comprando um contrato anual.

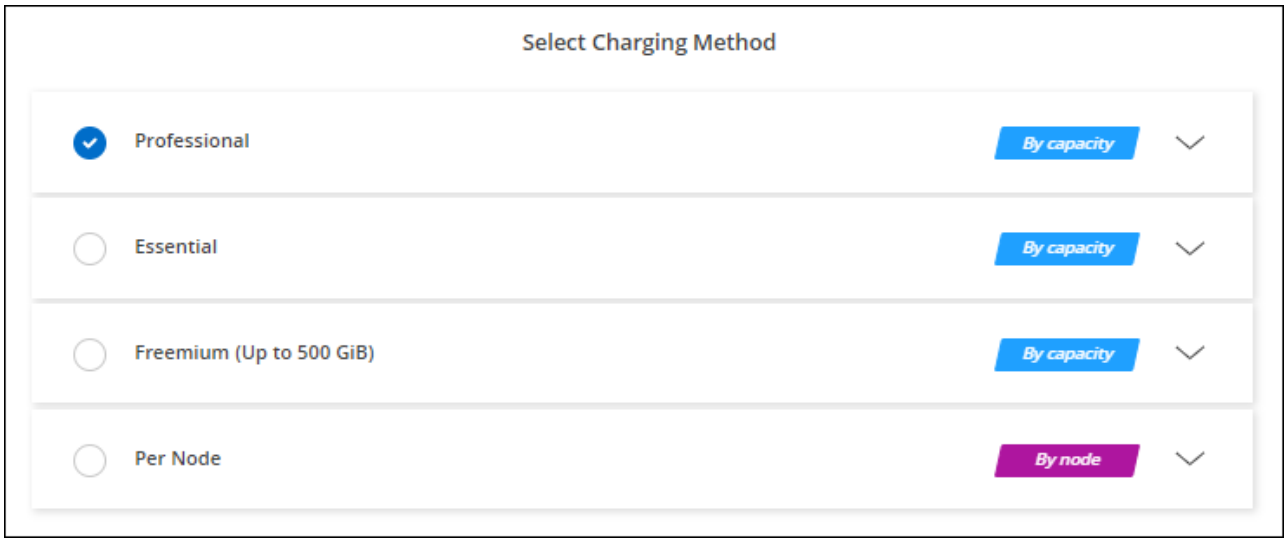
Passos

1. Entre em contato com seu representante de vendas da NetApp para adquirir um contrato anual.

   O contrato está disponível como uma oferta *privada* no Google Cloud Marketplace.

   Depois que a NetApp compartilhar a oferta privada com você, você poderá selecionar o plano anual ao assinar o Google Cloud Marketplace durante a criação do sistema.

2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas.
   a. Na página **Detalhes e credenciais**, clique em **Editar credenciais > Adicionar assinatura** e siga as instruções para assinar o plano anual no Google Cloud Marketplace.
   b. No Google Cloud, selecione o plano anual que foi compartilhado com sua conta e clique em **Assinar**.
   c. Após retornar ao Console, selecione um pacote baseado em capacidade quando chegar à página de métodos de cobrança.



"Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP no Google Cloud" .

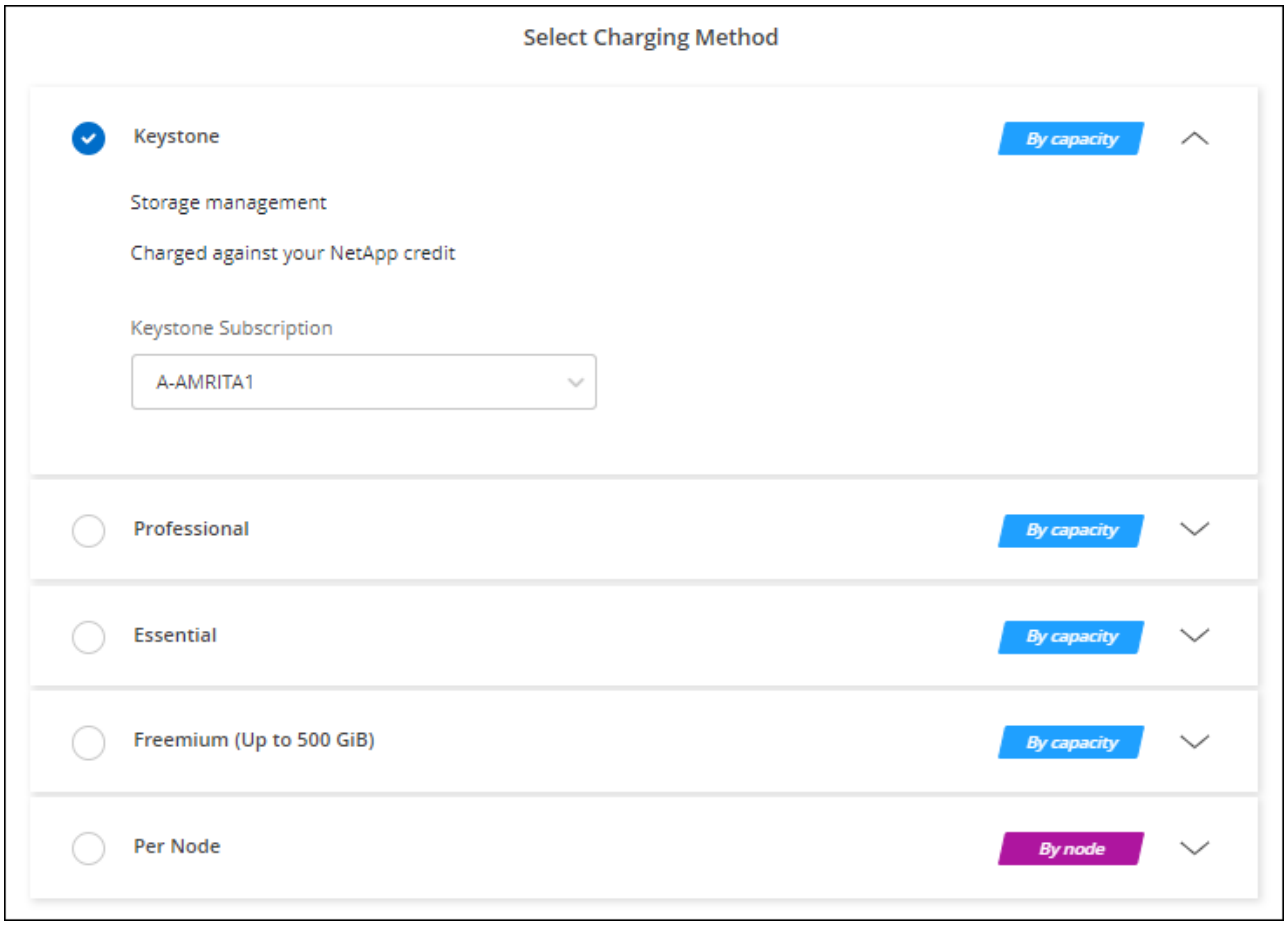
Assinatura Keystone

Uma assinatura Keystone é um serviço baseado em assinatura com pagamento conforme o crescimento. "Saiba mais sobre as assinaturas do NetApp Keystone" .

Passos

1. Se você ainda não tem uma assinatura, "entre em contato com a NetApp"
2. Entre em contato com a NetApp para autorizar sua conta de usuário do Console com uma ou mais assinaturas do Keystone .
3. Depois que a NetApp autorizar sua conta,"vincule suas assinaturas para uso com o Cloud Volumes ONTAP" .
4. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas.

    a. Selecione o método de cobrança da Assinatura Keystone quando solicitado a escolher um método de cobrança.



"Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP no Google Cloud" .

Licença baseada em nó

Uma licença baseada em nó é a licença da geração anterior para o Cloud Volumes ONTAP. Uma licença baseada em nó pode ser adquirida da NetApp (BYOL) e está disponível para renovações de licença apenas em casos específicos. Para obter informações, consulte:

- "Fim da disponibilidade de licenças baseadas em nós"
- "Fim da disponibilidade de licenças baseadas em nós"
- "Converter uma licença baseada em nós para uma licença baseada em capacidade."

Inicie o Cloud Volumes ONTAP no Google Cloud

Você pode iniciar o Cloud Volumes ONTAP em uma configuração de nó único ou como um par de HA no Google Cloud.

Antes de começar

Você precisa do seguinte antes de começar.

- Um agente da NetApp Console que está em funcionamento.
  - Você deveria ter um "Agente de console associado ao seu sistema" .
  - "Você deve estar preparado para deixar o agente do Console em execução o tempo todo" .

- A conta de serviço associada ao agente do Console "deve ter as permissões necessárias"

- Uma compreensão da configuração que você deseja usar.

  Você deve ter se preparado escolhendo uma configuração e obtendo informações de rede do Google Cloud com seu administrador. Para mais detalhes, consulte"Planejando sua configuração do Cloud Volumes ONTAP" .

- Uma compreensão do que é necessário para configurar o licenciamento do Cloud Volumes ONTAP.

  "Aprenda como configurar o licenciamento" .

- As APIs do Google Cloud devem ser "habilitado em seu projeto" :
  - API do Gerenciador de Implantação em Nuvem V2
  - API de registro em nuvem
  - API do Gerenciador de Recursos de Nuvem
  - API do mecanismo de computação
  - API de gerenciamento de identidade e acesso (IAM)

Inicie um sistema de nó único no Google Cloud

Crie um sistema no NetApp Console para iniciar o Cloud Volumes ONTAP no Google Cloud.

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as instruções.
3. **Escolha um local**: Selecione **Google Cloud** e * Cloud Volumes ONTAP*.
4. Se você for solicitado, "criar um agente de console" .
5. **Detalhes e credenciais**: selecione um projeto, especifique um nome de cluster, opcionalmente selecione uma conta de serviço, opcionalmente adicione rótulos e, em seguida, especifique as credenciais.

   A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Nome do sistema	O Console usa o nome do sistema para nomear o sistema Cloud Volumes ONTAP e a instância da VM do Google Cloud. Ele também usa o nome como prefixo para o grupo de segurança predefinido, se você selecionar essa opção.
Nome da conta de serviço	Se você planeja usar"hierarquização de dados" ou "NetApp Backup and Recovery" com o Cloud Volumes ONTAP, você precisa habilitar **Conta de serviço** e selecionar uma conta de serviço que tenha a função de administrador de armazenamento predefinida. "Aprenda a criar uma conta de serviço" .
Adicionar rótulos	Os rótulos são metadados para seus recursos do Google Cloud. O Console adiciona os rótulos ao sistema Cloud Volumes ONTAP e aos recursos do Google Cloud associados ao sistema. Você pode adicionar até quatro rótulos na interface do usuário ao criar um sistema e depois adicionar mais depois que ele for criado. Observe que a API não limita você a quatro rótulos ao criar um sistema. Para obter informações sobre rótulos, consulte o "Documentação do Google Cloud: Rotulagem de recursos" .

Campo	Descrição
Nome de usuário e senha	Estas são as credenciais para a conta de administrador do cluster Cloud Volumes ONTAP . Você pode usar essas credenciais para se conectar ao Cloud Volumes ONTAP por meio do ONTAP System Manager ou do ONTAP CLI. Mantenha o nome de usuário padrão *admin* ou altere-o para um nome de usuário personalizado.
Editar Projeto	Selecione o projeto onde você deseja que o Cloud Volumes ONTAP resida. O projeto padrão é o projeto onde o Console está localizado. Se você não vir nenhum projeto adicional na lista suspensa, significa que ainda não associou a conta de serviço a outros projetos. Vá para o Google Cloud Console, abra o serviço IAM e selecione o projeto. Adicione a conta de serviço com a função que você usa para o Console a esse projeto. Você precisará repetir esta etapa para cada projeto. Esta é a conta de serviço que você configurou para o Console,"conforme descrito nesta página" . Clique em **Adicionar assinatura** para associar as credenciais selecionadas a uma assinatura. Para criar um sistema Cloud Volumes ONTAP com pagamento conforme o uso, você precisa selecionar um projeto do Google Cloud associado a uma assinatura do Cloud Volumes ONTAP no marketplace do Google Cloud. Consulte "Associando uma assinatura do marketplace às credenciais do Google Cloud" .

6. **Serviços**: Selecione os serviços que você deseja usar neste sistema. Para selecionar Backup e Recuperação ou usar o NetApp Cloud Tiering, você deve ter especificado a Conta de Serviço na etapa 3.

   Se você quiser utilizar WORM e camadas de dados, desabilite o Backup e Recuperação e implante um sistema Cloud Volumes ONTAP com versão 9.8 ou superior.

7. **Localização e conectividade**: Selecione a região e a zona do Google Cloud para o seu sistema, escolha uma política de firewall e confirme a conectividade de rede com o storage do Google Cloud para o tiering de dados.

   A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Verificação de conectividade	Para hierarquizar dados frios em um bucket do Google Cloud Storage, a sub-rede na qual o Cloud Volumes ONTAP reside deve ser configurada para o Private Google Access. Para obter instruções, consulte "Documentação do Google Cloud: Configurando o acesso privado do Google" .

Campo	Descrição
Política de firewall gerada	Se você deixar o Console gerar a política de firewall para você, precisará escolher como permitirá o tráfego: • Se você escolher **Somente VPC selecionada**, o filtro de origem para tráfego de entrada será o intervalo de sub-rede da VPC selecionada e o intervalo de sub-rede da VPC onde o agente do Console reside. Esta é a opção recomendada. • Se você escolher **Todas as VPCs**, o filtro de origem para o tráfego de entrada será o intervalo de IP 0.0.0.0/0.
Usar política de firewall existente	Se você usar uma política de firewall existente, certifique-se de que ela inclua as regras necessárias:"Saiba mais sobre as regras de firewall para o Cloud Volumes ONTAP"

8. **Métodos de cobrança e conta NSS**: especifique qual opção de cobrança você gostaria de usar com este sistema e, em seguida, especifique uma conta do site de suporte da NetApp :
   - "Saiba mais sobre as opções de licenciamento do Cloud Volumes ONTAP"
   - "Aprenda como configurar o licenciamento"
9. **Pacotes pré-configurados**: selecione um dos pacotes para implantar rapidamente um sistema Cloud Volumes ONTAP ou clique em **Criar minha própria configuração**. Os pacotes pré-configurados variam de acordo com a versão do Cloud Volumes ONTAP selecionada. Por exemplo, para Cloud Volumes ONTAP 9.18.1 e versões posteriores, o Console exibe pacotes com VMs C3, incluindo discos Hyperdisk Balanced. Você pode modificar as configurações, como parâmetros de IOPS e throughput, com base nas necessidades da sua carga de trabalho.

   Se você escolher um dos pacotes, precisará apenas especificar um volume e depois revisar e aprovar a configuração.
10. **Licenciamento**: Altere a versão do Cloud Volumes ONTAP conforme necessário e selecione um tipo de máquina.

    Se uma versão mais recente de Release Candidate, Disponibilidade Geral ou patch estiver disponível para uma versão selecionada, o Console atualizará o sistema para essa versão ao criá-la. Por exemplo, a atualização ocorre se você selecionar Cloud Volumes ONTAP 9.13.1 e 9.13.1 P4 estiver disponível. A atualização não ocorre de uma versão para outra — por exemplo, da 9.13 para a 9.14.
11. **Recursos de armazenamento subjacentes**: escolha as configurações para o agregado inicial: um tipo de disco e o tamanho de cada disco.

    O tipo de disco é para o volume inicial. Você pode escolher um tipo de disco diferente para volumes subsequentes.

    O tamanho do disco é para todos os discos no agregado inicial e para quaisquer agregados adicionais que o Console cria quando você usa a opção de provisionamento simples. Você pode criar agregados que usam um tamanho de disco diferente usando a opção de alocação avançada.

    Para obter ajuda na escolha do tipo e tamanho do disco, consulte"Dimensione seu sistema no Google Cloud" .

12. **Flash Cache, Velocidade de Gravação e WORM**:

    a. Ative o **Flash Cache** ou escolha a velocidade de gravação **Normal** ou **Alta** se necessário.

    Saiba mais sobre "Cache Flash" e "velocidade de escrita".

    > Alta velocidade de gravação e uma unidade máxima de transmissão (MTU) maior de 8.896 bytes estão disponíveis por meio da opção de velocidade de gravação **Alta**. Além disso, a MTU mais alta de 8.896 exige a seleção de VPC-1, VPC-2 e VPC-3 para a implantação. Para obter mais informações sobre VPC-1, VPC-2 e VPC-3, consulte "Regras para VPC-1, VPC-2 e VPC-3" .

    b. Ative o armazenamento WORM (escreva uma vez e leia muitas vezes), se desejar.

    O WORM não pode ser habilitado se a hierarquização de dados estiver habilitada para as versões 9.7 e anteriores do Cloud Volumes ONTAP . A reversão ou o downgrade para o Cloud Volumes ONTAP 9.8 é bloqueado após a ativação do WORM e da hierarquização.

    "Saiba mais sobre o armazenamento WORM" .

    a. Se você ativar o armazenamento WORM, selecione o período de retenção.

13. **Classificação de dados em camadas no Google Cloud Platform**: escolha se deseja habilitar a classificação de dados em camadas no agregado inicial, escolha uma classe de armazenamento para os dados em camadas e, em seguida, selecione uma conta de serviço que tenha a função de administrador de armazenamento predefinida (necessária para o Cloud Volumes ONTAP 9.7 ou posterior) ou selecione uma conta do Google Cloud (necessária para o Cloud Volumes ONTAP 9.6).

    Observe o seguinte:

    - O Console define a conta de serviço na instância do Cloud Volumes ONTAP . Esta conta de serviço fornece permissões para hierarquização de dados para um bucket do Google Cloud Storage. Certifique-se de adicionar a conta de serviço do agente do Console como um usuário da conta de serviço em camadas; caso contrário, você não poderá selecioná-la no Console.
    - Para obter ajuda na adição de uma conta do Google Cloud, consulte "Configurando e adicionando contas do Google Cloud para camadas de dados com 9.6" .
    - Você pode escolher uma política específica de níveis de volume ao criar ou editar um volume.
    - Se você desativar o tiering de dados, poderá ativá-lo em agregados subsequentes, mas precisará desligar o sistema e adicionar uma conta de serviço no Google Cloud Console.

    "Saiba mais sobre camadas de dados" .

14. **Criar volume**: insira detalhes para o novo volume ou clique em **Ignorar**.

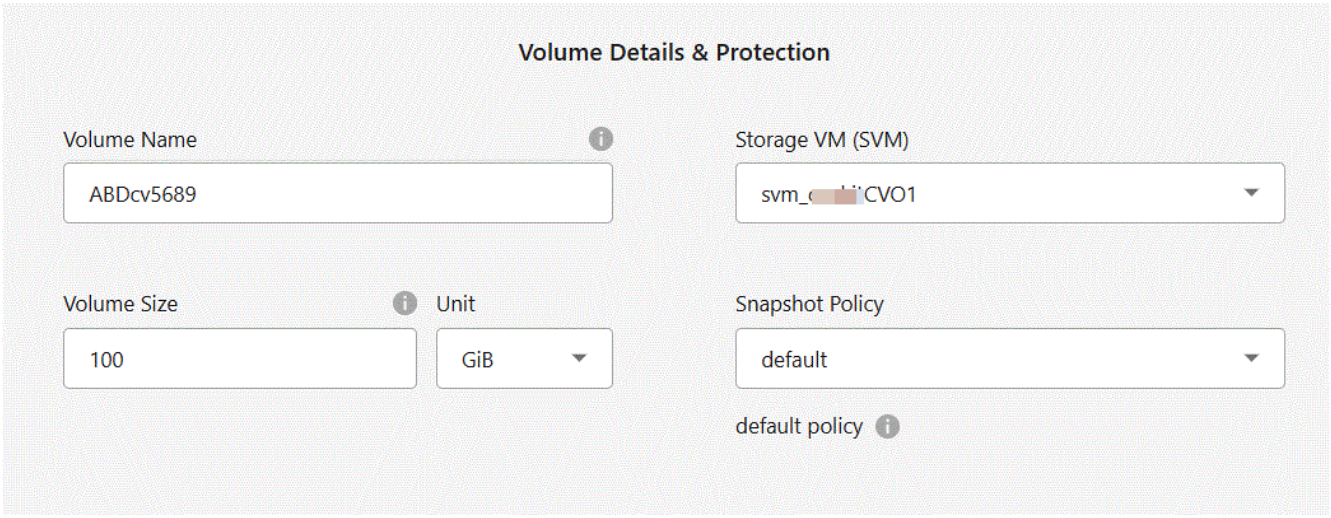
    "Saiba mais sobre os protocolos e versões de clientes suportados" .

    Alguns campos nesta página são autoexplicativos. A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Tamanho	O tamanho máximo que você pode inserir depende muito se você habilita o provisionamento fino, que permite criar um volume maior que o armazenamento físico disponível atualmente.

Campo	Descrição
Controle de acesso (somente para NFS)	Uma política de exportação define os clientes na sub-rede que podem acessar o volume. Por padrão, o Console insere um valor que fornece acesso a todas as instâncias na sub-rede.
Permissões e usuários/grupos (somente para CIFS)	Esses campos permitem que você controle o nível de acesso a um compartilhamento para usuários e grupos (também chamados de listas de controle de acesso ou ACLs). Você pode especificar usuários ou grupos locais ou de domínio do Windows, ou usuários ou grupos do UNIX. Se você especificar um nome de usuário de domínio do Windows, deverá incluir o domínio do usuário usando o formato domínio\nome de usuário.
Política de Snapshot	Uma política de cópia de instantâneo especifica a frequência e o número de cópias de instantâneo do NetApp criadas automaticamente. Uma cópia do NetApp Snapshot é uma imagem do sistema de arquivos de um momento específico que não tem impacto no desempenho e requer armazenamento mínimo. Você pode escolher a política padrão ou nenhuma. Você pode escolher nenhum para dados transitórios: por exemplo, tempdb para Microsoft SQL Server.
Opções avançadas (somente para NFS)	Selecione uma versão do NFS para o volume: NFSv3 ou NFSv4.
Grupo iniciador e IQN (somente para iSCSI)	Os destinos de armazenamento iSCSI são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Os grupos de iniciadores são tabelas de nomes de nós de host iSCSI e controlam quais iniciadores têm acesso a quais LUNs. Os destinos iSCSI se conectam à rede por meio de adaptadores de rede Ethernet padrão (NICs), placas de mecanismo de descarregamento TCP (TOE) com iniciadores de software, adaptadores de rede convergentes (CNAs) ou adaptadores de bust de host dedicados (HBAs) e são identificados por nomes qualificados iSCSI (IQNs). Quando você cria um volume iSCSI, o Console cria automaticamente um LUN para você. Simplificamos criando apenas um LUN por volume, portanto não há gerenciamento envolvido. Depois de criar o volume,"use o IQN para conectar-se ao LUN de seus hosts" .

A imagem a seguir mostra a primeira página do assistente de criação de volume:



15. **Configuração CIFS**: Se você escolher o protocolo CIFS, configure um servidor CIFS.

Campo	Descrição
Endereço IP primário e secundário do DNS	Os endereços IP dos servidores DNS que fornecem resolução de nomes para o servidor CIFS. Os servidores DNS listados devem conter os registros de localização de serviço (SRV) necessários para localizar os servidores LDAP do Active Directory e os controladores de domínio para o domínio ao qual o servidor CIFS se juntará. Se você estiver configurando o Google Managed Active Directory, o AD poderá ser acessado por padrão com o endereço IP 169.254.169.254.
Domínio do Active Directory para ingressar	O FQDN do domínio do Active Directory (AD) ao qual você deseja que o servidor CIFS ingresse.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com privilégios suficientes para adicionar computadores à Unidade Organizacional (UO) especificada dentro do domínio do AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio do AD.
Unidade Organizacional	A unidade organizacional dentro do domínio do AD a ser associada ao servidor CIFS. O padrão é CN=Computadores. Para configurar o Google Managed Microsoft AD como o servidor AD para o Cloud Volumes ONTAP, insira **OU=Computers,OU=Cloud** neste campo.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Documentação do Google Cloud: Unidades organizacionais no Google Managed Microsoft AD"^]
Domínio DNS	O domínio DNS para a máquina virtual de armazenamento (SVM) do Cloud Volumes ONTAP . Na maioria dos casos, o domínio é o mesmo que o domínio do AD.
Servidor NTP	Selecione **Usar domínio do Active Directory** para configurar um servidor NTP usando o DNS do Active Directory. Se você precisar configurar um servidor NTP usando um endereço diferente, use a API. Para obter informações, consulte o "Documentação de automação do NetApp Console" para mais detalhes. Observe que você só pode configurar um servidor NTP ao criar um servidor CIFS. Não é configurável depois de criar o servidor CIFS.

16. **Perfil de uso, tipo de disco e política de camadas**: escolha se deseja habilitar recursos de eficiência de armazenamento e alterar a política de camadas de volume, se necessário.

    Para mais informações, consulte"Escolha um perfil de uso de volume" ,"Visão geral da hierarquização de dados" , e "KB: Quais recursos de eficiência de armazenamento em linha são suportados pelo CVO?"

17. **Revisar e aprovar**: revise e confirme suas seleções.
    a. Revise os detalhes sobre a configuração.
    b. Clique em **Mais informações** para revisar detalhes sobre o suporte e os recursos do Google Cloud que o Console comprará.
    c. Selecione as caixas de seleção **Eu entendo…**.
    d. Clique em **Ir**.

Resultado

O Console implanta o sistema Cloud Volumes ONTAP . Você pode acompanhar o progresso na página **Auditoria**.

Se você tiver algum problema ao implantar o sistema Cloud Volumes ONTAP , revise a mensagem de falha. Você também pode selecionar o sistema e clicar em **Recriar ambiente**.

Para obter ajuda adicional, acesse "Suporte NetApp Cloud Volumes ONTAP" .

Depois que você terminar

- Se você provisionou um compartilhamento CIFS, conceda aos usuários ou grupos permissões para os arquivos e pastas e verifique se esses usuários podem acessar o compartilhamento e criar um arquivo.
- Se você quiser aplicar cotas aos volumes, use o ONTAP System Manager ou o ONTAP CLI.

  As cotas permitem que você restrinja ou rastreie o espaço em disco e o número de arquivos usados por um usuário, grupo ou qtree.

> Após a conclusão do processo de implantação, não modifique as configurações do Cloud Volumes ONTAP geradas pelo sistema no portal do Google Cloud, como as tags do sistema e os rótulos definidos nos recursos do Google Cloud. Quaisquer alterações feitas nessas configurações podem levar a comportamentos inesperados ou perda de dados.

Inicie um par de HA no Google Cloud

Crie um sistema no Console para iniciar o Cloud Volumes ONTAP no Google Cloud.

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique em **Armazenamento > Sistema** e siga as instruções.
3. **Escolha um local**: Selecione **Google Cloud** e * Cloud Volumes ONTAP HA*.
4. **Detalhes e credenciais**: selecione um projeto, especifique um nome de cluster, opcionalmente selecione uma conta de serviço, opcionalmente adicione rótulos e, em seguida, especifique as credenciais.

   A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Nome do sistema	O Console usa o nome do sistema para nomear o sistema Cloud Volumes ONTAP e a instância da VM do Google Cloud. Ele também usa o nome como prefixo para o grupo de segurança predefinido, se você selecionar essa opção.
Nome da conta de serviço	Se você planeja usar o"NetApp Cloud Tiering" ou "Backup e Recuperação" serviços, você precisa habilitar a opção **Conta de serviço** e então selecionar a Conta de serviço que tem a função de administrador de armazenamento predefinida.
Adicionar rótulos	Os rótulos são metadados para seus recursos do Google Cloud. O Console adiciona os rótulos ao sistema Cloud Volumes ONTAP e aos recursos do Google Cloud associados ao sistema. Você pode adicionar até quatro rótulos na interface do usuário ao criar um sistema e depois adicionar mais depois que ele for criado. Observe que a API não limita você a quatro rótulos ao criar um sistema. Para obter informações sobre rótulos, consulte "Documentação do Google Cloud: Rotulagem de recursos" .

Campo	Descrição
Nome de usuário e senha	Estas são as credenciais para a conta de administrador do cluster Cloud Volumes ONTAP . Você pode usar essas credenciais para se conectar ao Cloud Volumes ONTAP por meio do ONTAP System Manager ou do ONTAP CLI. Mantenha o nome de usuário padrão *admin* ou altere-o para um nome de usuário personalizado.
Editar Projeto	Selecione o projeto onde você deseja que o Cloud Volumes ONTAP resida. O projeto padrão é o projeto do Console. Se você não vir nenhum projeto adicional na lista suspensa, significa que ainda não associou a conta de serviço a outros projetos. Vá para o Google Cloud Console, abra o serviço IAM e selecione o projeto. Adicione a conta de serviço com a função que você usa para o Console a esse projeto. Você precisará repetir esta etapa para cada projeto. Esta é a conta de serviço que você configurou para o Console,"conforme descrito nesta página" . Clique em **Adicionar assinatura** para associar as credenciais selecionadas a uma assinatura. Para criar um sistema Cloud Volumes ONTAP com pagamento conforme o uso, você precisa selecionar um projeto do Google Cloud associado a uma assinatura do Cloud Volumes ONTAP no Google Cloud Marketplace. Consulte "Associando uma assinatura do marketplace às credenciais do Google Cloud" .

5. **Serviços**: Selecione os serviços que você deseja usar neste sistema. Para selecionar Backup e Recuperação ou usar o NetApp Cloud Tiering, você deve ter especificado a Conta de Serviço na etapa 3.

   Se você quiser utilizar WORM e camadas de dados, desabilite o Backup e Recuperação e implante um sistema Cloud Volumes ONTAP com versão 9.8 ou superior.

6. **Modelos de implantação de alta disponibilidade**: escolha várias zonas (recomendado) ou uma única zona para a configuração de alta disponibilidade. Em seguida, selecione uma região e uma zona.

   "Saiba mais sobre modelos de implantação de HA" .

7. **Conectividade**: Selecione quatro VPCs diferentes para a configuração de HA, uma sub-rede em cada VPC e, em seguida, escolha uma política de firewall.

   "Saiba mais sobre os requisitos de rede" .

   A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Política gerada	Se você deixar o Console gerar a política de firewall para você, precisará escolher como permitirá o tráfego: • Se você escolher **Somente VPC selecionada**, o filtro de origem para tráfego de entrada será o intervalo de sub-rede da VPC selecionada e o intervalo de sub-rede da VPC onde o agente do Console reside. Esta é a opção recomendada. • Se você escolher **Todas as VPCs**, o filtro de origem para o tráfego de entrada será o intervalo de IP 0.0.0.0/0.
Use existente	Se você usar uma política de firewall existente, certifique-se de que ela inclua as regras necessárias. "Saiba mais sobre as regras de firewall para o Cloud Volumes ONTAP" .

8. **Métodos de cobrança e conta NSS**: especifique qual opção de cobrança você gostaria de usar com este sistema e, em seguida, especifique uma conta do site de suporte da NetApp .
   - "Saiba mais sobre as opções de licenciamento do Cloud Volumes ONTAP" .
   - "Aprenda como configurar o licenciamento" .
9. **Pacotes pré-configurados**: selecione um dos pacotes para implantar rapidamente um sistema Cloud Volumes ONTAP ou clique em **Criar minha própria configuração**.

   Se você escolher um dos pacotes, precisará apenas especificar um volume e depois revisar e aprovar a configuração.

10. **Licenciamento**: Altere a versão do Cloud Volumes ONTAP conforme necessário e selecione um tipo de máquina.

    Se uma versão mais recente de Release Candidate, Disponibilidade Geral ou patch estiver disponível para a versão selecionada, o Console atualizará o sistema para essa versão ao criá-la. Por exemplo, a atualização ocorre se você selecionar Cloud Volumes ONTAP 9.13.1 e 9.13.1 P4 estiver disponível. A atualização não ocorre de uma versão para outra, por exemplo, da 9.13 para a 9.14.

11. **Recursos de armazenamento subjacentes**: escolha as configurações para o agregado inicial: um tipo de disco e o tamanho de cada disco.

    O tipo de disco é para o volume inicial. Você pode escolher um tipo de disco diferente para volumes subsequentes.

    O tamanho do disco é para todos os discos no agregado inicial e para quaisquer agregados adicionais que o Console cria quando você usa a opção de provisionamento simples. Você pode criar agregados que usam um tamanho de disco diferente usando a opção de alocação avançada.

    Para obter ajuda na escolha do tipo e tamanho do disco, consulte"Dimensione seu sistema no Google Cloud" .

12. **Flash Cache, Velocidade de Gravação e WORM**:

    a. Ative o **Flash Cache** ou escolha a velocidade de gravação **Normal** ou **Alta** se necessário.

Saiba mais sobre "Cache Flash" e "velocidade de escrita".

> Alta velocidade de gravação e uma unidade máxima de transmissão (MTU) maior de 8.896 bytes estão disponíveis por meio da opção de velocidade de gravação **Alta** com os tipos de instância n2-standard-16, n2-standard-32, n2-standard-48 e n2-standard-64. Além disso, a MTU mais alta de 8.896 exige a seleção de VPC-1, VPC-2 e VPC-3 para a implantação. Alta velocidade de gravação e uma MTU de 8.896 dependem do recurso e não podem ser desabilitadas individualmente em uma instância configurada. Para obter mais informações sobre VPC-1, VPC-2 e VPC-3, consulte "Regras para VPC-1, VPC-2 e VPC-3" .

b. Ative o armazenamento WORM (escreva uma vez e leia muitas vezes), se desejar.

   O WORM não pode ser habilitado se a hierarquização de dados estiver habilitada para as versões 9.7 e anteriores do Cloud Volumes ONTAP . A reversão ou o downgrade para o Cloud Volumes ONTAP 9.8 é bloqueado após a ativação do WORM e da hierarquização.

"Saiba mais sobre o armazenamento WORM" .

a. Se você ativar o armazenamento WORM, selecione o período de retenção.

13. **Classificação de dados no Google Cloud**: escolha se deseja habilitar a classificação de dados no agregado inicial, escolha uma classe de armazenamento para os dados em camadas e, em seguida, selecione uma conta de serviço que tenha a função predefinida de Administrador de armazenamento.

    Observe o seguinte:

    - O Console define a conta de serviço na instância do Cloud Volumes ONTAP . Esta conta de serviço fornece permissões para hierarquização de dados para um bucket do Google Cloud Storage. Certifique-se de adicionar a conta de serviço do agente do Console como um usuário da conta de serviço em camadas; caso contrário, você não poderá selecioná-la no Console.
    - Você pode escolher uma política específica de níveis de volume ao criar ou editar um volume.
    - Se você desativar o tiering de dados, poderá ativá-lo em agregados subsequentes, mas precisará desligar o sistema e adicionar uma conta de serviço no Google Cloud Console.

    "Saiba mais sobre camadas de dados" .

14. **Criar volume**: insira detalhes para o novo volume ou clique em **Ignorar**.

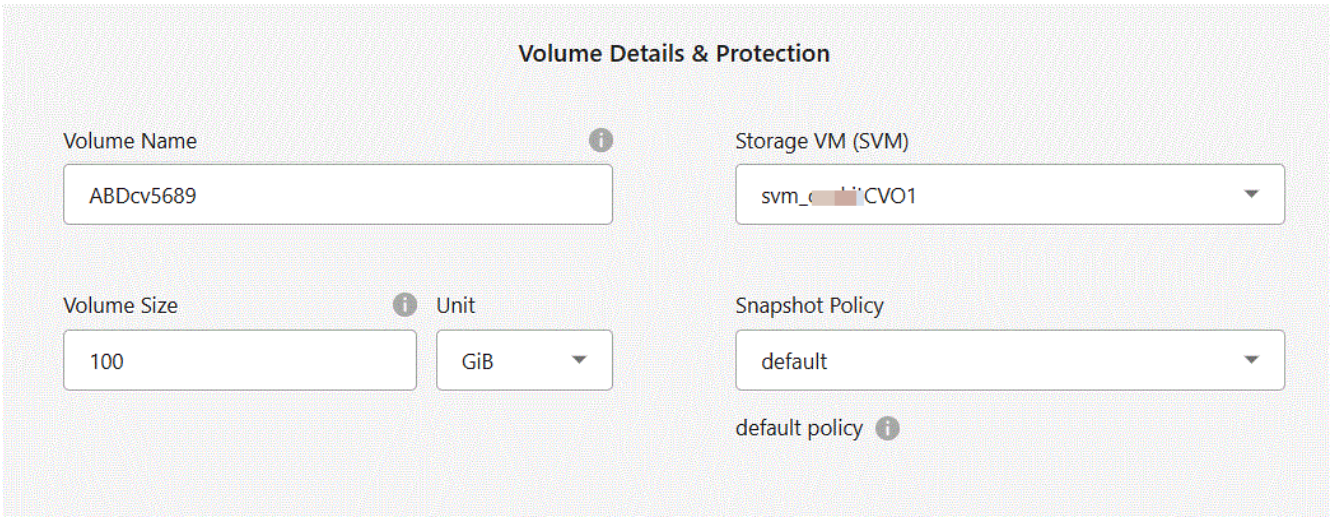
    "Saiba mais sobre os protocolos e versões de clientes suportados" .

    Alguns campos nesta página são autoexplicativos. A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Tamanho	O tamanho máximo que você pode inserir depende muito se você habilita o provisionamento fino, que permite criar um volume maior que o armazenamento físico disponível atualmente.
Controle de acesso (somente para NFS)	Uma política de exportação define os clientes na sub-rede que podem acessar o volume. Por padrão, o Console insere um valor que fornece acesso a todas as instâncias na sub-rede.

Campo	Descrição
Permissões e usuários/grupos (somente para CIFS)	Esses campos permitem que você controle o nível de acesso a um compartilhamento para usuários e grupos (também chamados de listas de controle de acesso ou ACLs). Você pode especificar usuários ou grupos locais ou de domínio do Windows, ou usuários ou grupos do UNIX. Se você especificar um nome de usuário de domínio do Windows, deverá incluir o domínio do usuário usando o formato domínio\nome de usuário.
Política de Snapshot	Uma política de cópia de instantâneo especifica a frequência e o número de cópias de instantâneo do NetApp criadas automaticamente. Uma cópia do NetApp Snapshot é uma imagem do sistema de arquivos de um momento específico que não tem impacto no desempenho e requer armazenamento mínimo. Você pode escolher a política padrão ou nenhuma. Você pode escolher nenhum para dados transitórios: por exemplo, tempdb para Microsoft SQL Server.
Opções avançadas (somente para NFS)	Selecione uma versão do NFS para o volume: NFSv3 ou NFSv4.
Grupo iniciador e IQN (somente para iSCSI)	Os destinos de armazenamento iSCSI são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Os grupos de iniciadores são tabelas de nomes de nós de host iSCSI e controlam quais iniciadores têm acesso a quais LUNs. Os destinos iSCSI se conectam à rede por meio de adaptadores de rede Ethernet padrão (NICs), placas de mecanismo de descarregamento TCP (TOE) com iniciadores de software, adaptadores de rede convergentes (CNAs) ou adaptadores de bust de host dedicados (HBAs) e são identificados por nomes qualificados iSCSI (IQNs). Quando você cria um volume iSCSI, o Console cria automaticamente um LUN para você. Simplificamos criando apenas um LUN por volume, portanto não há gerenciamento envolvido. Depois de criar o volume,"use o IQN para conectar-se ao LUN de seus hosts" .

A imagem a seguir mostra a primeira página do assistente de criação de volume:



15. **Configuração CIFS**: Se você escolher o protocolo CIFS, configure um servidor CIFS.

Campo	Descrição
Endereço IP primário e secundário do DNS	Os endereços IP dos servidores DNS que fornecem resolução de nomes para o servidor CIFS. Os servidores DNS listados devem conter os registros de localização de serviço (SRV) necessários para localizar os servidores LDAP do Active Directory e os controladores de domínio para o domínio ao qual o servidor CIFS se juntará. Se você estiver configurando o Google Managed Active Directory, o AD poderá ser acessado por padrão com o endereço IP 169.254.169.254.
Domínio do Active Directory para ingressar	O FQDN do domínio do Active Directory (AD) ao qual você deseja que o servidor CIFS ingresse.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com privilégios suficientes para adicionar computadores à Unidade Organizacional (UO) especificada dentro do domínio do AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio do AD.
Unidade Organizacional	A unidade organizacional dentro do domínio do AD a ser associada ao servidor CIFS. O padrão é CN=Computadores. Para configurar o Google Managed Microsoft AD como o servidor AD para o Cloud Volumes ONTAP, insira **OU=Computers,OU=Cloud** neste campo.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Documentação do Google Cloud: Unidades organizacionais no Google Managed Microsoft AD"^]
Domínio DNS	O domínio DNS para a máquina virtual de armazenamento (SVM) do Cloud Volumes ONTAP . Na maioria dos casos, o domínio é o mesmo que o domínio do AD.
Servidor NTP	Selecione **Usar domínio do Active Directory** para configurar um servidor NTP usando o DNS do Active Directory. Se você precisar configurar um servidor NTP usando um endereço diferente, use a API. Consulte o "Documentação de automação do NetApp Console" para mais detalhes. Observe que você só pode configurar um servidor NTP ao criar um servidor CIFS. Não é configurável depois de criar o servidor CIFS.

16. **Perfil de uso, tipo de disco e política de camadas**: escolha se deseja habilitar recursos de eficiência de armazenamento e alterar a política de camadas de volume, se necessário.

    Para mais informações, consulte"Escolha um perfil de uso de volume" ,"Visão geral da hierarquização de dados" , e "KB: Quais recursos de eficiência de armazenamento em linha são suportados pelo CVO?"

17. **Revisar e aprovar**: revise e confirme suas seleções.
    a. Revise os detalhes sobre a configuração.
    b. Clique em **Mais informações** para revisar detalhes sobre o suporte e os recursos do Google Cloud que o Console comprará.
    c. Selecione as caixas de seleção **Eu entendo…**.
    d. Clique em **Ir**.

Resultado

O Console implanta o sistema Cloud Volumes ONTAP . Você pode acompanhar o progresso na página **Auditoria**.

Se você tiver algum problema ao implantar o sistema Cloud Volumes ONTAP , revise a mensagem de falha. Você também pode selecionar o sistema e clicar em **Recriar ambiente**.

Para obter ajuda adicional, acesse "Suporte NetApp Cloud Volumes ONTAP" .

Depois que você terminar

- Se você provisionou um compartilhamento CIFS, conceda aos usuários ou grupos permissões para os arquivos e pastas e verifique se esses usuários podem acessar o compartilhamento e criar um arquivo.
- Se você quiser aplicar cotas aos volumes, use o ONTAP System Manager ou o ONTAP CLI.

  As cotas permitem que você restrinja ou rastreie o espaço em disco e o número de arquivos usados por um usuário, grupo ou qtree.

Após a conclusão do processo de implantação, não modifique as configurações do Cloud Volumes ONTAP geradas pelo sistema no portal do Google Cloud, como as tags do sistema e os rótulos definidos nos recursos do Google Cloud. Quaisquer alterações feitas nessas configurações podem levar a comportamentos inesperados ou perda de dados.

Links relacionados

- "Planejando sua configuração do Cloud Volumes ONTAP no Google Cloud"

Verificação de imagem da plataforma Google Cloud

Saiba como a imagem do Google Cloud é verificada no Cloud Volumes ONTAP

A verificação de imagem do Google Cloud está em conformidade com os requisitos de segurança aprimorados da NetApp . Foram feitas alterações no script que gera as imagens para assiná-las ao longo do caminho usando chaves privadas geradas especificamente para essa tarefa. Você pode verificar a integridade da imagem do Google Cloud usando o resumo assinado e o certificado público do Google Cloud, que podem ser baixados via "NSS" para um lançamento específico.

A verificação de imagens do Google Cloud é compatível com o software Cloud Volumes ONTAP versão 9.13.0 ou superior.

Converter imagem do Google Cloud para formato bruto para Cloud Volumes ONTAP

A imagem que está sendo usada para implantar novas instâncias, atualizações ou que está sendo usada em imagens existentes será compartilhada com os clientes por meio de "o site de suporte da NetApp (NSS)" . O resumo assinado e os certificados estarão disponíveis para download no portal do NSS. Certifique-se de que você está baixando o resumo e os certificados para a versão correta correspondente à imagem compartilhada pelo Suporte da NetApp . Por exemplo, imagens 9.13.0 terão um resumo assinado 9.13.0 e certificados disponíveis no NSS.

Por que essa etapa é necessária?

As imagens do Google Cloud não podem ser baixadas diretamente. Para verificar a imagem em relação ao resumo assinado e aos certificados, você precisa ter um mecanismo para comparar os dois arquivos e baixar

a imagem. Para fazer isso, você deve exportar/converter a imagem para o formato disk.raw e salvar os resultados em um bucket de armazenamento no Google Cloud. O arquivo disk.raw é compactado em tar e gzip no processo.

A conta de usuário/serviço precisará de privilégios para executar o seguinte:

- Acesso ao bucket de armazenamento do Google
- Gravar no bucket do Google Storage
- Criar trabalhos de criação de nuvem (usados durante o processo de exportação)
- Acesso à imagem desejada
- Criar tarefas de exportação de imagem

Para verificar a imagem, ela deve ser convertida para o formato disk.raw e depois baixada.

Use a linha de comando do Google Cloud para exportar a imagem do Google Cloud

A maneira preferida de exportar uma imagem para o Cloud Storage é usar o "comando gcloud compute images export" . Este comando pega a imagem fornecida e a converte em um arquivo disk.raw, que é tarado e compactado em gzip. O arquivo gerado é salvo na URL de destino e pode ser baixado para verificação.

O usuário/conta deve ter privilégios para acessar e gravar no bucket desejado, exportar a imagem e criar na nuvem (usado pelo Google para exportar a imagem) para executar esta operação.

Exportar imagem do Google Cloud usando gcloud

Clique para exibir

```
$ gcloud compute images export \
    --destination-uri DESTINATION_URI \
    --image IMAGE_NAME

# For our example:
$ gcloud compute images export \
    --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-
gcp-demo \
    --image example-user-20230120115139


## DEMO ##
# Step 1 - Optional: Checking access and listing objects in the
destination bucket
$ gsutil ls gs://example-user-export-image-bucket/

# Step 2 - Exporting the desired image to the bucket
$ gcloud compute images export --image example-user-export-image-demo
--destination-uri gs://example-user-export-image-bucket/export-
demo.tar.gz
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-
project/locations/us-central1/builds/xxxxxxxxxxxx].
Logs are available at [https://console.cloud.google.com/cloud-
build/builds;region=us-central1/xxxxxxxxxxxx?project=xxxxxxxxxxxx].
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-
export-image-demo" from project "example-demo-project".
[image-export]: 2023-01-25T18:13:49Z Validating workflow
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-
export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "setup-disks"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "run-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "wait-for-inst-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "copy-image-object"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "delete-inst"
[image-export]: 2023-01-25T18:13:51Z Validation Complete
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-
project
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

```
[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch:
["ExportFailed:"] (this is not an error), StatusMatch: "GCEExport:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
```

```
StatusMatch found: "GCEExport: <serial-output key:'source-size-gb'
value:'10'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Running export tool."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size
will most likely be much smaller."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Beginning export process..."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Copying \"/dev/sdb\" to gs://example-
demo-project-example-bkt-us/example-image-export-20230125-18:13:49-
r88px/outs/image-export-export-disk.tar.gz."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Using \"/root/upload\" as the buffer
prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Creating gzipped image of \"/dev/sdb\"."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec),
total written size: 992 MiB (198 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec),
total written size: 1.5 GiB (17 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished creating gzipped image of
\"/dev/sdb\" in 48.956433327s [213 MiB/s] with a compression ratio of
6."
```

```
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished export in  48.957347731s"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: <serial-output key:'target-size-gb'
value:'2'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
SuccessMatch found "ExportSuccess"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-
25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-
export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step
"delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk"
(IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-
size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-
size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning
up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z Workflow "image-export" finished
cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz


# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION
```

```
$ gcloud storage cp gs://example-user-export-image-bucket/export-
demo.tar.gz CVO_GCP_Signed_Digest.tar.gz
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to
file://CVO_GCP_Signed_Digest.tar.gz
  Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s

Average throughput: 213.3MiB/s
$ ls -l
total 1565036
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44
CVO_GCP_Signed_Digest.tar.gz
```

Extraia os arquivos compactados

```
# Extracting files from the digest
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```

Para obter mais informações sobre como exportar uma imagem por meio do Google Cloud, consulte o "Documento do Google Cloud sobre como exportar uma imagem" .

Verificação de assinatura de imagem

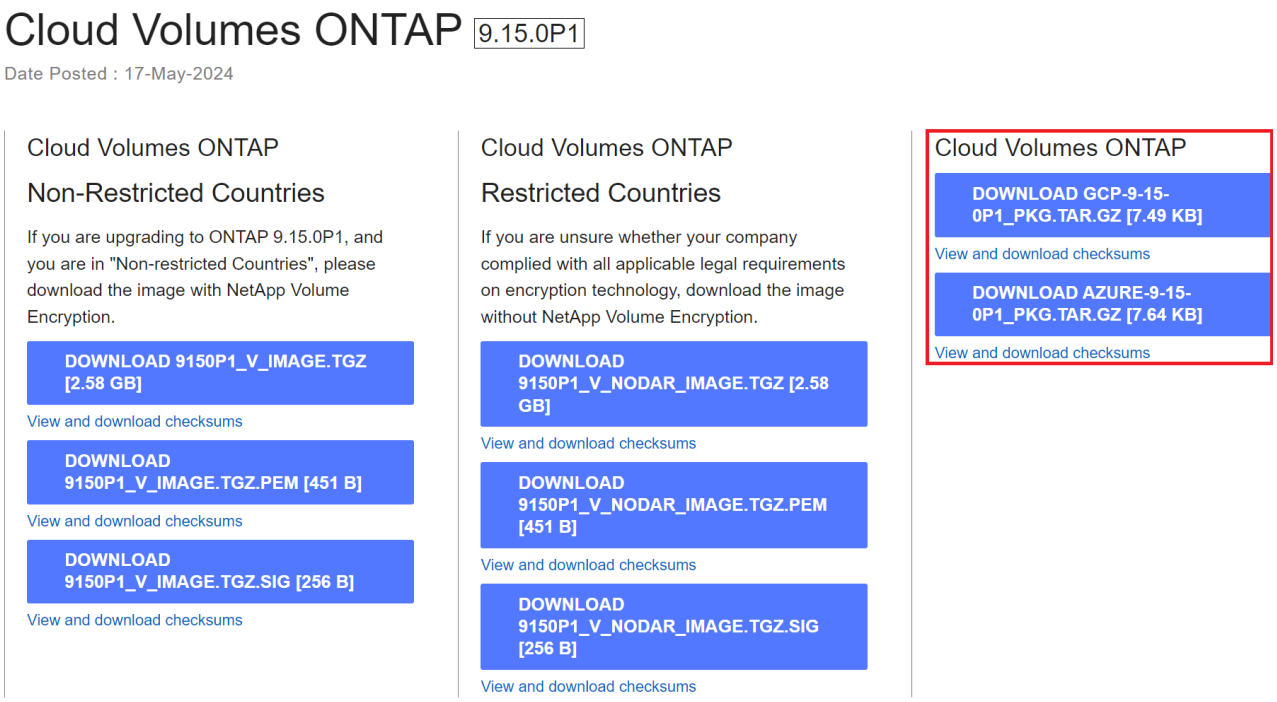
Verificação de assinatura de imagem do Google Cloud para Cloud Volumes ONTAP

Para verificar a imagem assinada do Google Cloud exportada, você deve baixar o arquivo de resumo da imagem do NSS para validar o arquivo disk.raw e o conteúdo do arquivo de resumo.

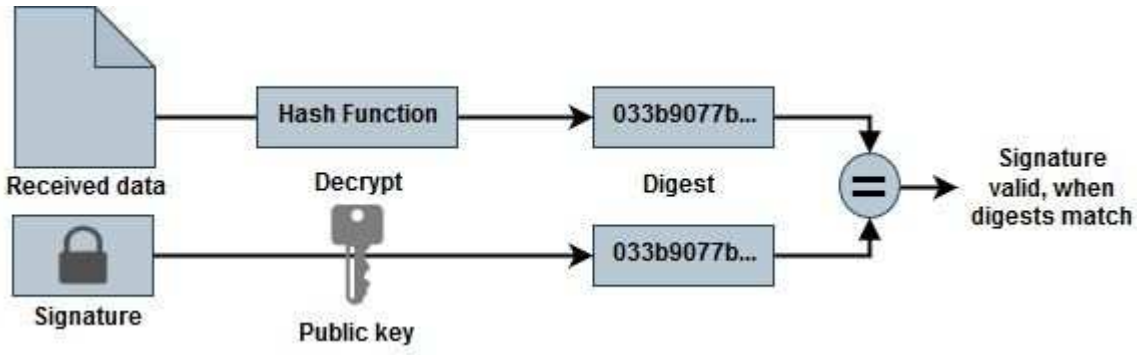
Resumo do fluxo de trabalho de verificação de imagem assinada

A seguir, uma visão geral do processo de fluxo de trabalho de verificação de imagem assinada do Google Cloud.

- Do "NSS" , baixe o arquivo do Google Cloud contendo os seguintes arquivos:
  - Resumo assinado (.sig)
  - Certificado contendo a chave pública (.pem)
  - Cadeia de certificados (.pem)



- Baixe o arquivo disk.raw convertido
- Validar o certificado usando a cadeia de certificados
- Valide o resumo assinado usando o certificado que contém a chave pública
  - Descriptografe o resumo assinado usando a chave pública para extrair o resumo do arquivo de imagem
  - Crie um resumo do arquivo disk.raw baixado
  - Compare os dois arquivos de resumo para validação



Verifique o arquivo disk.raw da imagem do Google Cloud para o Cloud Volumes ONTAP usando OpenSSL

Você pode verificar o arquivo disk.raw baixado pelo Google Cloud em relação ao conteúdo do arquivo de resumo disponível por meio do "NSS" usando OpenSSL.

Os comandos OpenSSL para validar a imagem são compatíveis com máquinas Linux, macOS e Windows.

Passos

1. Verifique o certificado usando OpenSSL.

Clique para exibir

```
# Step 1 - Optional, but recommended: Verify the certificate using
OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a
directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in <Certificate-
Chain.pem>)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OCSP request for the certificate
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -reqout req.der

# Step 1.4 - Optional: Check the new file "req.der" has been
generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OCSP Manager using openssl to send the
OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem  -url ${ocsp_url} -resp_text
-respout resp.der
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
    Produced At: Jan 19 15:14:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5
    Cert Status: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
         f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
         af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
         1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
         d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
         cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
         1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
         15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
         8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
         e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
         5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
         b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
         9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
         24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
         5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
         2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
         17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
         d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
         15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
         44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
         cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
         e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
         6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
         77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:
```

```
          e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
          22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
          38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
          fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
          bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK
```

2. Coloque o arquivo disk.raw baixado, a assinatura e os certificados em um diretório.
3. Extraia a chave pública do certificado usando OpenSSL.
4. Descriptografe a assinatura usando a chave pública extraída e verifique o conteúdo do arquivo disk.raw baixado.

Clique para exibir

```
# Step 1 - Place the downloaded disk.raw, the signature and the
certificates in a directory
$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) >
(public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-
0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and
verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature
(signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary
../sample_file.txt
Verification Failure
```

Informações sobre direitos autorais

Informações sobre marcas comerciais