Comece na Amazon Web Services

Cloud Volumes ONTAP

NetApp
February 13, 2026

Índice

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	

Informações da AWS	Seu valor
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

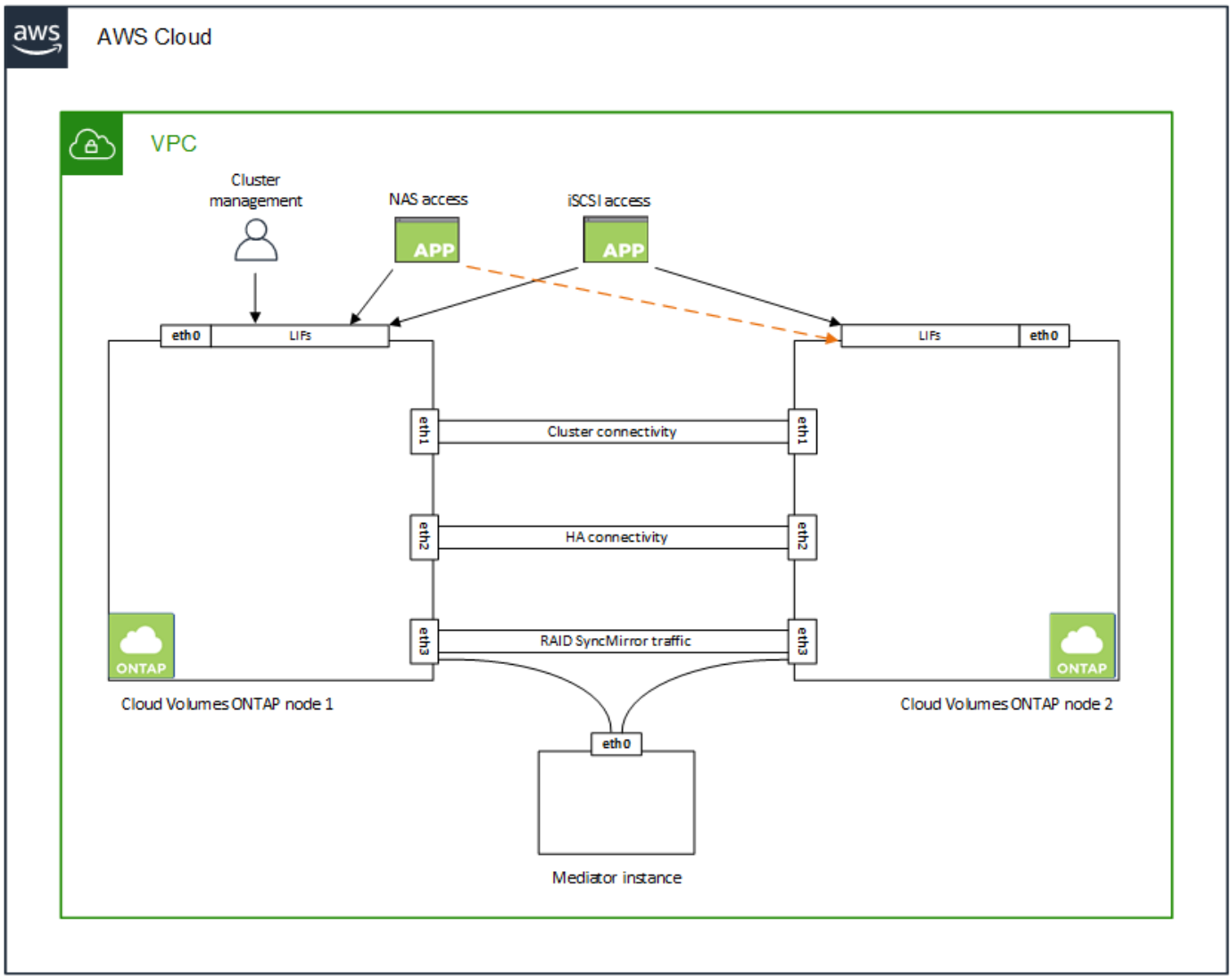
O Console aloca 6 endereços IP para um sistema de nó único.

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" .

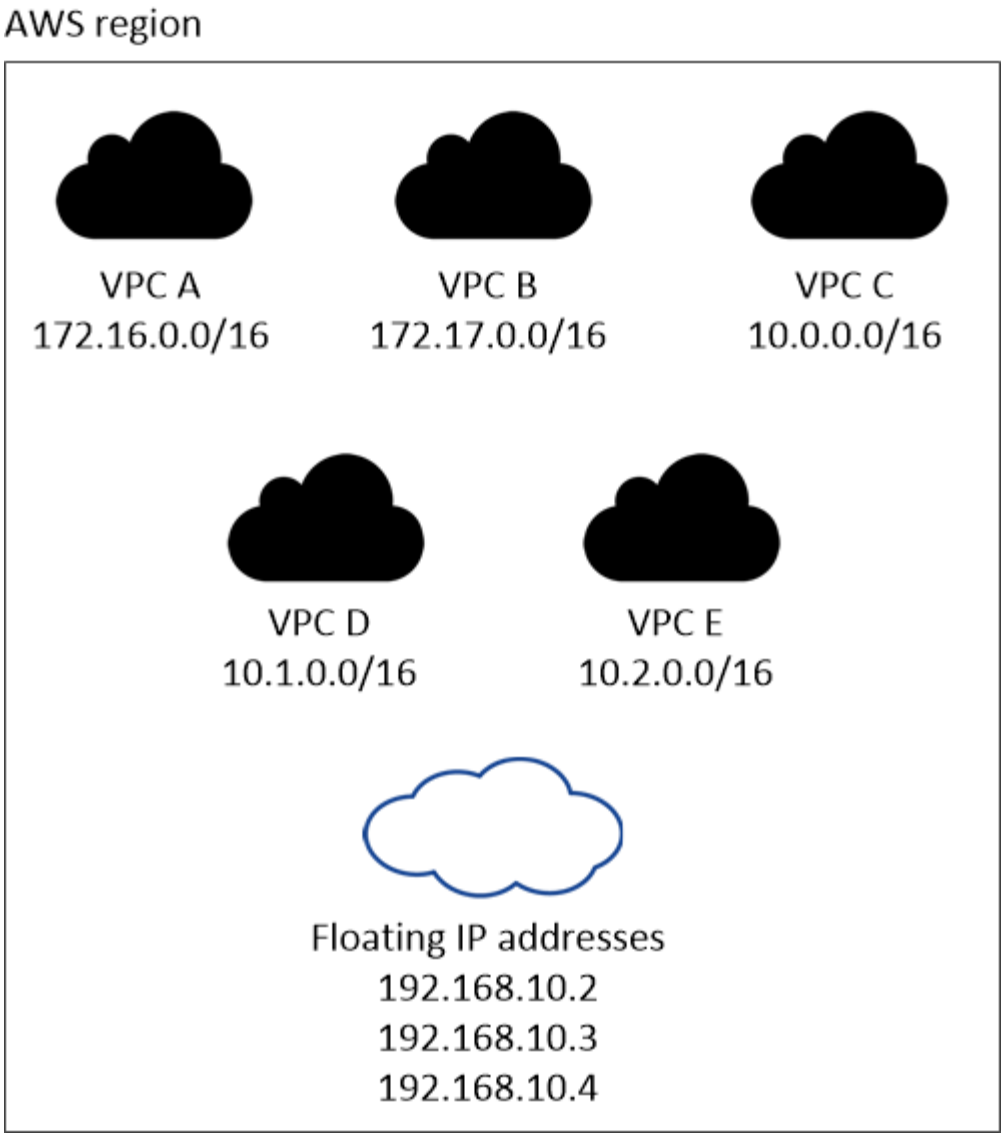
Um endereço IP flutuante é para gerenciamento de cluster, um é para dados NFS/CIFS no nó 1 e um é para dados NFS/CIFS no nó 2. Um quarto endereço IP flutuante para gerenciamento de SVM é opcional.

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" .

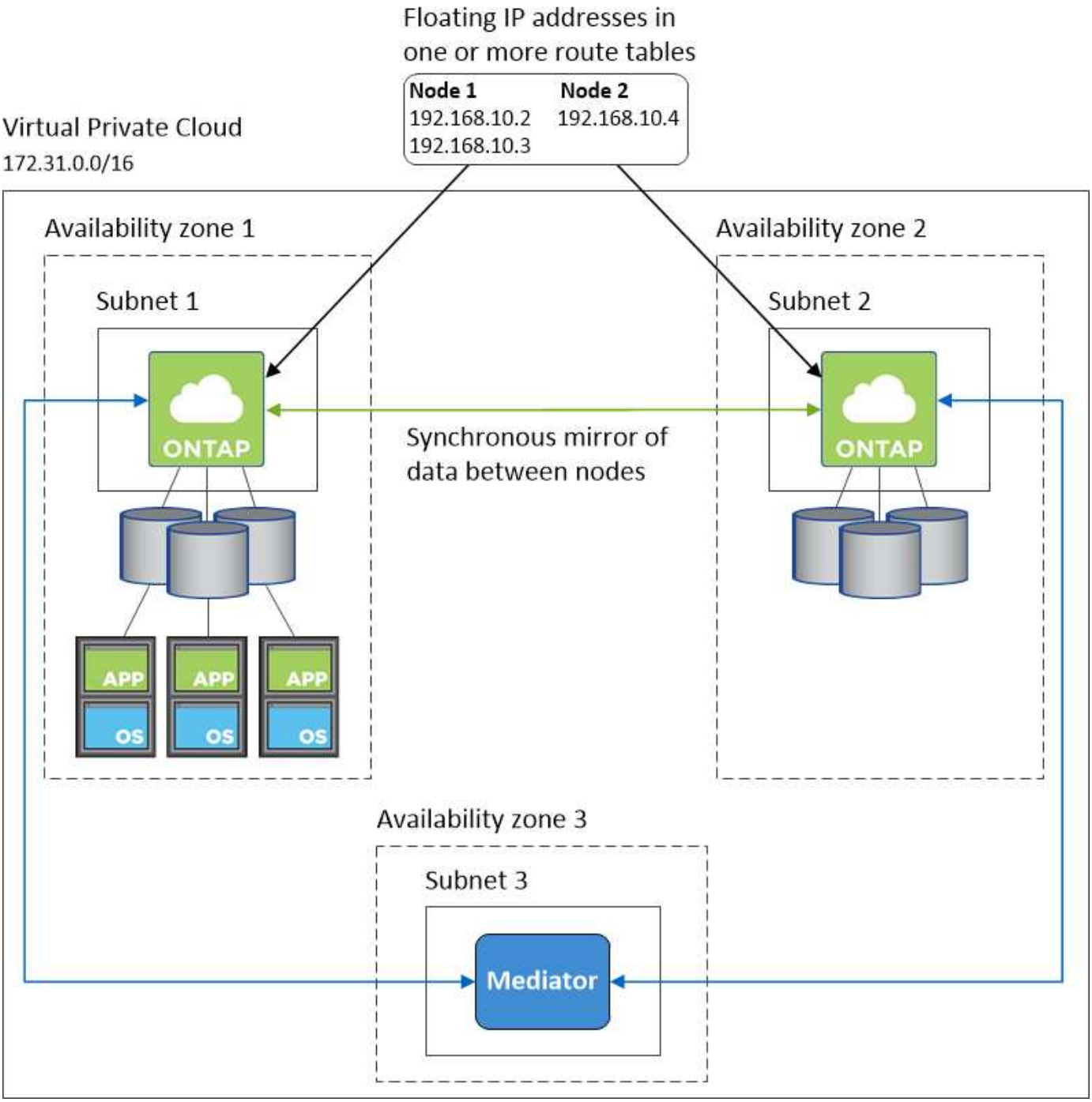
Conexão com ferramentas de gerenciamento da NetApp

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

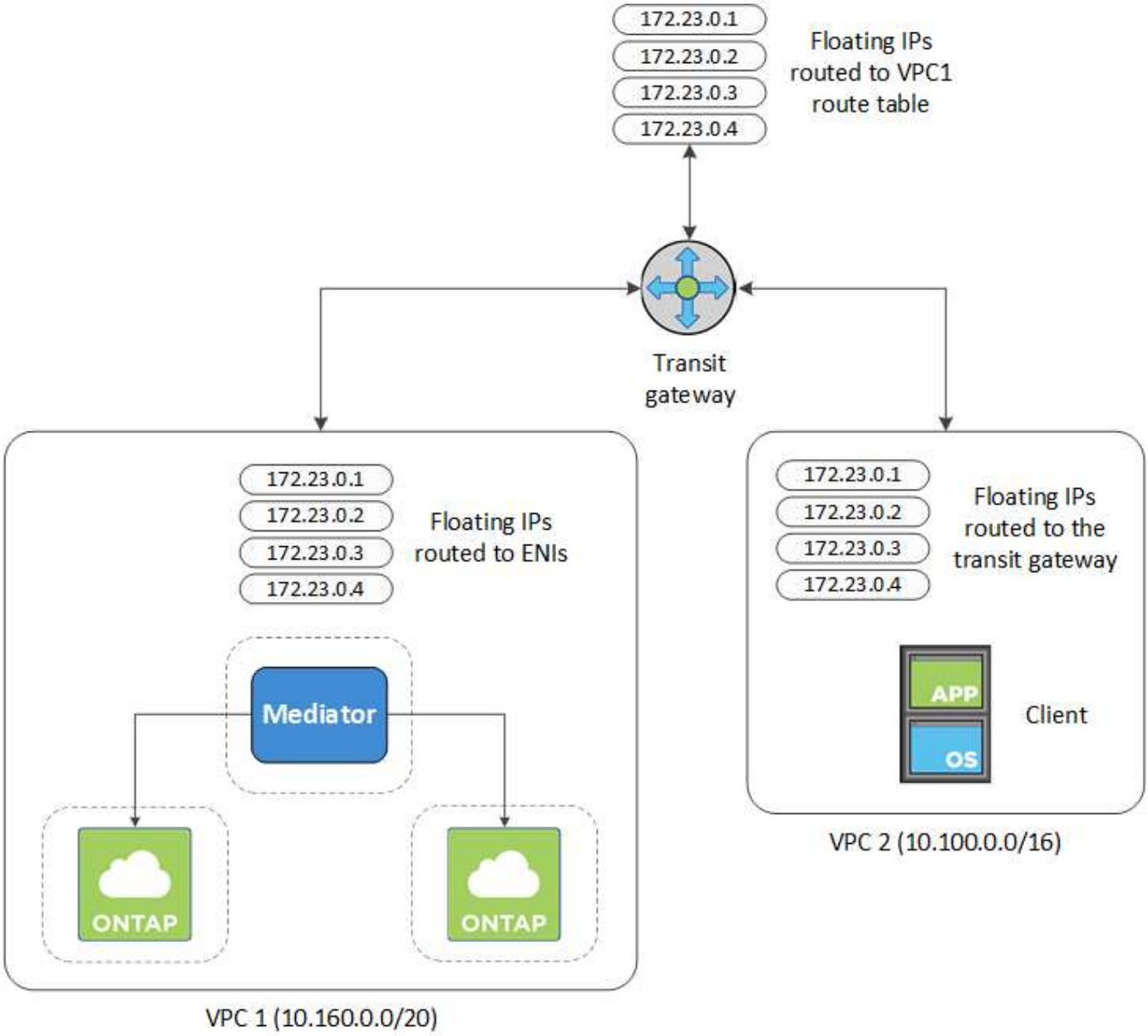
Configure um gateway de trânsito da AWS para permitir o acesso a um par de HA"endereços IP flutuantes" de fora da VPC onde o par HA reside.

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.

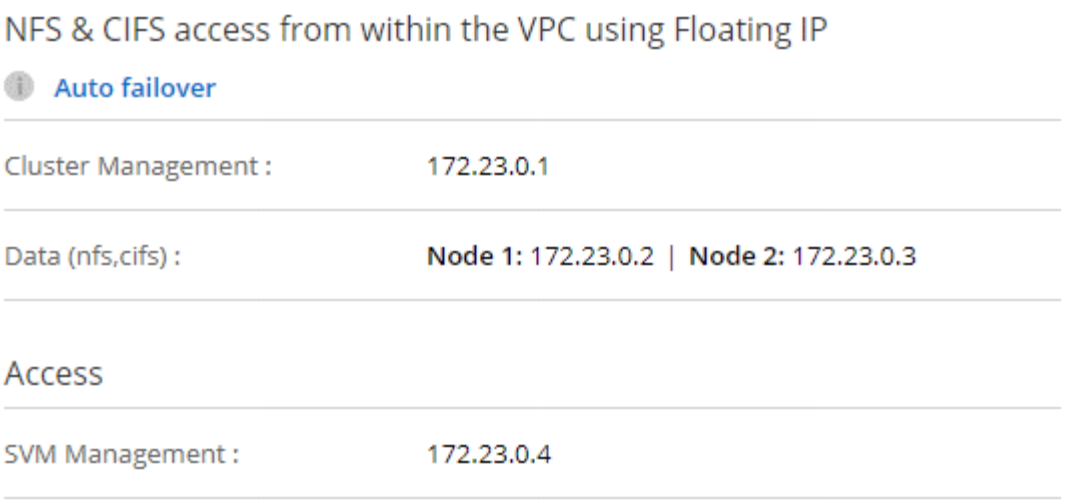


As etapas a seguir ilustram como configurar uma configuração semelhante.

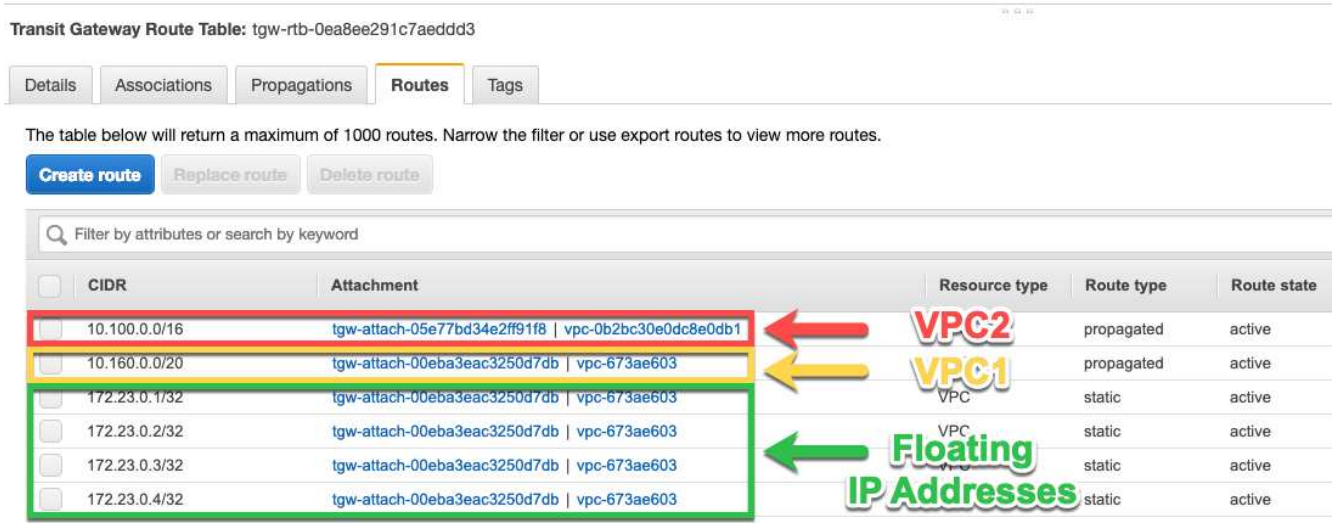
Passos

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.

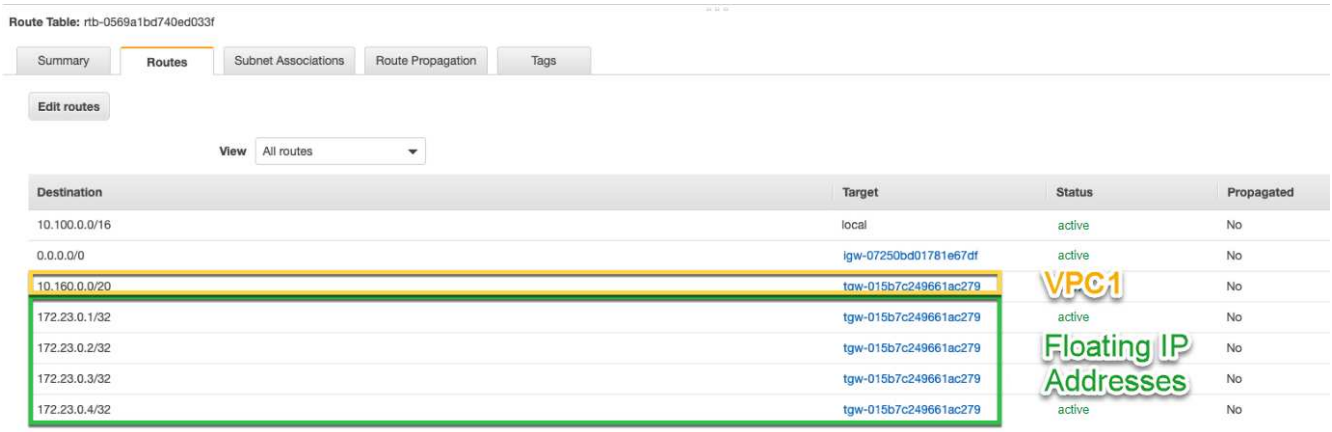


4. Modifique a tabela de rotas de VPCs que precisam acessar os endereços IP flutuantes.

   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.

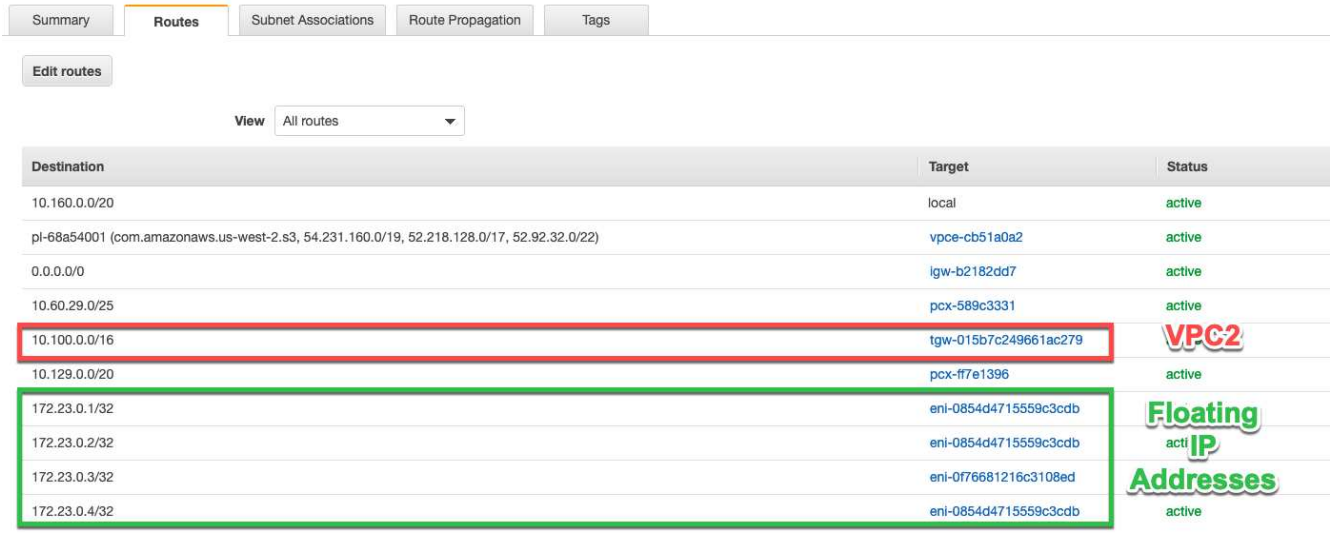
      A imagem de exemplo a seguir mostra a tabela de rotas para a VPC 2, que inclui rotas para a VPC 1 e os endereços IP flutuantes.



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.

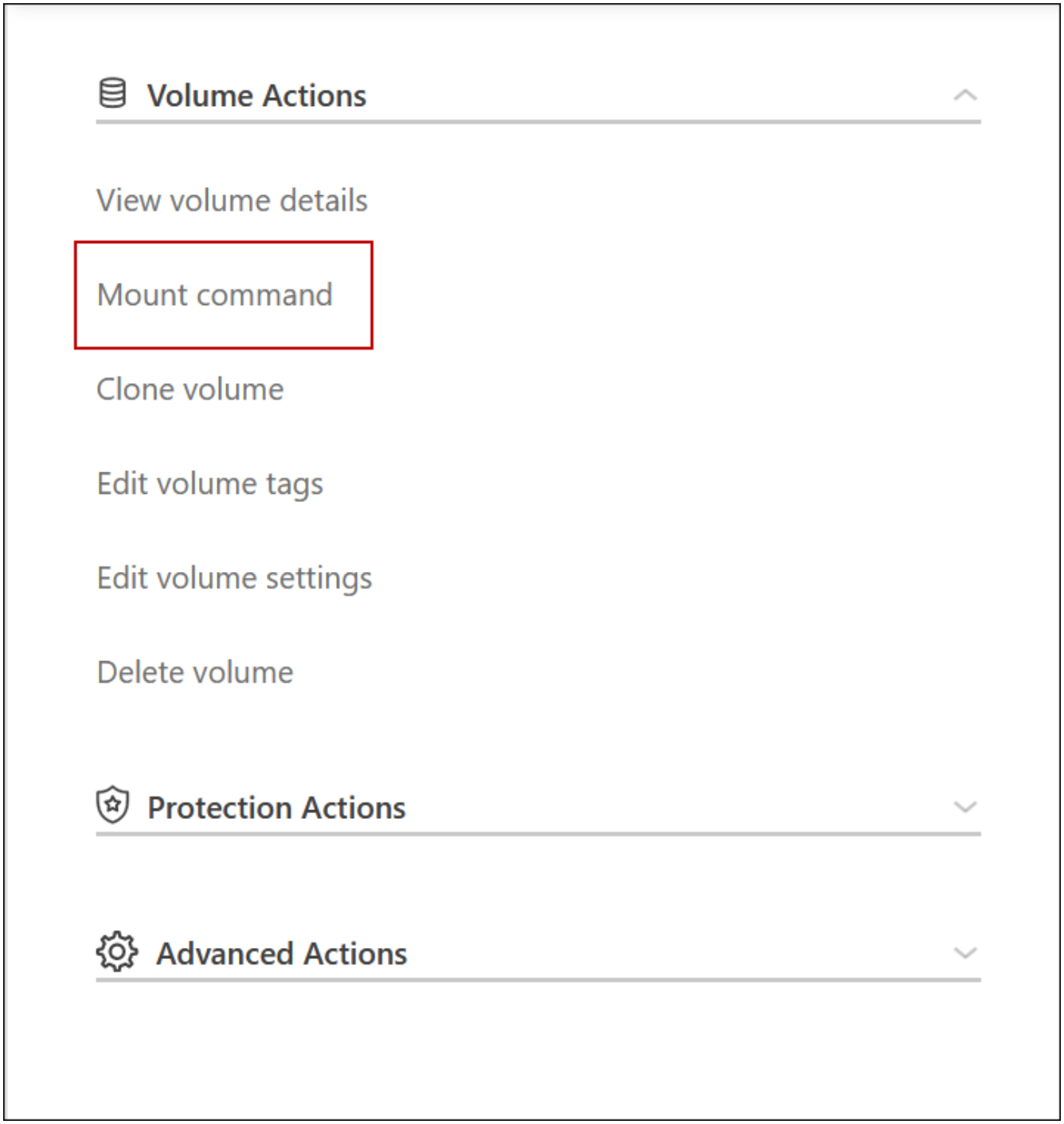
   A imagem de exemplo a seguir mostra a tabela de rotas para a VPC 1. Inclui uma rota para os endereços IP flutuantes e para a VPC 2, que é onde reside um cliente. O Console adicionou automaticamente os IPs flutuantes à tabela de rotas quando implantou o par HA.



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

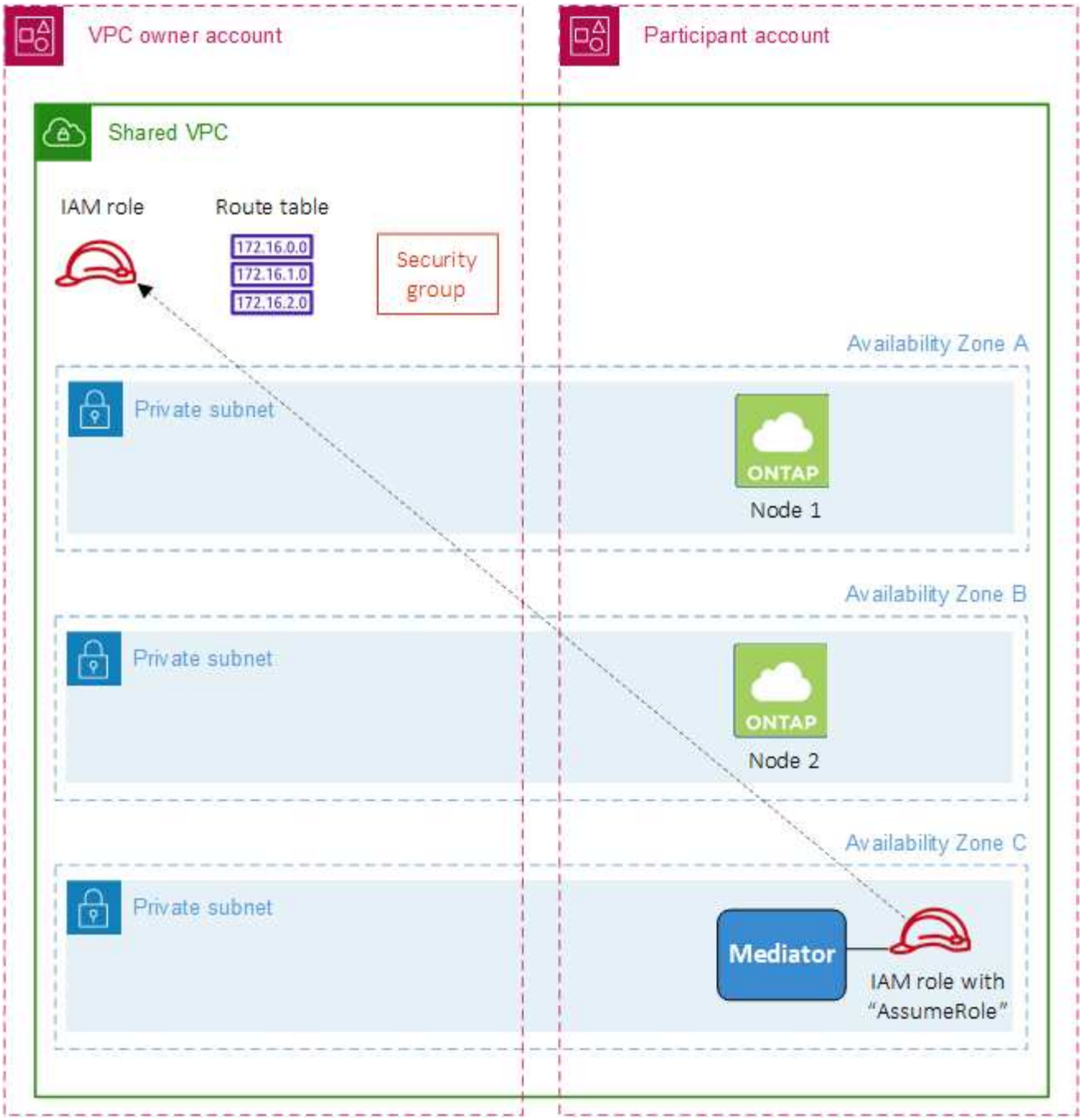
A partir da versão 9.11.1, os pares de HA do Cloud Volumes ONTAP são suportados na AWS com compartilhamento de VPC. O compartilhamento de VPC permite que sua organização compartilhe sub-redes com outras contas da AWS. Para usar esta configuração, você deve configurar seu ambiente AWS e então implantar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

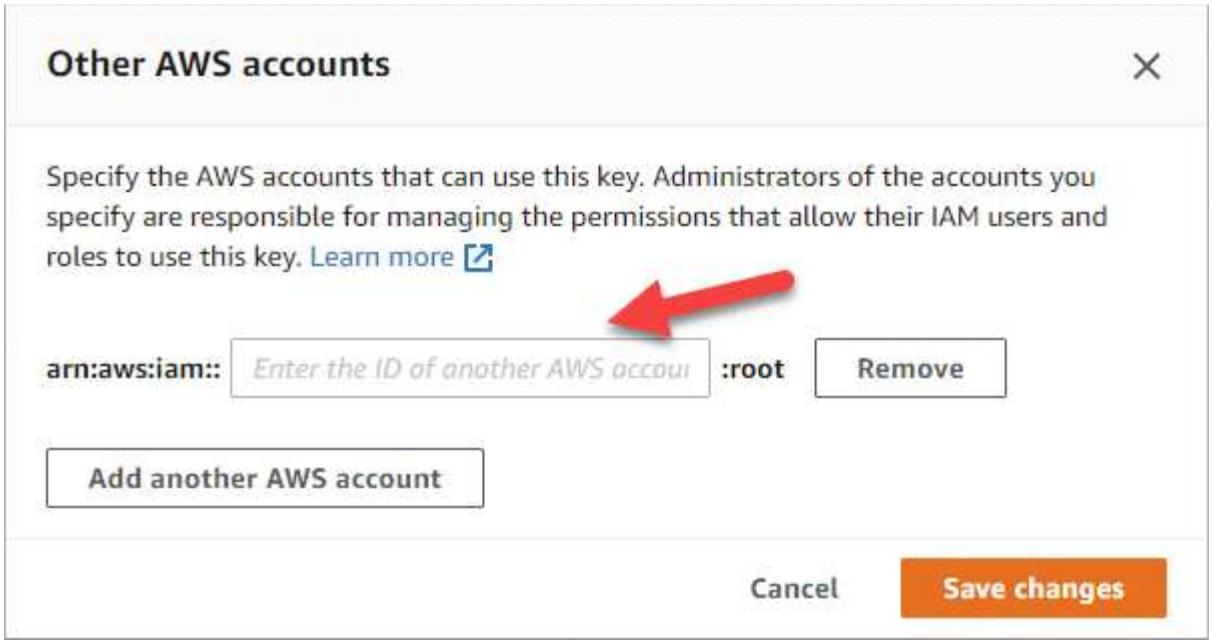
3. Se a CMK estiver em uma conta diferente da AWS, conclua as seguintes etapas:

   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

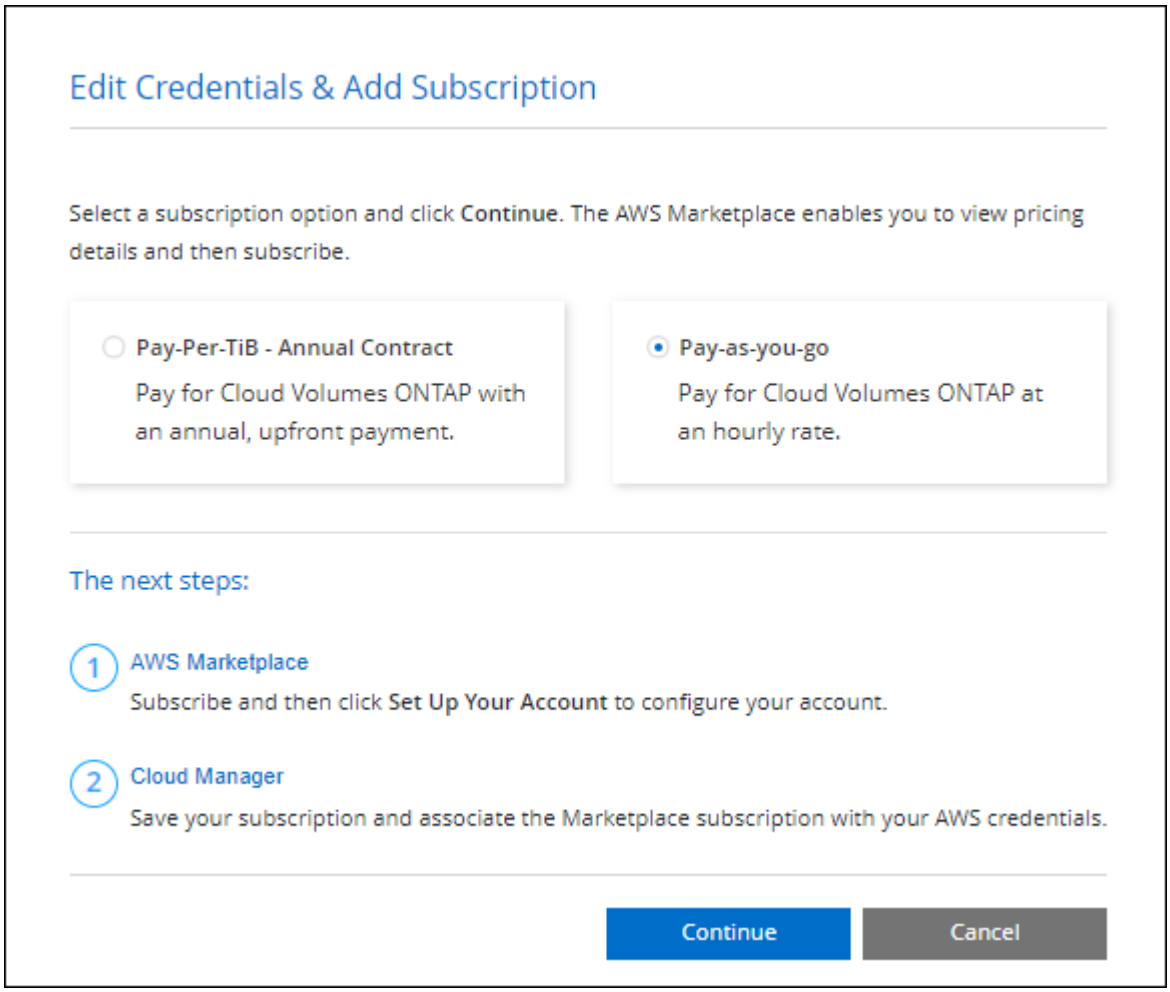
Selecione a oferta Freemium para usar o Cloud Volumes ONTAP gratuitamente com até 500 GiB de capacidade provisionada. "Saiba mais sobre a oferta Freemium" .

Passos

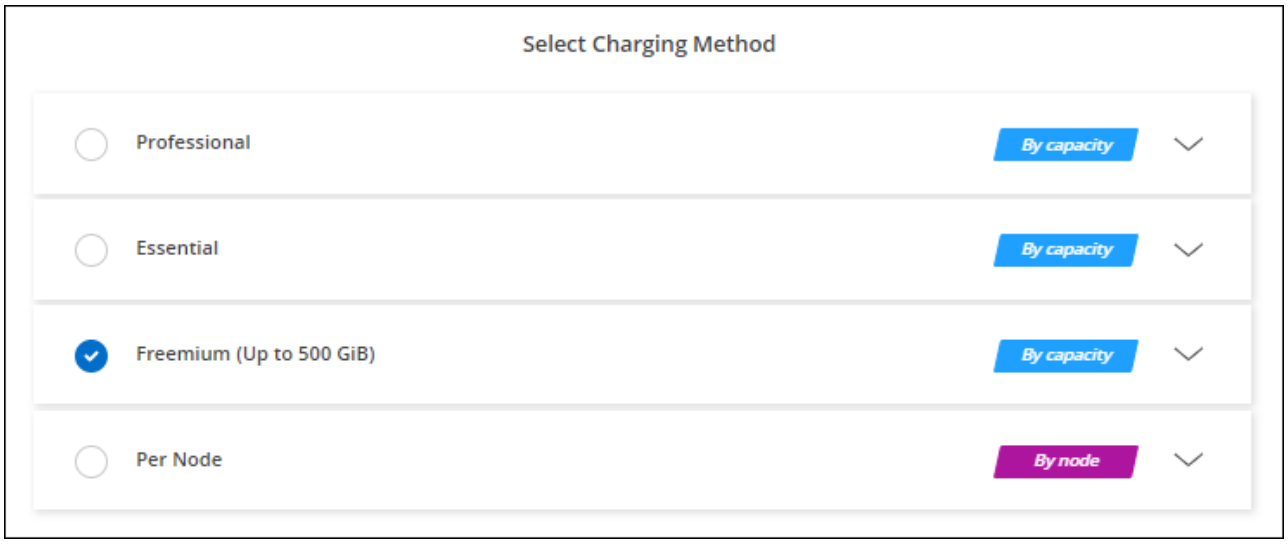
1. No menu de navegação esquerdo do NetApp Console, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas.

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"

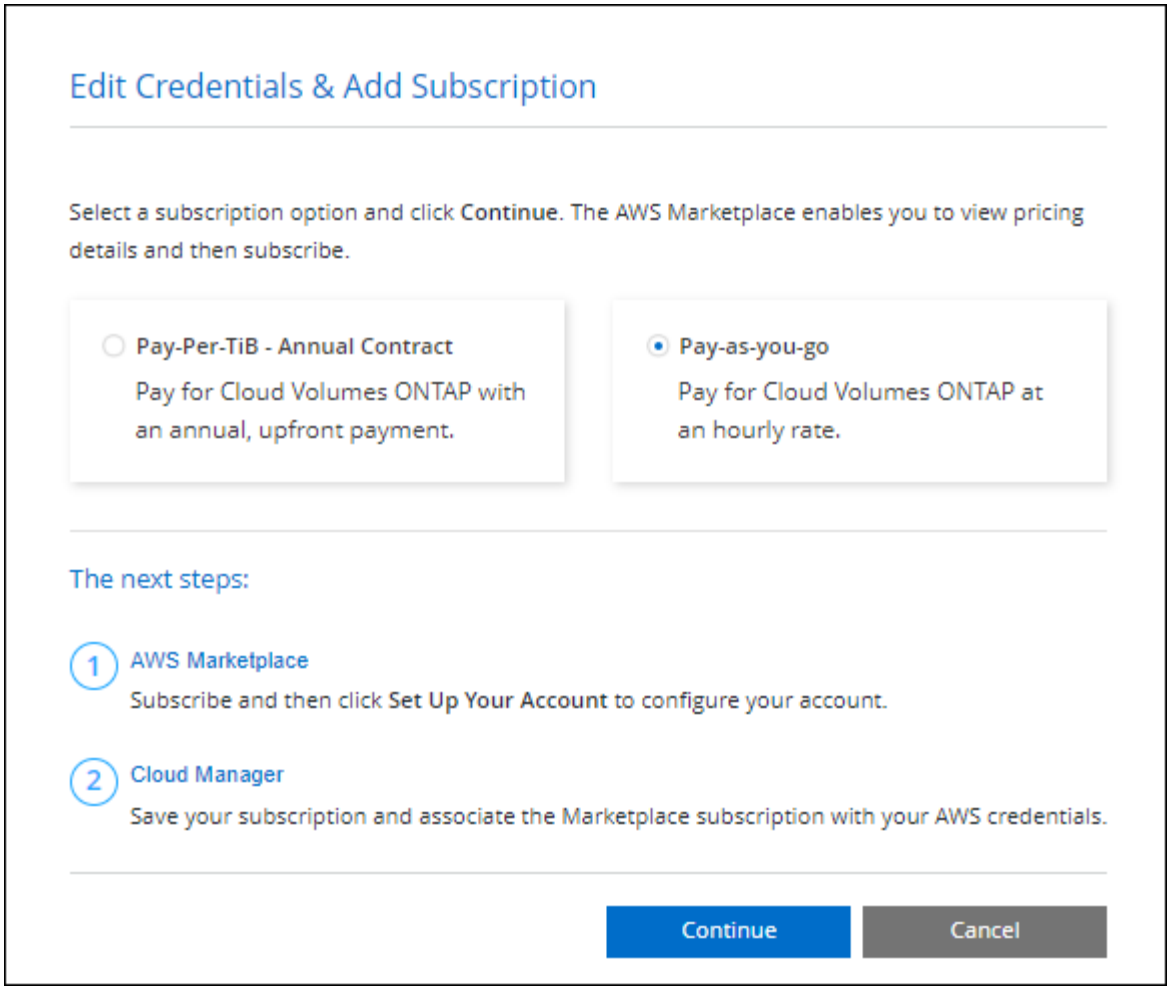
   O Console consulta automaticamente o serviço de licenciamento da NetApp para obter detalhes sobre as licenças associadas à sua conta do Site de Suporte da NetApp . Se não houver erros, o Console adicionará automaticamente as licenças ao Console.

   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" .

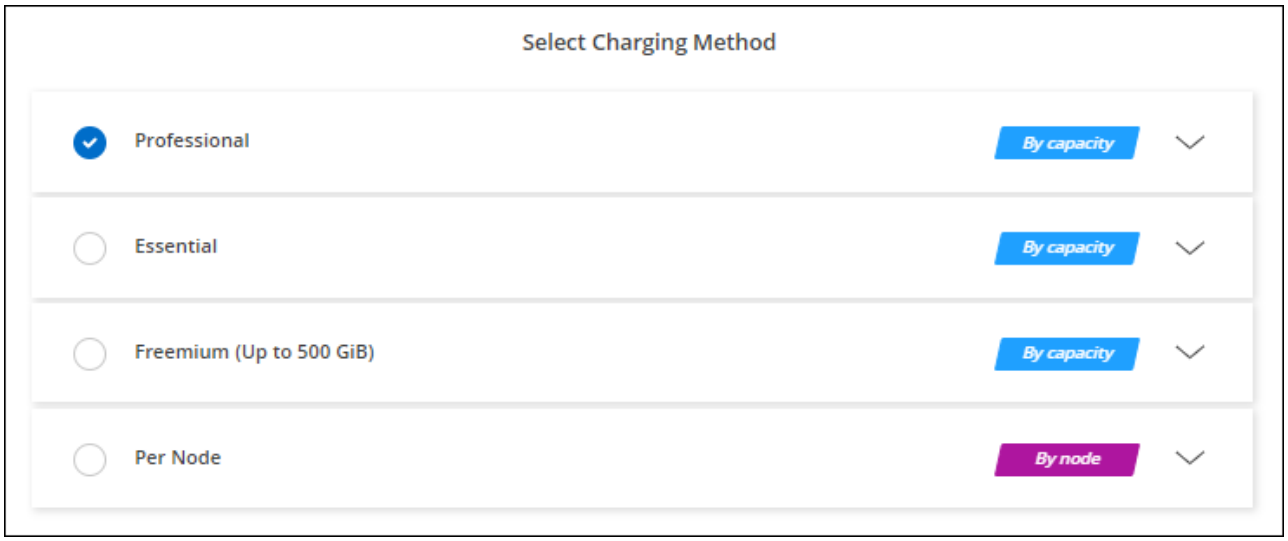
3. Na página **Sistemas** do Console, clique em **Adicionar Sistema** e siga as etapas.

   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" .

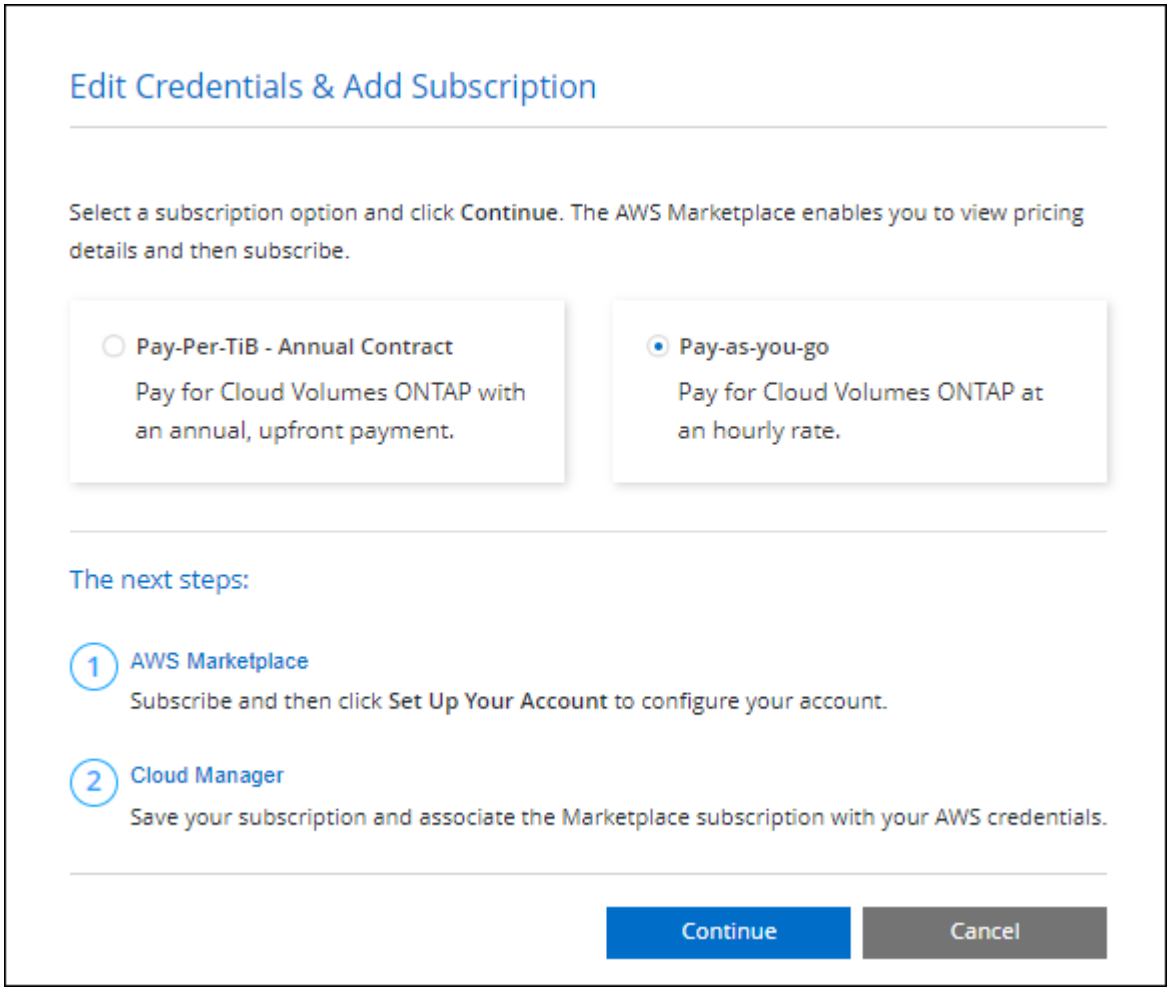
Assinatura PAYGO

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

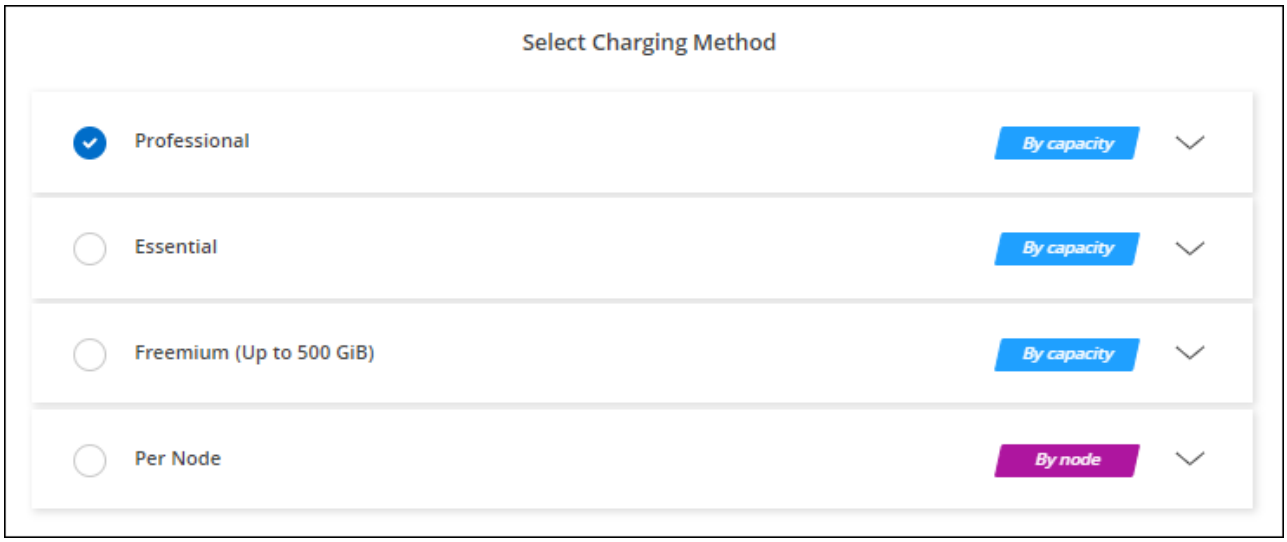
Quando você cria um sistema Cloud Volumes ONTAP , o Console solicita que você assine o contrato disponível no AWS Marketplace. Essa assinatura é então associada ao sistema de cobrança. Você pode usar a mesma assinatura para sistemas Cloud Volumes ONTAP adicionais.

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"

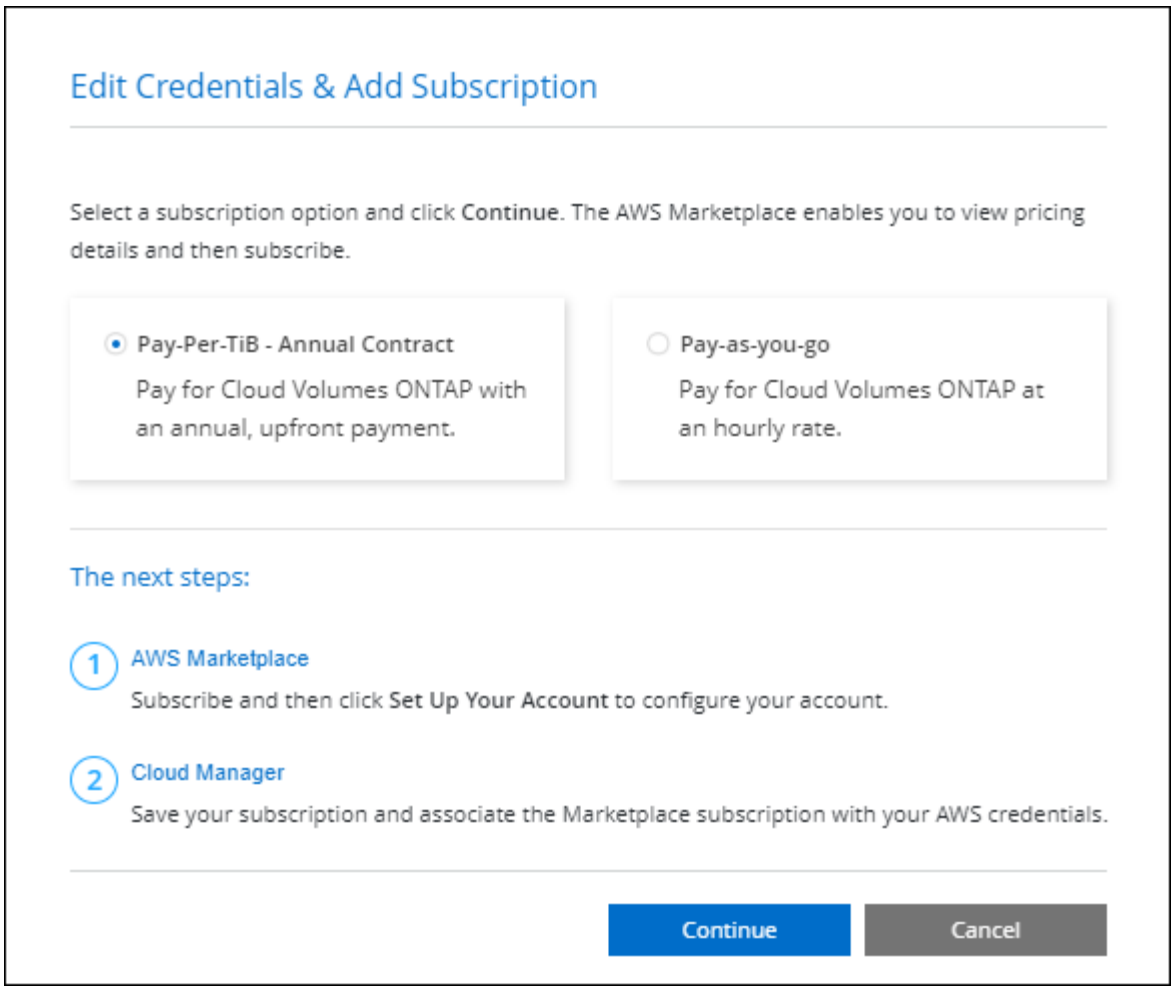
Contrato anual

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

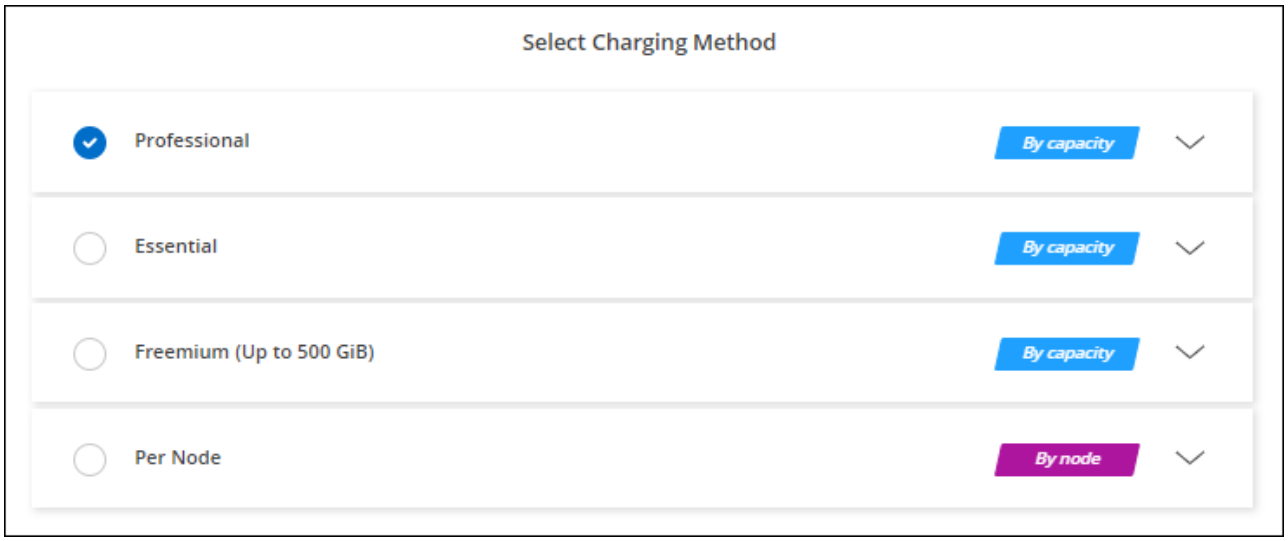
Semelhante a uma assinatura por hora, o Console solicita que você assine o contrato anual disponível no AWS Marketplace.

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" .

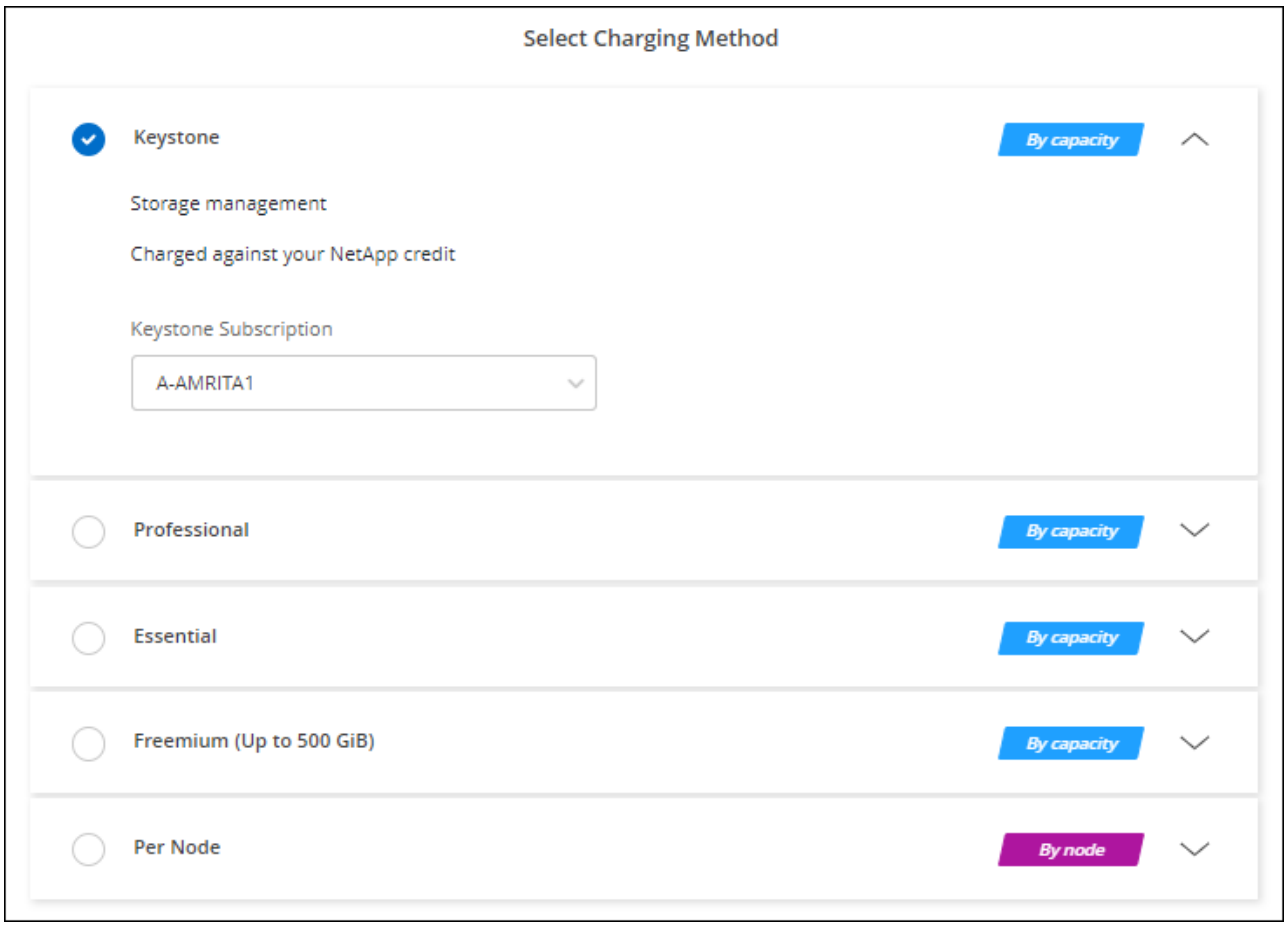
Assinatura Keystone

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.

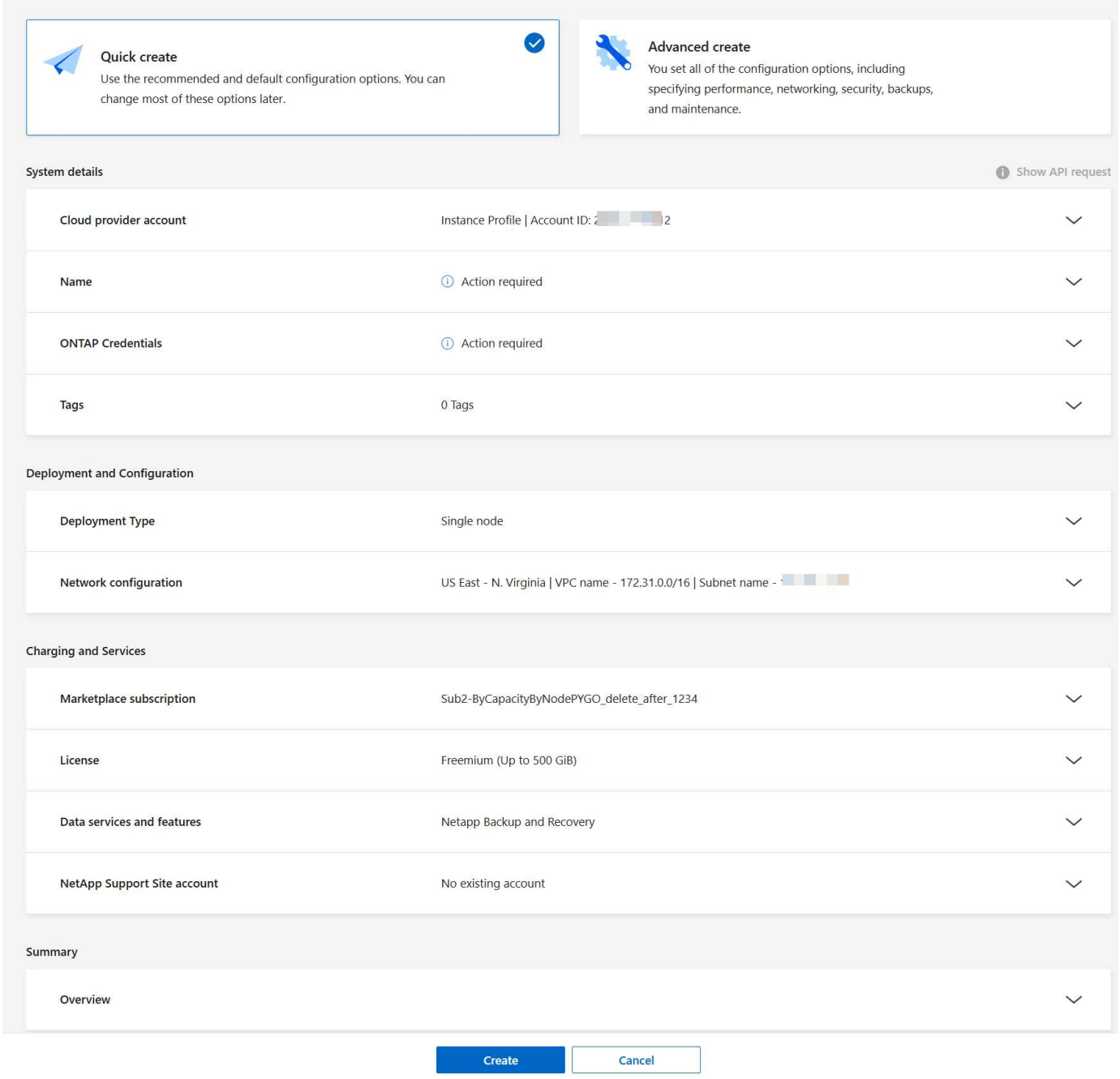
  Para mais detalhes, consulte"Requisitos de rede para Cloud Volumes ONTAP na AWS" .

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

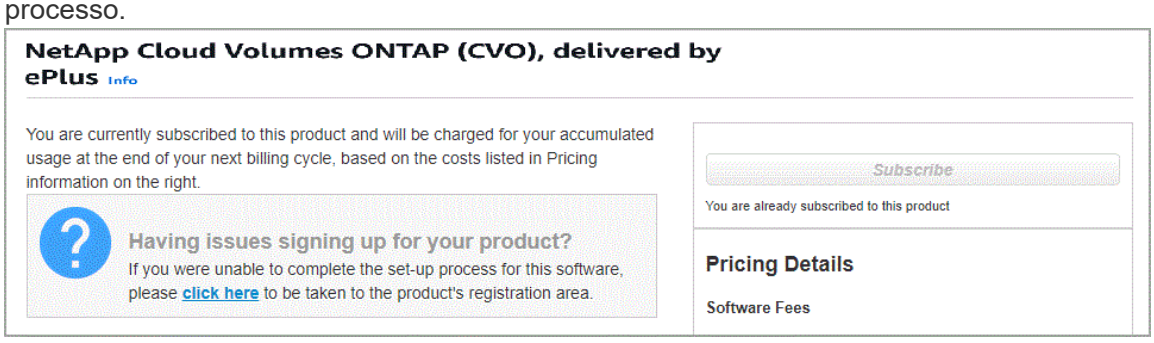
1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as instruções.
3. Selecione **Amazon Web Services** e * Cloud Volumes ONTAP Single Node*.
4. Selecione **Criação avançada**. Como o modo **Criação rápida** 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.

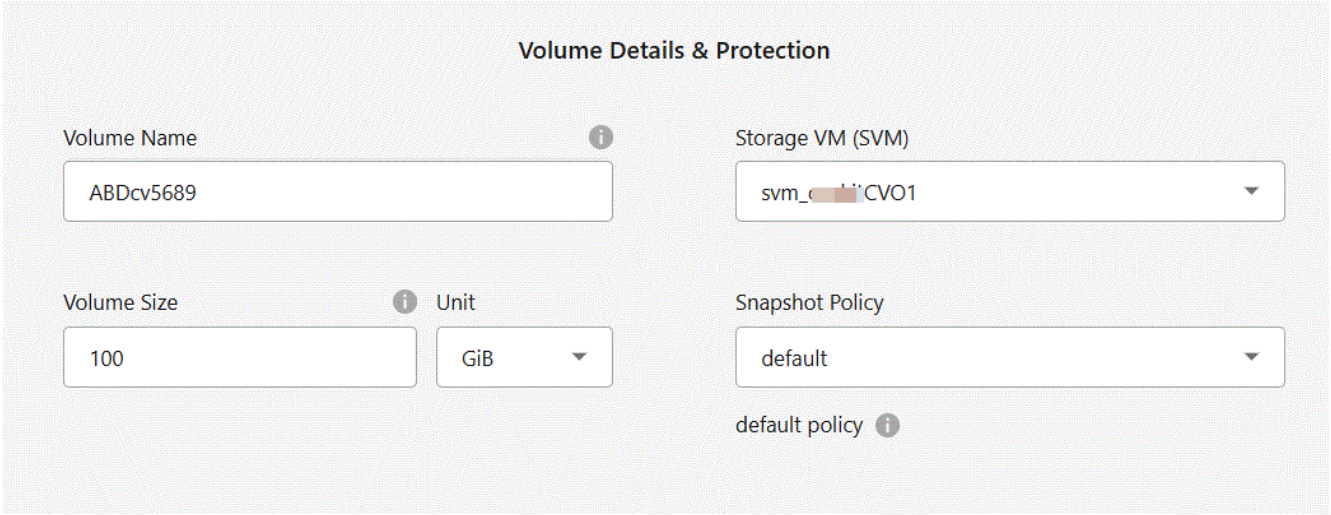
17. **Criar volume**: insira detalhes para o novo volume ou clique em **Ignorar**.

    "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"" .

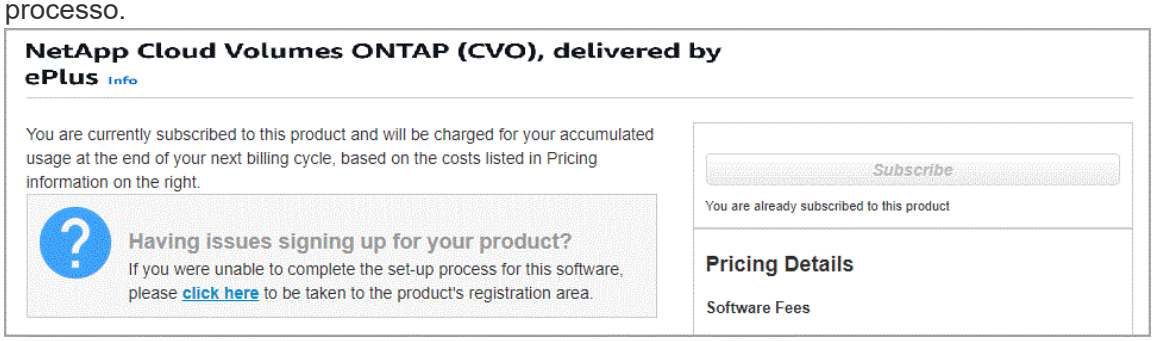
   Se você estiver executando o agente do Console 3.9.36 ou inferior, será necessário adicionar o `DescribeAvailabilityZones` permissão para a função AWS no console AWS EC2.

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.

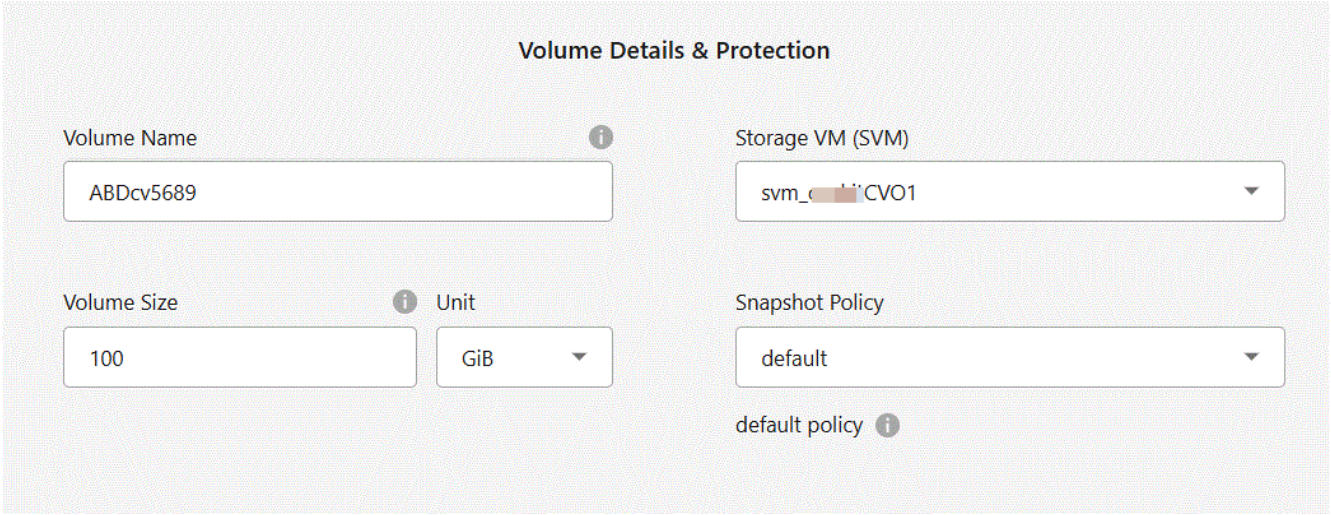
19. **Criar volume**: insira detalhes para o novo volume ou clique em **Ignorar**.

    "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>`

Informações sobre direitos autorais

Informações sobre marcas comerciais