



Requisitos de rede

Cloud Manager 3.6

NetApp
October 23, 2024

Índice

- Requisitos de rede 1
 - Requisitos de rede para o Cloud Manager 1
 - Requisitos de rede para o Cloud Volumes ONTAP na AWS 4
 - Configurando um gateway de trânsito da AWS para pares de HA em vários AZs 11
 - Requisitos de rede para o Cloud Volumes ONTAP no Azure 15

Requisitos de rede

Requisitos de rede para o Cloud Manager

Você precisa configurar sua rede para que o Cloud Manager possa implantar sistemas Cloud Volumes ONTAP na AWS ou no Microsoft Azure. O passo mais importante é garantir o acesso de saída à Internet a vários endpoints.



Se a rede usar um servidor proxy para toda a comunicação com a Internet, o Cloud Manager solicitará que você especifique o proxy durante a configuração. Você também pode especificar o servidor proxy na página Configurações. ["Configurando o Cloud Manager para usar um servidor proxy"](#) Consulte a .

Conexão com redes de destino

O Cloud Manager requer uma conexão de rede com os VPCs da AWS e os VNets do Azure na qual você deseja implantar o Cloud Volumes ONTAP.

Por exemplo, se você instalar o Cloud Manager em sua rede corporativa, deverá configurar uma conexão VPN com a VPC ou o Azure VNet no qual você inicia o Cloud Volumes ONTAP.

Acesso de saída à Internet

O Cloud Manager requer acesso de saída à Internet para implantar e gerenciar o Cloud Volumes ONTAP. O acesso de saída à Internet também é necessário ao acessar o Cloud Manager a partir do navegador da Web e ao executar o instalador do Cloud Manager em um host Linux.

As seções a seguir identificam os endpoints específicos.

Acesso de saída à Internet para gerenciar o Cloud Volumes ONTAP na AWS

O Cloud Manager requer acesso de saída à Internet para entrar em Contato com os seguintes endpoints ao implantar e gerenciar o Cloud Volumes ONTAP na AWS:

Endpoints	Finalidade
Serviços da AWS (amazonaws.com): <ul style="list-style-type: none">• CloudFormation• Nuvem de computação elástica (EC2)• Key Management Service (KMS)• Serviço de token de segurança (STS)• Serviço de armazenamento simples (S3) O endpoint exato depende da região em que você implementa o Cloud Volumes ONTAP. "Consulte a documentação da AWS para obter detalhes."	Permite que o Cloud Manager implante e gerencie o Cloud Volumes ONTAP na AWS.
https://api.services.cloud.NetApp.com:443	Solicitações de API para o NetApp Cloud Central.

Endpoints	Finalidade
https://cloud.support.NetApp.com.s3.us-west-1.amazonaws.com	Fornecer acesso a imagens de software, manifestos e modelos.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com	Permite que o Cloud Manager acesse e baixe manifestos, modelos e imagens de atualização do Cloud Volumes ONTAP.
https://kinesis.us-east-1.amazonaws.com	Permite que o NetApp transmita dados de Registros de auditoria.
https://cloudmanager.cloud.NetApp.com	Comunicação com o serviço Cloud Manager, que inclui contas do Cloud Central.
https://NetApp-cloud-account.auth0.com	Comunicação com o NetApp Cloud Central para autenticação centralizada de usuários.
https://support.NetApp.com/aods/asupmessage https://support.NetApp.com/asupprod/post/1,0/postAsup	Comunicação com NetApp AutoSupport.
https://support.NetApp.com/svcgw https://support.NetApp.com/ServiceGW/direito	Comunicação com a NetApp para licenciamento e Registro de suporte.
https://packages.cloud.google.com/yum https://github.com/NetApp/Trident/Releases/download/	Necessário para conectar sistemas Cloud Volumes ONTAP a um cluster Kubernetes. Os endpoints permitem a instalação do NetApp Trident.
Vários locais de terceiros, por exemplo: <ul style="list-style-type: none"> https://repo1.maven.org/maven2 https://oss.sonatype.org/content/repositories https://repo.typesafe.org Locais de terceiros estão sujeitos a alterações.	Durante as atualizações, o Cloud Manager baixa os pacotes mais recentes para dependências de terceiros.

Acesso de saída à Internet para gerenciar o Cloud Volumes ONTAP no Azure

O Cloud Manager requer acesso de saída à Internet para contactar os seguintes endpoints ao implementar e gerir o Cloud Volumes ONTAP no Microsoft Azure:

Endpoints	Finalidade
https://management.azure.com https://login.microsoftonline.com	Permite que o Cloud Manager implante e gerencie o Cloud Volumes ONTAP na maioria das regiões do Azure.
https://management.microsoftazure.de https://login.microsoftonline.de	Permite que o Cloud Manager implante e gerencie o Cloud Volumes ONTAP nas regiões Azure Alemanha.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Permite que o Cloud Manager implante e gerencie o Cloud Volumes ONTAP nas regiões Azure US Gov.
https://api.services.cloud.NetApp.com:443	Solicitações de API para o NetApp Cloud Central.

Endpoints	Finalidade
https://cloud.support.NetApp.com.s3.us-west-1.amazonaws.com	Fornecer acesso a imagens de software, manifestos e modelos.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com	Permite que o Cloud Manager acesse e baixe manifestos, modelos e imagens de atualização do Cloud Volumes ONTAP.
https://kinesis.us-east-1.amazonaws.com	Permite que o NetApp transmita dados de Registros de auditoria.
https://NetApp-cloud-account.auth0.com	Comunicação com o NetApp Cloud Central para autenticação centralizada de usuários.
https://mysupport.NetApp.com	Comunicação com NetApp AutoSupport.
https://support.NetApp.com/svcgw https://support.NetApp.com/ServiceGW/direito	Comunicação com a NetApp para licenciamento e Registro de suporte.
https://packages.cloud.google.com/yum https://github.com/NetApp/Trident/Releases/download/	Necessário para conectar sistemas Cloud Volumes ONTAP a um cluster Kubernetes. Os endpoints permitem a instalação do NetApp Trident.
Vários locais de terceiros, por exemplo: <ul style="list-style-type: none"> • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org <p>Locais de terceiros estão sujeitos a alterações.</p>	Durante as atualizações, o Cloud Manager baixa os pacotes mais recentes para dependências de terceiros.

Acesso de saída à Internet a partir do seu navegador da Web

Os usuários devem acessar o Cloud Manager a partir de um navegador da Web. A máquina que executa o navegador da Web deve ter conexões com os seguintes endpoints:

Endpoints	Finalidade
O host do Cloud Manager	<p>Você deve inserir o endereço IP do host de um navegador da Web para carregar o console do Cloud Manager.</p> <p>Dependendo da sua conectividade com o seu provedor de nuvem, você pode usar o IP privado ou um IP público atribuído ao host:</p> <ul style="list-style-type: none"> • Um IP privado funciona se você tiver uma VPN e acesso direto à sua rede virtual • Um IP público funciona em qualquer cenário de rede <p>Em qualquer caso, você deve proteger o acesso à rede, garantindo que as regras do grupo de segurança permitam o acesso somente de IPs ou sub-redes autorizados.</p>
https://auth0.com https://cdn.auth0.com://NetApp-cloud-account.auth0.com https://services.cloud.NetApp.com	Seu navegador da Web se conecta a esses endpoints para autenticação de usuário centralizada por meio do NetApp Cloud Central.
https://widget.intercom.io	Para um bate-papo no produto que permite conversar com especialistas em nuvem da NetApp.

Acesso de saída à Internet para instalar o Cloud Manager em um host Linux

O instalador do Cloud Manager deve acessar os seguintes URLs durante o processo de instalação:

- <http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm>
- <https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm>
- <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip>

Portas e grupos de segurança

- Se você implantar o Cloud Manager a partir do Cloud Central ou a partir das imagens do mercado, consulte o seguinte:
 - ["Regras do grupo de segurança para o Cloud Manager na AWS"](#)
 - ["Regras do grupo de segurança para o Cloud Manager no Azure"](#)
- Se você instalar o Cloud Manager em um host Linux existente, ["Requisitos de host do Cloud Manager"](#) consulte .

Requisitos de rede para o Cloud Volumes ONTAP na AWS

Configure sua rede AWS para que os sistemas Cloud Volumes ONTAP possam operar corretamente.

Procurando a lista de endpoints para os quais o Cloud Manager requer acesso? Eles agora são mantidos em um único local. ["Clique aqui para mais detalhes"](#).

Requisitos gerais de rede da AWS para o Cloud Volumes ONTAP

Os requisitos a seguir devem ser atendidos na AWS.

Acesso de saída à Internet para nós Cloud Volumes ONTAP

Os nós do Cloud Volumes ONTAP exigem acesso de saída à Internet para enviar mensagens para o NetApp AutoSupport, que monitora proativamente a integridade do storage.

As políticas de roteamento e firewall devem permitir o tráfego HTTP/HTTPS da AWS para os seguintes endpoints, para que o Cloud Volumes ONTAP possa enviar mensagens do AutoSupport:

- <https://support.NetApp.com/aods/asupmessage>
- <https://support.NetApp.com/asupprod/post/1,0/postSup>

Se você tiver uma instância NAT, deverá definir uma regra de grupo de segurança de entrada que permita o tráfego HTTPS da sub-rede privada para a Internet.

Acesso de saída à Internet para o mediador HA

A instância de mediador de HA precisa ter uma conexão de saída para o serviço AWS EC2 para que a TI possa ajudar no failover de storage. 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 de VPC de interface da sub-rede de destino para o serviço AWS EC2. Para obter detalhes sobre endpoints da VPC, "[Documentação da AWS: Endpoints da interface VPC \(AWS PrivateLink\)](#)" consulte .

Grupos de segurança

Você não precisa criar grupos de segurança porque o Cloud Manager faz isso por você. Se você precisar usar o seu próprio, "[Regras do grupo de segurança](#)" consulte .

Conexão do Cloud Volumes ONTAP ao AWS S3 para categorização de dados

Se você quiser usar o EBS como um nível de desempenho e o AWS S3 como um nível de capacidade, deve garantir que o Cloud Volumes ONTAP tenha uma conexão com o S3. A melhor maneira de fornecer essa conexão é criando um endpoint VPC para o serviço S3. Para obter instruções, "[Documentação da AWS: Criando um endpoint do Gateway](#)" consulte .

Ao criar o endpoint VPC, certifique-se de selecionar a tabela região, VPC e rota que corresponde à instância do Cloud Volumes ONTAP. Você também deve modificar o grupo de segurança para adicionar uma regra HTTPS de saída que permita o tráfego para o endpoint S3. Caso contrário, o Cloud Volumes ONTAP não pode se conectar ao serviço S3.

Se tiver algum problema, consulte "[AWS Support Knowledge Center: Por que não consigo me conectar a um bucket do S3 usando um endpoint VPC de gateway?](#)"

Conexões com sistemas ONTAP em outras redes

Para replicar dados entre um sistema Cloud Volumes ONTAP na AWS e sistemas ONTAP em outras redes, você precisa ter uma conexão VPN entre a VPC da AWS e a outra rede, por exemplo, um VNet do Azure ou sua rede corporativa. Para obter instruções, "[Documentação da AWS: Configurando uma conexão VPN da AWS](#)" consulte .

DNS e ative Directory para CIFS

Se você quiser provisionar o storage CIFS, configure o DNS e o ative Directory na AWS ou estenda 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 padrão EC2, que não deve ser o servidor DNS usado pelo ambiente Active Directory.

Para obter instruções, ["Documentação da AWS: Serviços de domínio do Active Directory na implantação de referência de início rápido da AWS Cloud"](#) consulte .

Requisitos de rede da AWS para o Cloud Volumes ONTAP HA em vários AZs

Requisitos adicionais de rede da AWS se aplicam a configurações do Cloud Volumes ONTAP HA que usam várias zonas de disponibilidade (AZs). Você deve analisar esses requisitos antes de iniciar um par de HA, pois deve inserir os detalhes da rede no Cloud Manager.

Para entender como os pares de HA funcionam, ["Pares de alta disponibilidade"](#) consulte .

Zonas de disponibilidade

Este modelo de implantação de HA usa vários AZs para garantir alta disponibilidade de 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 de HA.

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

As configurações de HA em vários AZs usam endereços IP flutuantes que migram entre nós se ocorrerem falhas. Eles não são diretamente acessíveis de fora da VPC, a menos que você ["Configure um gateway de trânsito da AWS"](#).

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



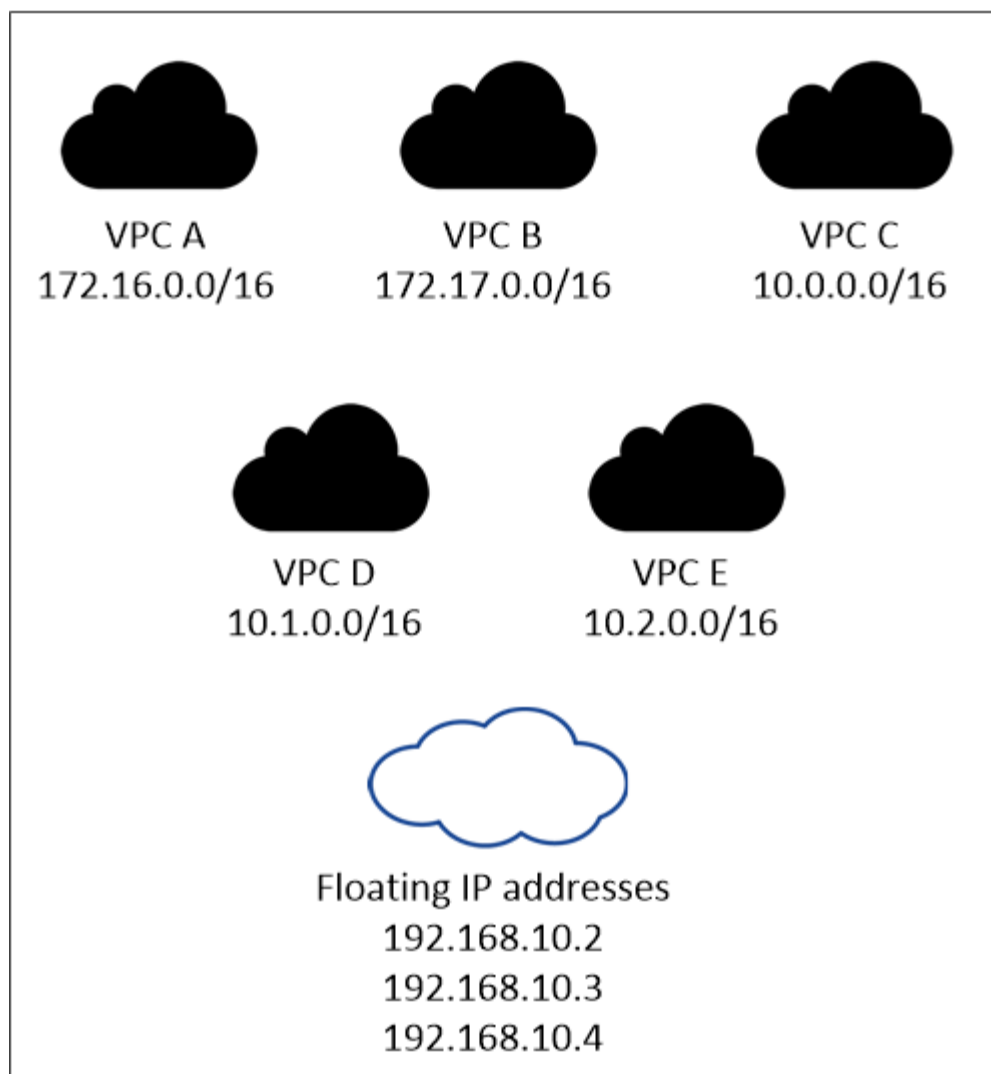
Um endereço IP flutuante é necessário para o LIF de gerenciamento da SVM se você usar o SnapDrive para Windows ou SnapCenter com o par de HA. Se você não especificar o endereço IP ao implantar o sistema, poderá criar o LIF mais tarde. Para obter detalhes, ["Configurar o Cloud Volumes ONTAP"](#) consulte .

Você precisa inserir os endereços IP flutuantes no Cloud Manager ao criar um ambiente de trabalho do Cloud Volumes ONTAP HA. O Cloud Manager aloca os endereços IP para o par de HA quando ele inicia o sistema.

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

O exemplo a seguir mostra a relação entre endereços IP flutuantes e os VPCs em uma região da AWS. Enquanto os endereços IP flutuantes estão fora dos blocos CIDR para todos os VPCs, eles são roteáveis para sub-redes através de tabelas de rota.

AWS region



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

Gateway de trânsito para habilitar o acesso IP flutuante de fora da VPC

["Configure um gateway de trânsito da AWS"](#) Para habilitar 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 no Cloud Manager, você precisa selecionar as tabelas de rota que devem incluir rotas para os endereços IP flutuantes. Isso permite o acesso do cliente ao par de HA.

Se você tiver apenas uma tabela de rota para as sub-redes na VPC (a tabela de rotas principal), o Cloud Manager adicionará automaticamente os endereços IP flutuantes a essa tabela de rotas. Se tiver mais de uma tabela de rota, é muito importante selecionar as tabelas de rota 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 tabelas de rota diferentes. Se você selecionar a

tabela de rota A, mas não a tabela de rota B, os clientes na sub-rede associada à tabela de rota A podem acessar o par de HA, mas os clientes na sub-rede associada à tabela de rota B.

Para obter mais informações sobre tabelas de rotas, ["Documentação da AWS: Tabelas de rotas"](#) consulte .

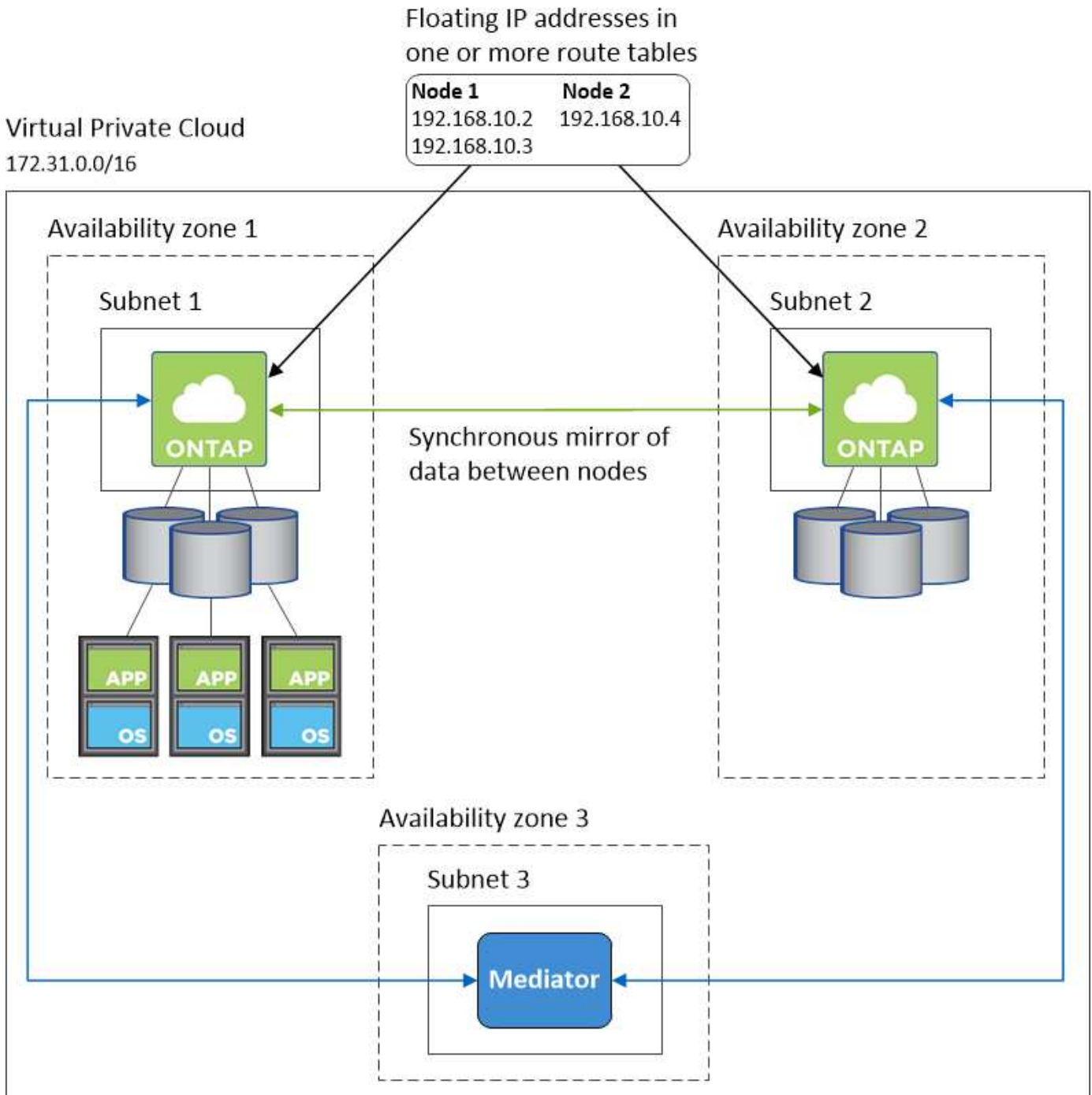
Conexão com ferramentas de gerenciamento do NetApp

Para usar as ferramentas de gerenciamento do NetApp com configurações de HA em vários AZs, você tem duas opções de conexão:

1. Implante as ferramentas de gerenciamento do NetApp em uma VPC diferente e ["Configure um gateway de trânsito da AWS"](#)no . O gateway permite o acesso ao endereço IP flutuante para a interface de gerenciamento de cluster de fora da VPC.
2. Implante as ferramentas de gerenciamento do NetApp na mesma VPC com uma configuração de roteamento semelhante aos clientes nas.

Exemplo de configuração

A imagem a seguir mostra uma configuração de HA ideal na AWS operando como uma configuração ativo-passivo:



Exemplo de configurações de VPC

Para entender melhor como você pode implantar o Cloud Manager e o Cloud Volumes ONTAP na AWS, leia as configurações de VPC mais comuns.

- Uma VPC com sub-redes públicas e privadas e um dispositivo NAT
- Uma VPC com uma sub-rede privada e uma conexão VPN à rede

Uma VPC com sub-redes públicas e privadas e um dispositivo NAT

Essa configuração de VPC inclui sub-redes públicas e privadas, um gateway de Internet que conecta a VPC à Internet e um gateway NAT ou instância NAT na sub-rede pública que permite o tráfego de saída da Internet a

partir da sub-rede privada. Nessa configuração, você pode executar o Cloud Manager em uma sub-rede pública ou privada, mas a sub-rede pública é recomendada porque permite o acesso de hosts fora da VPC. Em seguida, é possível iniciar instâncias do Cloud Volumes ONTAP na sub-rede privada.

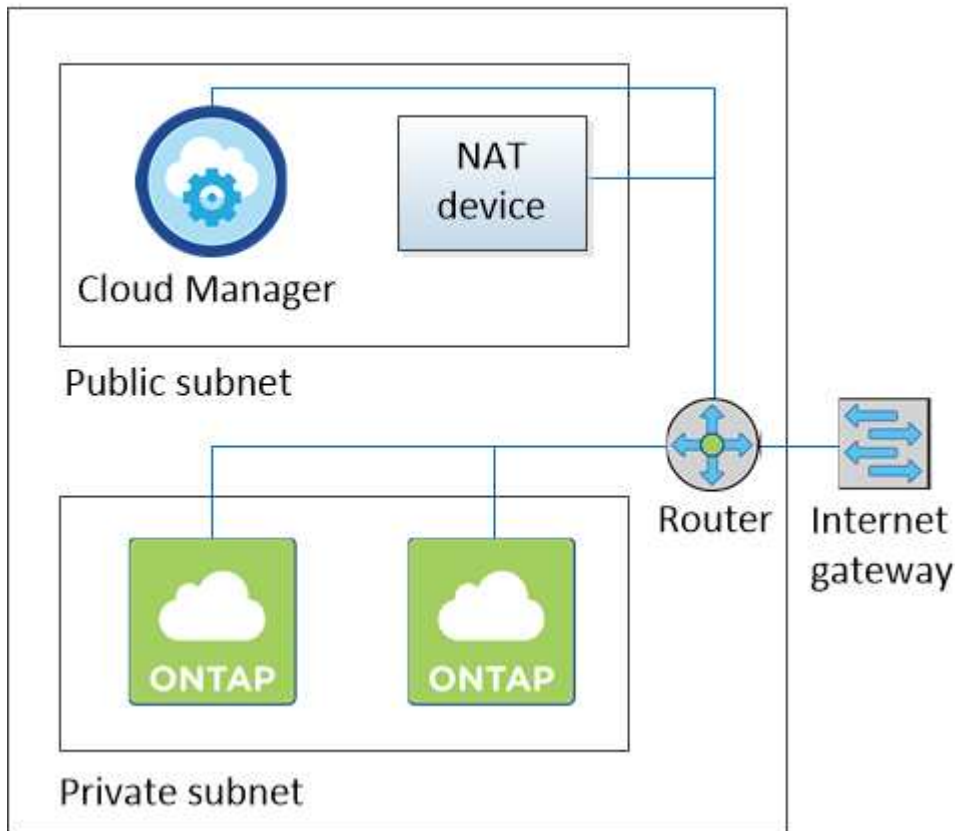


Em vez de um dispositivo NAT, você pode usar um proxy HTTP para fornecer conectividade à Internet.

Para obter mais detalhes sobre este cenário, "[Documentação da AWS: Cenário 2: VPC com sub-redes públicas e privadas \(NAT\)](#)" consulte .

O gráfico a seguir mostra o Cloud Manager em execução em uma sub-rede pública e em sistemas de nó único em execução em uma sub-rede privada:

Virtual Private Cloud



Uma VPC com uma sub-rede privada e uma conexão VPN à rede

Essa configuração de VPC é uma configuração de nuvem híbrida na qual o Cloud Volumes ONTAP se torna uma extensão do seu ambiente privado. A configuração inclui uma sub-rede privada e um gateway privado virtual com uma conexão VPN à sua rede. O roteamento através do túnel VPN permite que as instâncias EC2 acessem a Internet através da rede e firewalls. Você pode executar o Cloud Manager na sub-rede privada ou no data center. Em seguida, você iniciaria o Cloud Volumes ONTAP na sub-rede privada.



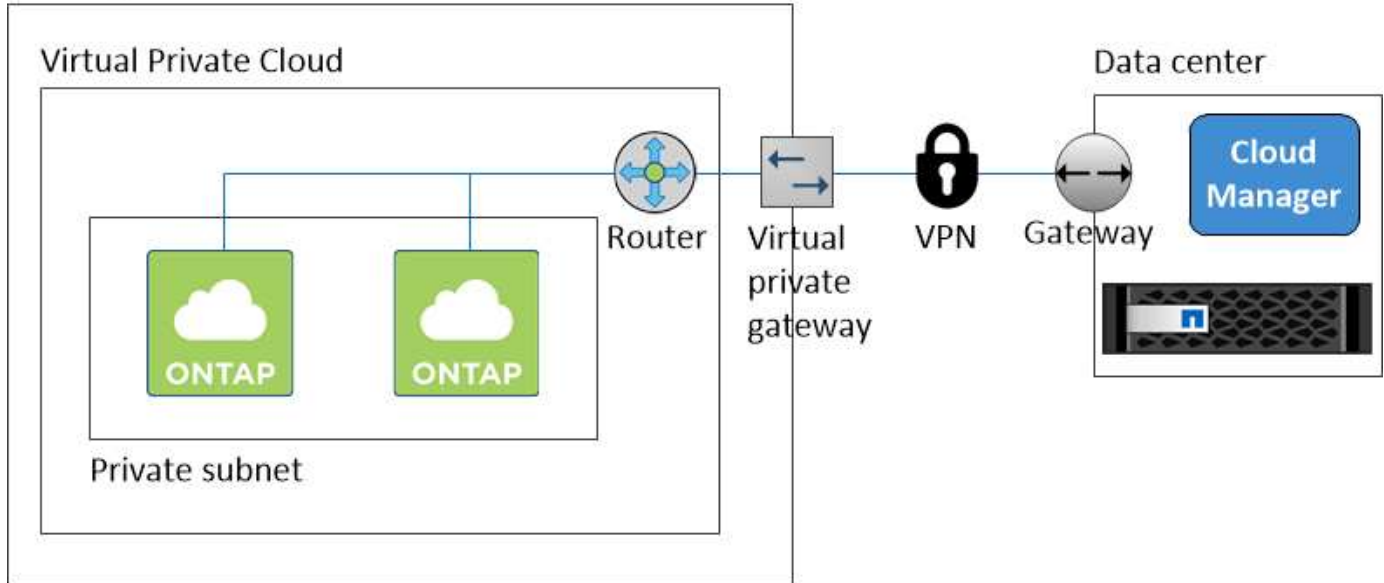
Você também pode usar um servidor proxy nesta configuração para permitir o acesso à Internet. O servidor proxy pode estar no data center ou na AWS.

Se você quiser replicar dados entre sistemas FAS em seu data center e sistemas Cloud Volumes ONTAP na AWS, use uma conexão VPN para que o link fique seguro.

Para obter mais detalhes sobre este cenário, "[Documentação da AWS: Cenário 4: VPC somente com um Private Subnet e acesso AWS Managed VPN](#)" consulte .

O gráfico a seguir mostra o Cloud Manager em execução em seus sistemas de data center e nó único em execução em uma sub-rede privada:

AWS region



Configurando um gateway de trânsito da AWS para pares de HA em vários AZs

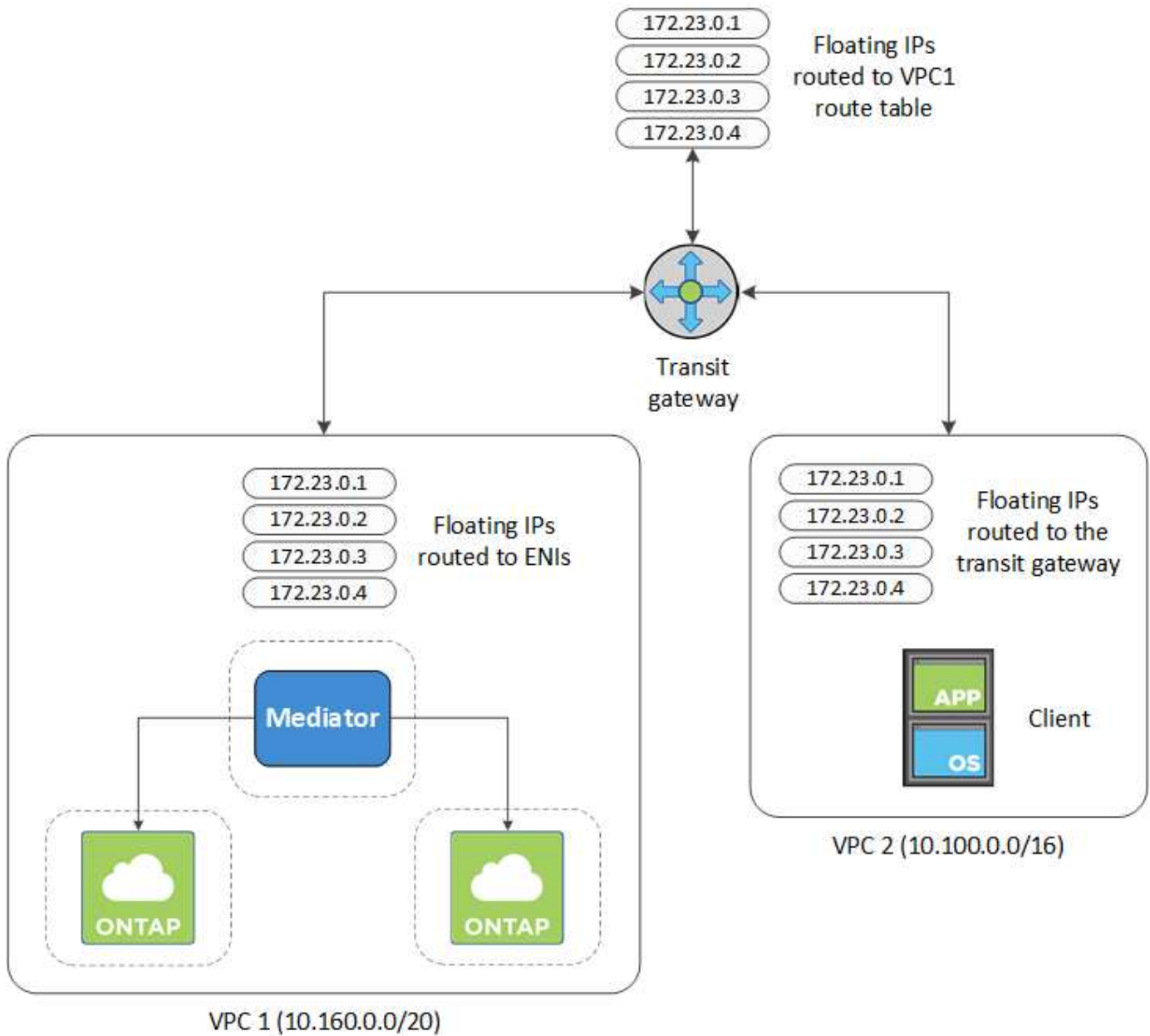
Configure um gateway de trânsito da AWS para permitir o acesso aos endereços IP flutuantes de um par de HA de fora da VPC onde o par de HA reside.

Quando uma configuração do Cloud Volumes ONTAP HA é espalhada por várias zonas de disponibilidade da AWS, os endereços IP flutuantes são necessários para o acesso a dados na a partir da VPC. Esses endereços IP flutuantes podem migrar entre nós quando ocorrem falhas, mas não são diretamente 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 opcional SVM.

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

Aqui está um exemplo que mostra dois VPCs conectados por um gateway de trânsito. Um sistema de HA reside em uma VPC, enquanto um cliente reside no outro. Em seguida, você pode 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 conecte os VPCs ao gateway".
2. 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 informações do ambiente de trabalho no Cloud Manager. Aqui está um exemplo:

NFS & CIFS access from within the VPC using Floating IP

Auto failover

Cluster Management : 172.23.0.1

Data (nfs,cifs) : Node 1: 172.23.0.2 | Node 2: 172.23.0.3

Access

SVM Management : 172.23.0.4

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

Transit Gateway Route Table: tgw-rtb-0ea8ee291c7aeddd3

Details Associations Propagations **Routes** Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route Replace route Delete route

Filter by attributes or search by keyword

<input type="checkbox"/>	CIDR	Attachment	Resource type	Route type	Route state
<input type="checkbox"/>	10.100.0.0/16	tgw-attach-05e77bd34e2ff91f8 vpc-0b2bc30e0dc8e0db1	VPC2	propagated	active
<input type="checkbox"/>	10.160.0.0/20	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC1	propagated	active
<input type="checkbox"/>	172.23.0.1/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.2/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.3/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.4/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active

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

- Adicione entradas de rota aos endereços IP flutuantes.
- Adicione uma entrada de rota ao bloco CIDR da VPC onde o par de 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.

Route Table: rtb-0569a1bd740ed033f

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	active	No
0.0.0.0/0	igw-07250bd01781e67df	active	No
10.160.0.0/20	tgw-015b7c249661ac279	active	No
172.23.0.1/32	tgw-015b7c249661ac279	active	No
172.23.0.2/32	tgw-015b7c249661ac279	active	No
172.23.0.3/32	tgw-015b7c249661ac279	active	No
172.23.0.4/32	tgw-015b7c249661ac279	active	No

VPC1
Floating IP Addresses

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

Esta etapa é importante porque completa o roteamento entre os VPCs.

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

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status
10.160.0.0/20	local	active
pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22)	vpce-cb51a0a2	active
0.0.0.0/0	igw-b2182dd7	active
10.60.29.0/25	pcx-589c3331	active
10.100.0.0/16	tgw-015b7c249661ac279	active
10.129.0.0/20	pcx-ff7e1396	active
172.23.0.1/32	eni-0854d4715559c3cdb	active
172.23.0.2/32	eni-0854d4715559c3cdb	active
172.23.0.3/32	eni-0f76681216c3108ed	active
172.23.0.4/32	eni-0854d4715559c3cdb	active

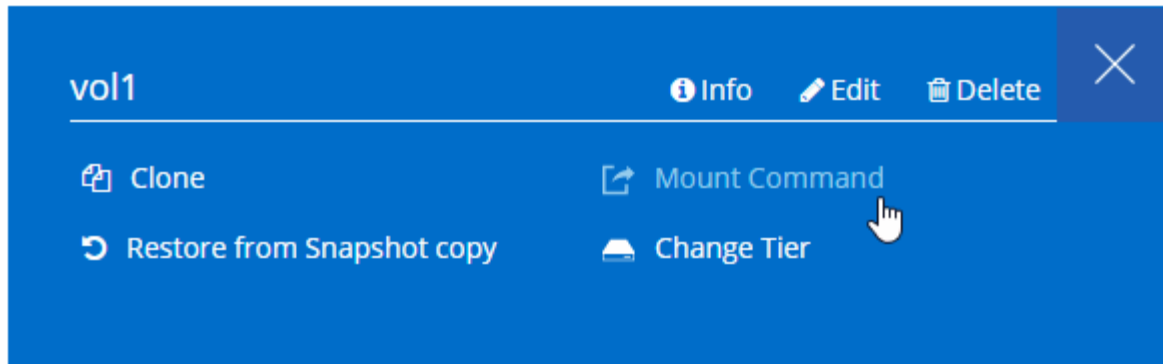
VPC2
Floating act IP Addresses

- Monte volumes em clientes usando o endereço IP flutuante.

Você pode encontrar o endereço IP correto no Cloud Manager selecionando um volume e clicando em **Mount Command**.

Volumes

2 Volumes | 0.22 TB Allocated | < 0.01 TB Used (0 TB in S3)



- Ligações relacionadas*
- ["Pares de alta disponibilidade na AWS"](#)
- ["Requisitos de rede para o Cloud Volumes ONTAP na AWS"](#)

Requisitos de rede para o Cloud Volumes ONTAP no Azure

Você deve configurar sua rede Azure para que os sistemas Cloud Volumes ONTAP possam funcionar corretamente.

Procurando a lista de endpoints para os quais o Cloud Manager requer acesso? Eles agora são mantidos em um único local. ["Clique aqui para mais detalhes"](#).

Acesso de saída à Internet para Cloud Volumes ONTAP

O Cloud Volumes ONTAP requer acesso de saída à Internet para enviar mensagens para o NetApp AutoSupport, que monitora proativamente a integridade do seu armazenamento.

As políticas de roteamento e firewall devem permitir o tráfego HTTP/HTTPS da AWS para os seguintes endpoints, para que o Cloud Volumes ONTAP possa enviar mensagens do AutoSupport:

- <https://support.NetApp.com/aods/asupmessage>
- <https://support.NetApp.com/asupprod/post/1,0/postSup>

Grupos de segurança

Você não precisa criar grupos de segurança porque o Cloud Manager faz isso por você. Se você precisar usar o seu próprio, ["Regras do grupo de segurança"](#) consulte .

Conexão do Cloud Volumes ONTAP ao storage Blob do Azure para categorização de dados

Se você quiser categorizar dados inativos no armazenamento de Blob do Azure, não precisa configurar um endpoint de serviço VNet desde que o Cloud Manager tenha as permissões necessárias:

```
"Microsoft.Network/virtualNetworks/subnets/write",  
"Microsoft.Network/routeTables/join/action",
```

Essas permissões estão incluídas no último ["Política do Cloud Manager"](#).

Para obter detalhes sobre como configurar a disposição de dados em camadas, ["Disposição em camadas de dados inativos no storage de objetos de baixo custo"](#) consulte .

Conexões com sistemas ONTAP em outras redes

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

Para obter instruções, ["Documentação do Microsoft Azure: Crie uma conexão Site-to-Site no portal do Azure"](#) consulte .

Informações sobre direitos autorais

Copyright © 2024 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPTÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.