Configure a rede

Cloud Manager 3.8

NetApp
October 22, 2024

Índice

Configure a rede

Requisitos de rede para o Cloud Volumes ONTAP na AWS

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

Requisitos gerais 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.

  "Saiba como configurar o AutoSupport".

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 .

Número de endereços IP

O Cloud Manager aloca o seguinte número de endereços IP para o Cloud Volumes ONTAP na AWS:

- Nó único: 6 endereços IP
- Pares HA em AZs únicos: Endereços 15
- Pares DE HA em vários AZs: 15 ou 16 endereços IP

  Observe que o Cloud Manager cria um LIF de gerenciamento de SVM em sistemas de nó único, mas não em pares de HA em uma única AZ. Você pode escolher se deseja criar um LIF de gerenciamento de SVM em pares de HA em vários AZs.

  Um LIF é um endereço IP associado a uma porta física. É necessário um LIF de gerenciamento de SVM para ferramentas de gerenciamento como o SnapCenter.

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 conetar ao serviço S3.

Se tiver algum problema, consulte "AWS Support Knowledge Center: Por que não consigo me conetar 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 ative 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 ative Directory.

Para obter instruções, "Documentação da AWS: Serviços de domínio do ative Directory na nuvem AWS: Implantação de referência de início rápido" consulte .

Requisitos para pares de HA em várias 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

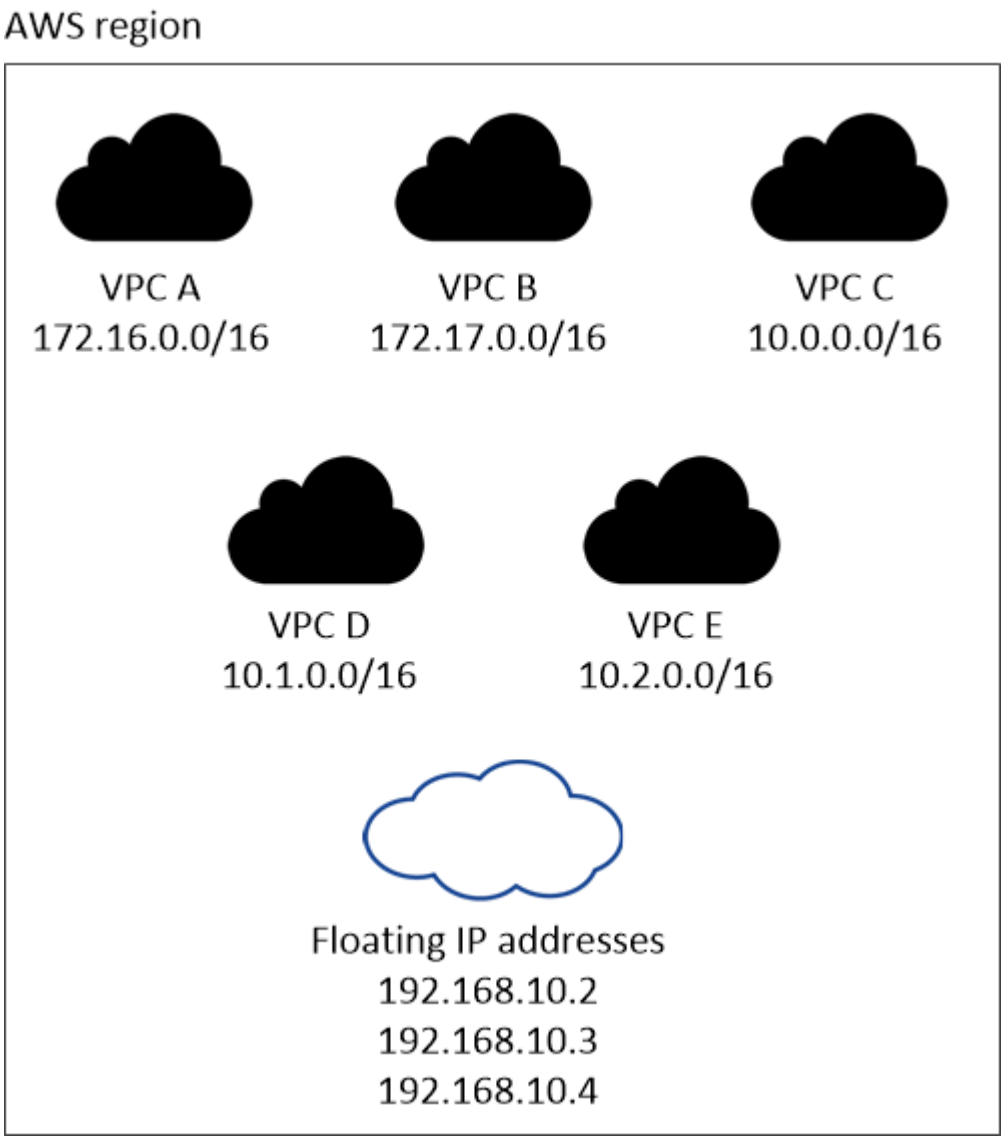
dados NFS/CIFS no nó 2. Um quarto endereço IP flutuante para gerenciamento de SVM é opcional.

> 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.



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 .

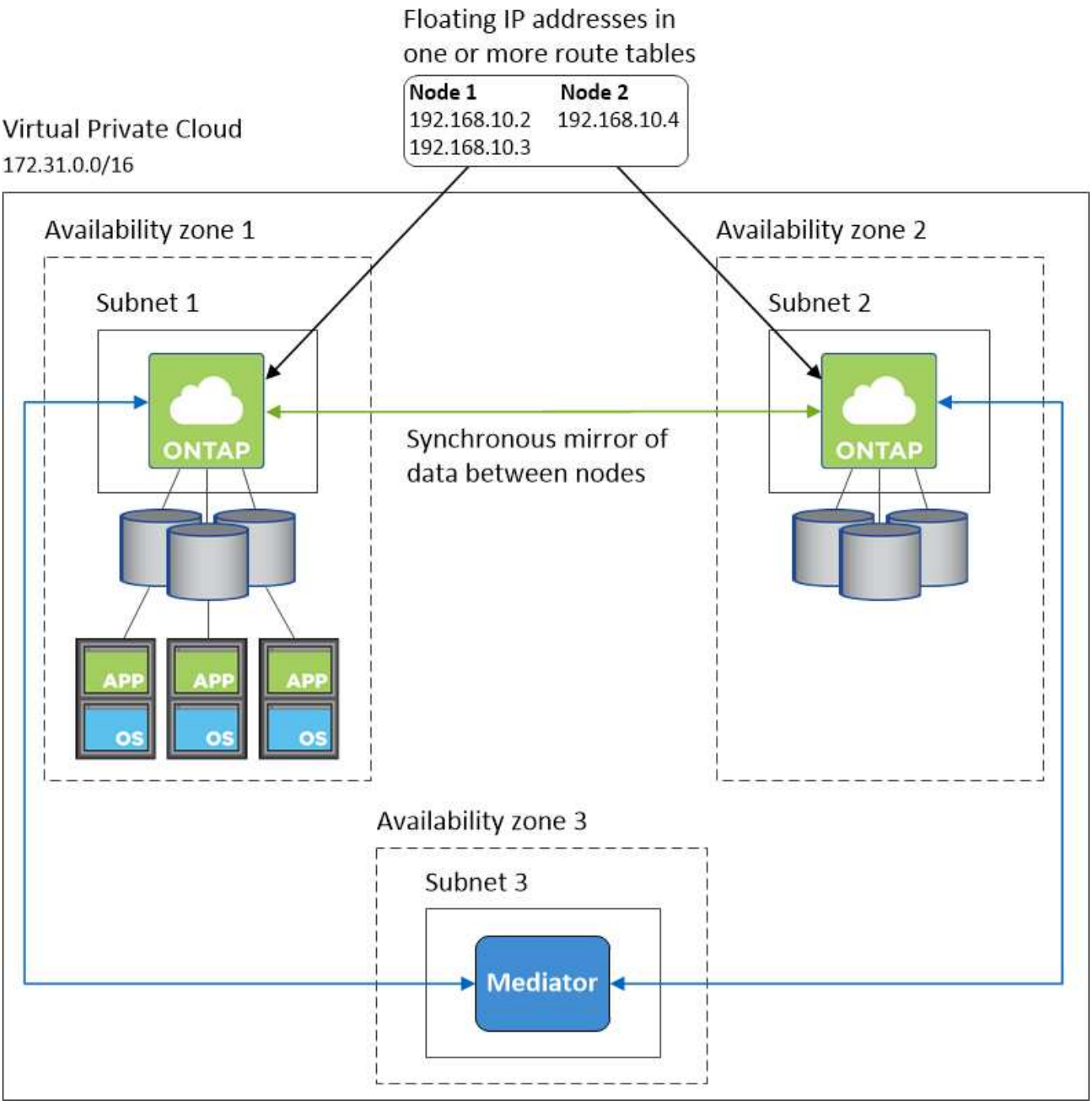
Conexão com ferramentas de gerenciamento do NetApp

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 de HA

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



Requisitos para o conetor

Configure sua rede para que o conetor possa gerenciar recursos e processos em seu ambiente de nuvem pública. O passo mais importante é garantir o acesso de saída à Internet a vários endpoints.

Se a rede utilizar um servidor proxy para toda a comunicação com a Internet, pode especificar o servidor proxy a partir da página Definições. "Configurando o conetor para usar um servidor proxy"Consulte a .

Conexão com redes de destino

Um conetor requer uma conexão de rede com os VPCs e VNets nos quais você deseja implantar o Cloud

Volumes ONTAP.

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

Acesso de saída à Internet

O conetor requer acesso de saída à Internet para gerenciar recursos e processos em seu ambiente de nuvem pública. Um conetor entra em Contato com os seguintes endpoints ao gerenciar recursos na AWS:

Endpoints	Finalidade
Serviços da AWS (amazonaws.com): • 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.
https://cloud.support.NetApp.com.s3.us-west-1.amazonaws.com	Fornece acesso a imagens de software, manifestos e modelos.
https://repo.cloud.support.NetApp.com	Usado para baixar dependências do Cloud Manager.
http://repo.mysql.com/	Usado para baixar MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-NetApp-com-accelerated.s3.amazonaws.com	Permite que o Cloud Manager acesse e baixe manifestos, modelos e imagens de atualização do Cloud Volumes ONTAP.
https://cloudmanagerinfraprod.azurecr.io	Acesso a imagens de software de componentes de contentor para uma infraestrutura que esteja executando o Docker e fornece uma solução para integrações de serviços com o Cloud Manager.
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.

Endpoints	Finalidade
https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist	Usado para adicionar seu ID de conta da AWS à lista de usuários permitidos para Backup em S3.
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/Entitlement - https://eval.lic.NetApp.com.s3.us-west-1.amazonaws.com - https://cloud-support-NetApp-com.s3.us-west-1.amazonaws.com	Comunicação com o NetApp para licenciamento de sistema e Registro de suporte.
https://ipa-signer.cloudmanager.NetApp.com	Permite que o Cloud Manager gere licenças (por exemplo, uma licença FlexCache para Cloud Volumes ONTAP)
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: • 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.

Embora você deva executar quase todas as tarefas a partir da interface de usuário SaaS, uma interface de usuário local ainda está disponível no conetor. A máquina que executa o navegador da Web deve ter conexões com os seguintes endpoints:

Endpoints	Finalidade
O host do conetor	Você deve inserir o endereço IP do host de um navegador da Web para carregar o console do Cloud Manager. Dependendo da sua conetividade com o seu provedor de nuvem, você pode usar o IP privado ou um IP público atribuído ao host: • 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 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.

Endpoints	Finalidade
https://auth0.com https://cdn.auth0.com://NetApp-cloud-account.auth0.com https://services.cloud.NetApp.com	Seu navegador da Web se coneta 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.

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

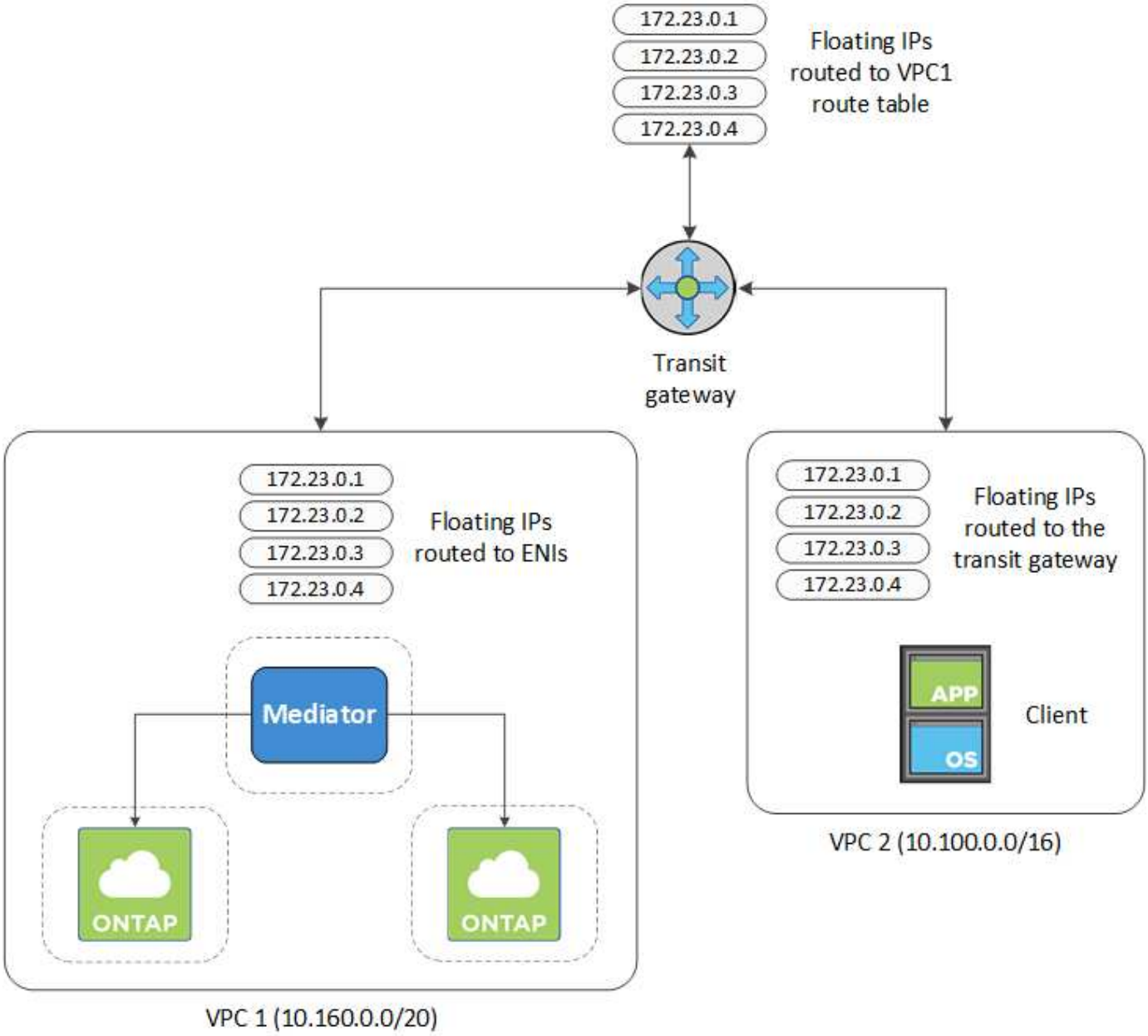
Configure um gateway de trânsito da AWS para permitir o acesso a um par de HA "Endereços IP flutuantes"de fora da VPC onde o par de HA reside.

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 nas 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 conetados 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.

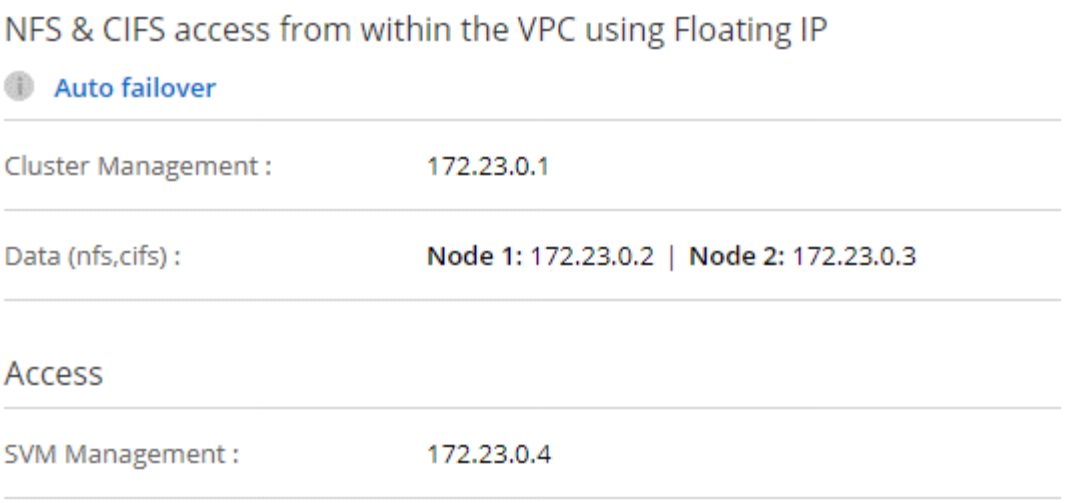


As etapas a seguir ilustram como configurar uma configuração semelhante.

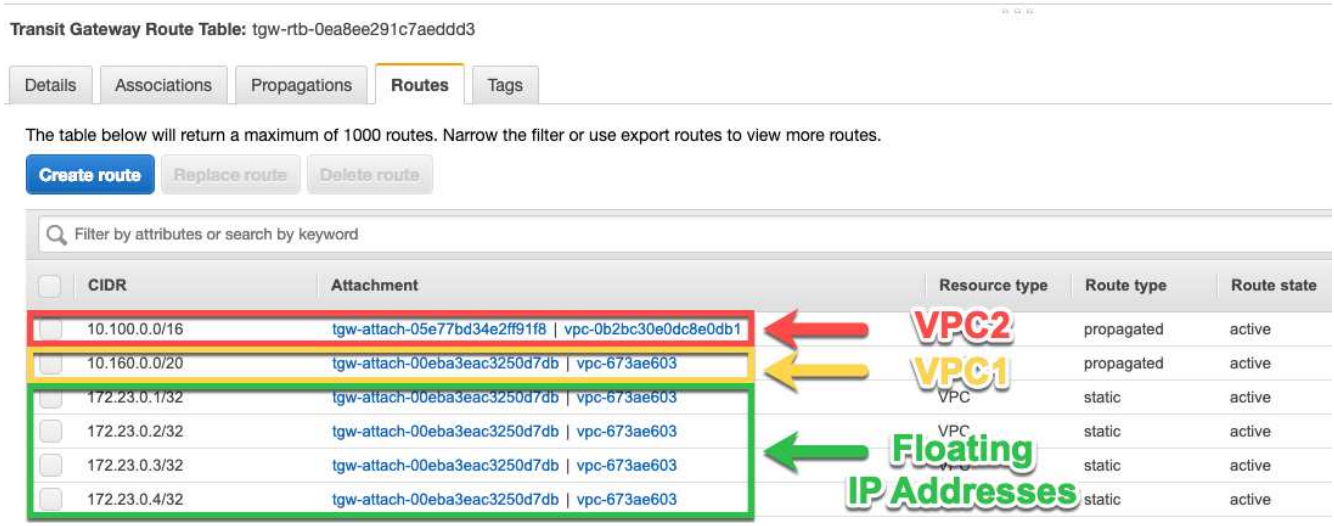
Passos

1. "Crie um gateway de trânsito e conete 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:



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.

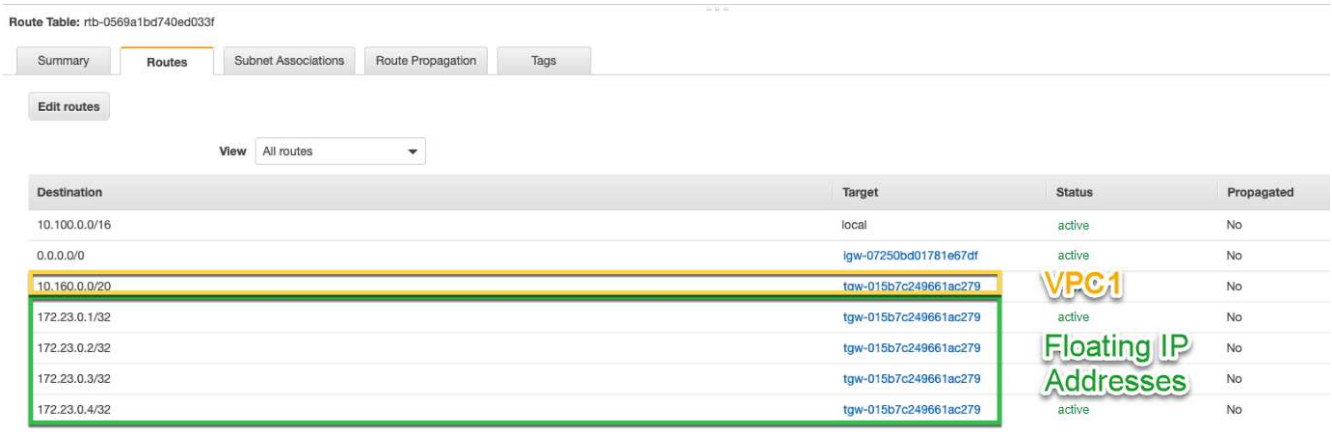


3. Modifique a tabela de rotas dos VPCs que precisam acessar os endereços IP flutuantes.

   a. Adicione entradas de rota aos endereços IP flutuantes.

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

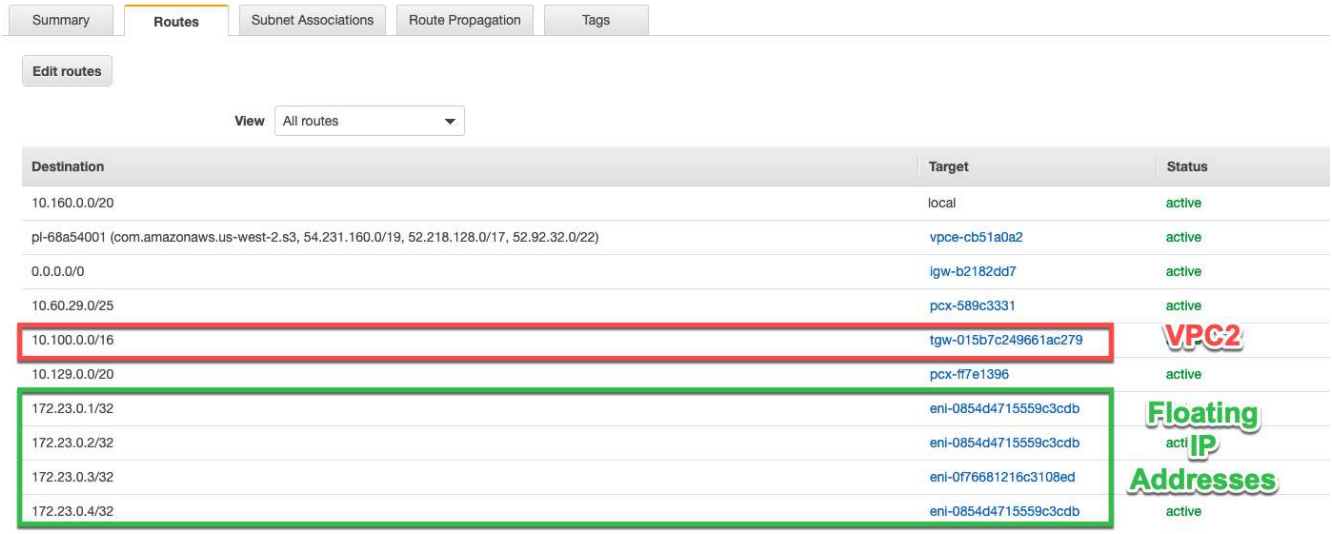
      A imagem de exemplo a seguir mostra a tabela de rotas para a VPC 2, que inclui rotas para a VPC 1 e os endereços IP flutuantes.



4. 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.

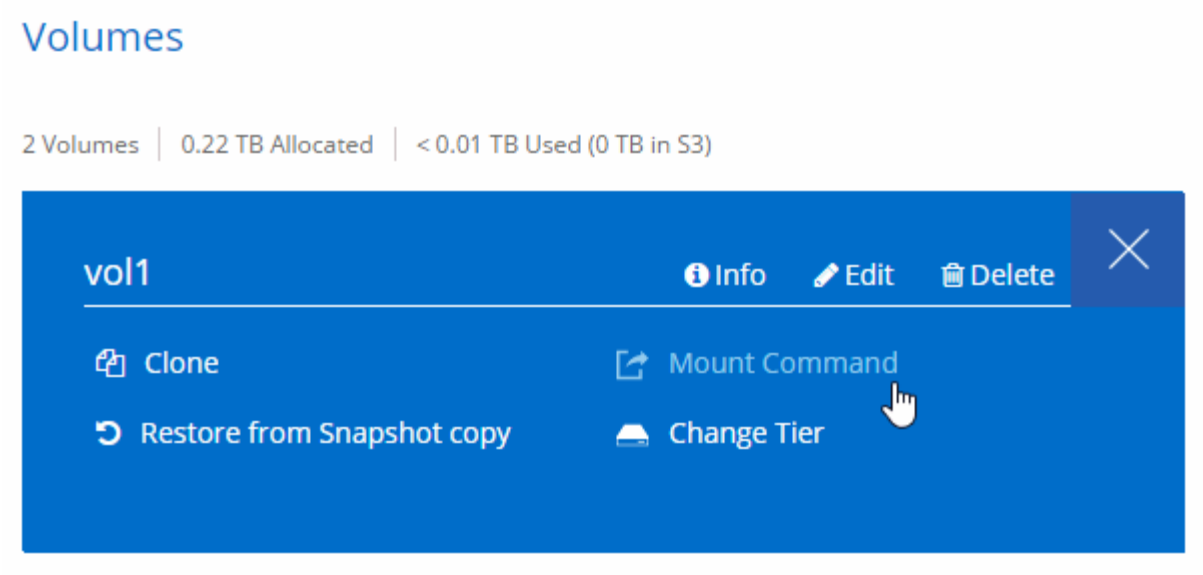
   Esta etapa é importante porque completa o roteamento entre os VPCs.

   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.



5. 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**.



- Ligações relacionadas*
- "Pares de alta disponibilidade na AWS"
- "Requisitos de rede para o Cloud Volumes ONTAP na AWS"

Regras do grupo de segurança para a AWS

O Cloud Manager cria grupos de segurança da AWS que incluem as regras de entrada e saída que o conetor e o Cloud Volumes ONTAP precisam operar com êxito. Você pode querer consultar as portas para fins de teste ou se preferir que o use seus próprios grupos de segurança.

Regras para Cloud Volumes ONTAP

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

Regras de entrada

A origem das regras de entrada no grupo de segurança predefinido é 0,0.0,0/0.

Protocolo	Porta	Finalidade
Todo o ICMP	Tudo	Fazer ping na instância
HTTP	80	Acesso HTTP ao console da Web do System Manager usando o endereço IP do LIF de gerenciamento de cluster
HTTPS	443	Acesso HTTPS ao console da Web do System Manager usando o endereço IP do LIF de gerenciamento de cluster
SSH	22	Acesso SSH ao endereço IP do LIF de gerenciamento de cluster ou um LIF de gerenciamento de nó
TCP	111	Chamada de procedimento remoto para NFS

Protocolo	Porta	Finalidade
TCP	139	Sessão de serviço NetBIOS para CIFS
TCP	161-162	Protocolo de gerenciamento de rede simples
TCP	445	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
TCP	635	Montagem em NFS
TCP	749	Kerberos
TCP	2049	Daemon do servidor NFS
TCP	3260	Acesso iSCSI através do iSCSI data LIF
TCP	4045	Daemon de bloqueio NFS
TCP	4046	Monitor de status da rede para NFS
TCP	10000	Backup usando NDMP
TCP	11104	Gestão de sessões de comunicação entre clusters para SnapMirror
TCP	11105	Transferência de dados SnapMirror usando LIFs entre clusters
UDP	111	Chamada de procedimento remoto para NFS
UDP	161-162	Protocolo de gerenciamento de rede simples
UDP	635	Montagem em NFS
UDP	2049	Daemon do servidor NFS
UDP	4045	Daemon de bloqueio NFS
UDP	4046	Monitor de status da rede para NFS
UDP	4049	Protocolo rquotad NFS

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 você 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	Finalidade
Todo o ICMP	Tudo	Todo o tráfego de saída
Todo o TCP	Tudo	Todo o tráfego de saída
Todos os UDP	Tudo	Todo o tráfego de saída

Regras de saída avançadas

Se você 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	Finalidade
Ative Directory					

	TCP	445	DATA LIF (NFS, CIFS)	Floresta do ative Directory	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
Serviço	**Protocolo**	**Porta**	**Fonte**	**Destino**	**Finalidade**
	TCP	464	DATA LIF (NFS, CIFS)	Floresta do ative Directory	Kerberos V alterar e definir senha (SET_CHANGE)
	UDP	464	DATA LIF (NFS, CIFS)	Floresta do ative Directory	Administração de chaves Kerberos
	TCP	749	DATA LIF (NFS, CIFS)	Floresta do ative Directory	Palavra-passe de alteração e definição Kerberos V (RPCSEC_GSS)
Cópia de segurança para S3	TCP	5010	LIF entre clusters	Ponto de extremidade de backup ou ponto de extremidade de restauração	Fazer backup e restaurar operações para o recurso Backup to S3
Cluster	Todo o tráfego	Todo o tráfego	Todos os LIFs em um nó	Todos os LIFs no outro nó	Comunicações entre clusters (apenas Cloud Volumes ONTAP HA)
	TCP	3000	LIF de gerenciamento de nós	Ha mediador	Chamadas ZAPI (somente Cloud Volumes ONTAP HA)
	ICMP	1	LIF de gerenciamento de nós	Ha mediador	Manter vivo (apenas Cloud Volumes ONTAP HA)
DHCP	UDP	68	LIF de gerenciamento de nós	DHCP	Cliente DHCP para configuração pela primeira vez
DHCPS	UDP	67	LIF de gerenciamento de nós	DHCP	Servidor DHCP
DNS	UDP	53	LIF e LIF de dados de gerenciamento de nós (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	LIF de gerenciamento de nós	Servidores de destino	Cópia NDMP
SMTP	TCP	25	LIF de gerenciamento de nós	Servidor de correio	Alertas SMTP, podem ser usados para AutoSupport

Serviço	Protocolo	Porta	Fonte	Destino	Finalidade
SNMP	TCP	161	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
	UDP	161	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
	TCP	162	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
	UDP	162	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
SnapMirror	TCP	11104	LIF entre clusters	LIFs ONTAP entre clusters	Gestão de sessões de comunicação entre clusters para SnapMirror
	TCP	11105	LIF entre clusters	LIFs ONTAP entre clusters	Transferência de dados SnapMirror
Syslog	UDP	514	LIF de gerenciamento de nós	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 de HA do Cloud Volumes ONTAP inclui as seguintes regras de entrada e saída.

Regras de entrada

A fonte para regras de entrada é 0,0.0,0/0.

Protocolo	Porta	Finalidade
SSH	22	Conexões SSH com o mediador HA
TCP	3000	Acesso à API RESTful a partir do conetor

Regras de saída

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

Regras básicas de saída

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

Protocolo	Porta	Finalidade
Todo o TCP	Tudo	Todo o tráfego de saída

Protocolo	Porta	Finalidade
Todos os UDP	Tudo	Todo o tráfego de saída

Regras de saída avançadas

Se você precisar de regras rígidas para o tráfego de saída, use as informações a seguir para abrir somente as portas necessárias para a comunicação de saída pelo mediador de HA.

Protocolo	Porta	Destino	Finalidade
HTTP	80	Endereço IP do conetor	Faça o download de atualizações para o mediador
HTTPS	443	Serviços de API da AWS	Assistência com failover de storage
UDP	53	Serviços de API da AWS	Assistência com failover de storage

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 do mediador HA

O grupo de segurança interno predefinido do mediador Cloud Volumes ONTAP HA inclui as seguintes regras. O Cloud Manager 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	Finalidade
Todo o tráfego	Tudo	Comunicação entre o mediador de HA e os nós de HA

Regras de saída

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

Protocolo	Porta	Finalidade
Todo o tráfego	Tudo	Comunicação entre o mediador de HA e os nós de HA

Regras para o conetor

O grupo de segurança do conetor requer regras de entrada e saída.

Regras de entrada

A origem das regras de entrada no grupo de segurança predefinido é 0,0.0,0/0.

Protocolo	Porta	Finalidade
SSH	22	Fornece acesso SSH ao host do conetor

Protocolo	Porta	Finalidade
HTTP	80	Fornece acesso HTTP a partir de navegadores da Web cliente para a interface de usuário local e conexões a partir do Cloud Compliance
HTTPS	443	Fornece acesso HTTPS a partir de navegadores da Web cliente para a interface de usuário local
TCP	3128	Fornece à instância de conformidade com a nuvem acesso à Internet, se sua rede AWS não usar um NAT ou proxy

Regras de saída

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

Regras básicas de saída

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

Protocolo	Porta	Finalidade
Todo o TCP	Tudo	Todo o tráfego de saída
Todos os UDP	Tudo	Todo o tráfego de saída

Regras de saída avançadas

Se você 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 conetor.

O endereço IP de origem é o host do conetor.

Serviço	Protocolo	Porta	Destino	Finalidade
Ative Directory	TCP	88	Floresta do ative Directory	Autenticação Kerberos V.
	TCP	139	Floresta do ative Directory	Sessão de serviço NetBIOS
	TCP	389	Floresta do ative Directory	LDAP
	TCP	445	Floresta do ative Directory	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
	TCP	464	Floresta do ative Directory	Kerberos V alterar e definir senha (SET_CHANGE)
	TCP	749	Floresta do ative Directory	Palavra-passe de alteração e definição Kerberos V do ative Directory (RPCSEC_GSS)
	UDP	137	Floresta do ative Directory	Serviço de nomes NetBIOS
	UDP	138	Floresta do ative Directory	Serviço de datagrama NetBIOS
	UDP	464	Floresta do ative Directory	Administração de chaves Kerberos
Chamadas de API e AutoSupport	HTTPS	443	LIF de gerenciamento de cluster de ONTAP e Internet de saída	Chamadas de API para AWS e ONTAP e envio de mensagens AutoSupport para o NetApp
Chamadas de API	TCP	3000	LIF de gerenciamento de clusters ONTAP	Chamadas de API para ONTAP
	TCP	8088	Cópia de segurança para S3	Chamadas de API para Backup para S3
DNS	UDP	53	DNS	Usado para resolução de DNS pelo Cloud Manager
Conformidade com a nuvem	HTTP	80	Instância de Cloud Compliance	Cloud Compliance para Cloud Volumes ONTAP

Informações sobre direitos autorais

Informações sobre marcas comerciais