Comece a usar o Azure

Cloud Manager 3.8

NetApp
October 22, 2024

Índice

Comece a usar o Azure

Introdução ao Cloud Volumes ONTAP para Azure

Comece a usar o Cloud Volumes ONTAP para Azure em alguns passos.

Crie um conetor

Se você ainda não tem um"Conetor", um administrador de conta precisa criar um. "Saiba como criar um conetor no Azure".

Quando você cria seu primeiro ambiente de trabalho do Cloud Volumes ONTAP, o Cloud Manager solicita que você implante um conetor se ainda não tiver um.

Planeje sua configuração

O Cloud Manager 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, você deve entender as opções disponíveis para você. "Saiba mais".

Configure a rede

1. Certifique-se de que o VNet e as sub-redes suportarão a conetividade entre o conetor e o Cloud Volumes ONTAP.
2. Ative o acesso de saída à Internet a partir do VNet de destino para que o conetor e o Cloud Volumes ONTAP possam contactar vários pontos de extremidade.

   Esta etapa é importante porque o conetor não pode gerenciar o Cloud Volumes ONTAP sem acesso de saída à Internet. Se precisar limitar a conetividade de saída, consulte a lista de endpoints para "O conetor e o Cloud Volumes ONTAP".

"Saiba mais sobre os requisitos de rede".

Inicie o Cloud Volumes ONTAP usando o Cloud Manager

Clique em **Adicionar ambiente de trabalho**, selecione o tipo de sistema que deseja implantar e conclua as etapas no assistente. "Leia as instruções passo a passo".

Links relacionados

- "A avaliar"
- "Criando um conetor do Cloud Manager"
- "Criando um conetor a partir do Azure Marketplace"
- "Instalar o software Connector em um host Linux"

- "O que o Cloud Manager faz com as permissões do Azure"

Planejando sua configuração do Cloud Volumes ONTAP no Azure

Ao implantar o Cloud Volumes ONTAP no Azure, você pode escolher um sistema pré-configurado que corresponda aos requisitos de workload ou criar sua própria configuração. Se você escolher sua própria configuração, você deve entender as opções disponíveis para você.

Escolhendo um tipo de licença

O Cloud Volumes ONTAP está disponível em duas opções de preço: Pagamento conforme o uso e traga sua própria licença (BYOL). Para pagamento conforme o uso, você pode escolher entre três licenças: Explore, Standard ou Premium. Cada licença oferece diferentes opções de computação e capacidade.

"Configurações compatíveis com o Cloud Volumes ONTAP 9,7 no Azure"

Compreender os limites de armazenamento

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

"Limites de storage para o Cloud Volumes ONTAP 9,7 no Azure"

Dimensionamento do seu sistema no Azure

O dimensionamento do seu sistema Cloud Volumes ONTAP pode ajudar você a atender aos requisitos de performance e capacidade. Você deve estar ciente de alguns pontos-chave ao escolher um tipo de VM, tipo de disco e tamanho de disco:

Tipo de máquina virtual

Observe os tipos de máquina virtual suportados no "Notas de versão do Cloud Volumes ONTAP" e, em seguida, revise os detalhes sobre cada tipo de VM suportado. Esteja ciente de que cada tipo de VM suporta um número específico de discos de dados.

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

Tipo de disco Azure

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

Os SISTEMAS HA usam blobs de página Premium. Enquanto isso, os sistemas de nó único podem usar dois tipos de discos gerenciados do Azure:

- *Discos gerenciados SSD premium* fornecem alto desempenho para cargas de trabalho com uso intenso de e/S a um custo mais alto.
- *Discos gerenciados SSD padrão* fornecem desempenho consistente para cargas de trabalho que exigem IOPS baixo.

- *Discos gerenciados HDD padrão* são uma boa escolha se você não precisa de IOPS alto e quer reduzir seus custos.

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

Tamanho do disco do Azure

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

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

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

O desempenho do armazenamento Premium do Azure está vinculado ao tamanho do disco. Discos maiores fornecem IOPS e taxa de transferência mais altas. Por exemplo, a escolha de discos de 1 TB pode proporcionar um melhor desempenho do que os discos de 500 GB, a um custo mais elevado.

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

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

- "Microsoft Azure: Preços de discos gerenciados"
- "Microsoft Azure: Preços de Blobs de páginas"

Escolhendo uma configuração compatível com Flash Cache

Uma configuração do Cloud Volumes ONTAP no Azure inclui armazenamento NVMe local, que o Cloud Volumes ONTAP usa como *Flash Cache* para melhor desempenho. "Saiba mais sobre o Flash Cache".

Planilha de informações de rede do Azure

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

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

Escolhendo uma velocidade de escrita

O Cloud Manager permite escolher uma configuração de velocidade de gravação para sistemas Cloud Volumes ONTAP de nó único. Antes de escolher uma velocidade de gravação, você deve entender as diferenças entre as configurações normal e alta e os riscos e recomendações ao usar alta velocidade de gravação.

Diferença entre velocidade de gravação normal e alta velocidade de gravação

Quando você escolhe a velocidade de gravação normal, os dados são gravados diretamente no disco, reduzindo assim a probabilidade de perda de dados no caso de uma falha não planejada do sistema.

Quando você escolhe alta velocidade de gravação, os dados são armazenados em buffer na memória antes de serem gravados no disco, o que proporciona um desempenho de gravação mais rápido. Devido a esse armazenamento em cache, existe o potencial de perda de dados se ocorrer uma falha não planejada do sistema.

A quantidade de dados que pode ser perdida no caso de uma falha não planejada do sistema é a extensão dos dois últimos pontos de consistência. Um ponto de consistência é o ato de gravar dados armazenados em buffer no disco. Um ponto de consistência ocorre quando o log de gravação está cheio ou após 10 segundos (o que ocorrer primeiro). No entanto, o desempenho do volume do AWS EBS pode afetar o tempo de processamento do ponto de consistência.

Quando usar alta velocidade de gravação

A alta velocidade de gravação é uma boa opção se for necessário um desempenho de gravação rápido para sua carga de trabalho e você pode resistir ao risco de perda de dados no caso de uma interrupção não planejada do sistema.

Recomendações ao usar alta velocidade de gravação

Se você ativar alta velocidade de gravação, deve garantir a proteção contra gravação na camada de aplicação.

Escolhendo um perfil de uso de volume

O ONTAP inclui vários recursos de eficiência de storage que podem reduzir a quantidade total de storage de que você precisa. Ao criar um volume no Cloud Manager, você pode escolher um perfil que ative esses recursos ou um perfil que os desabilite. Você deve aprender mais sobre esses recursos para ajudá-lo a decidir qual perfil usar.

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

Thin Provisioning

Apresenta storage mais lógico para hosts ou usuários do que você realmente tem no pool de storage físico. Em vez de pré-alocar espaço de armazenamento, o espaço de armazenamento é alocado dinamicamente a cada volume à medida que os dados são gravados.

Deduplicação

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 storage eliminando blocos redundantes de dados que residem no mesmo volume.

Compactação

Reduz a capacidade física necessária para armazenar dados comprimindo dados dentro de um volume em armazenamento primário, secundário e de arquivo.

Requisitos de rede para implantar e gerenciar o Cloud Volumes ONTAP no Azure

Configure sua rede Azure para que os sistemas Cloud Volumes ONTAP possam funcionar corretamente. Isso inclui a rede para o conetor e Cloud Volumes ONTAP.

Requisitos para o Cloud Volumes ONTAP

Os seguintes requisitos de rede devem ser atendidos no Azure.

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 para os seguintes endpoints para que o Cloud Volumes ONTAP possa enviar mensagens AutoSupport:

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

"Saiba como configurar o AutoSupport".

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, consulte as regras do grupo de segurança listadas abaixo.

Número de endereços IP

O Cloud Manager aloca o seguinte número de endereços IP para o Cloud Volumes ONTAP no Azure:

- Nó único: 5 endereços IP
- Par HA: 16 endereços IP

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

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.

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

Se você quiser categorizar dados inativos no storage de Blob do Azure, não precisa configurar uma conexão entre a categoria de performance e a categoria de capacidade, contanto que o Cloud Manager tenha as permissões necessárias. O Cloud Manager habilita um endpoint de serviço VNet para você se a política do Cloud Manager tiver estas permissões:

```
"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 .

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 .

Conexões 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 no 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.
https://cloud.support.NetApp.com.s3.us-west-1.amazonaws.com	Fornece acesso a imagens de software, manifestos e modelos.

Endpoints	Finalidade
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.
https://mysupport.NetApp.com	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.
*.blob.core.windows.net	Necessário para pares de HA ao usar um proxy.
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.
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.

Regras do grupo de segurança para o Cloud Volumes ONTAP

O Cloud Manager cria grupos de segurança do Azure que incluem as regras de entrada e saída que o Cloud Volumes ONTAP precisa para operar com sucesso. Você pode querer consultar as portas para fins de teste ou se preferir que o use seus próprios grupos de segurança.

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

Regras de entrada para sistemas de nó único

As regras listadas abaixo permitem tráfego, a menos que a descrição observe que bloqueia tráfego de entrada específico.

Prioridade e nome	Porta e protocolo	Origem e destino	Descrição
1000 inbound_ssh	22 TCP	Qualquer a qualquer	Acesso SSH ao endereço IP do LIF de gerenciamento de cluster ou um LIF de gerenciamento de nó
1001 inbound_http	80 TCP	Qualquer a qualquer	Acesso HTTP ao console da Web do System Manager usando o endereço IP do LIF de gerenciamento de cluster

Prioridade e nome	Porta e protocolo	Origem e destino	Descrição
1002 inbound_111_tcp	111 TCP	Qualquer a qualquer	Chamada de procedimento remoto para NFS
1003 inbound_111_udp	111 UDP	Qualquer a qualquer	Chamada de procedimento remoto para NFS
1004 inbound_139	139 TCP	Qualquer a qualquer	Sessão de serviço NetBIOS para CIFS
1005 inbound_161-162 _tcp	161-162 TCP	Qualquer a qualquer	Protocolo de gerenciamento de rede simples
1006 inbound_161-162 _udp	161-162 UDP	Qualquer a qualquer	Protocolo de gerenciamento de rede simples
1007 inbound_443	443 TCP	Qualquer a qualquer	Acesso HTTPS ao console da Web do System Manager usando o endereço IP do LIF de gerenciamento de cluster
1008 inbound_445	445 TCP	Qualquer a qualquer	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
1009 inbound_635_tcp	635 TCP	Qualquer a qualquer	Montagem em NFS
1010 inbound_635_udp	635 UDP	Qualquer a qualquer	Montagem em NFS
1011 inbound_749	749 TCP	Qualquer a qualquer	Kerberos
1012 inbound_2049_tcp	2049 TCP	Qualquer a qualquer	Daemon do servidor NFS
1013 inbound_2049_udp	2049 UDP	Qualquer a qualquer	Daemon do servidor NFS
1014 inbound_3260	3260 TCP	Qualquer a qualquer	Acesso iSCSI através do iSCSI data LIF
1015 inbound_4045-4046_tcp	4045-4046 TCP	Qualquer a qualquer	Daemon de bloqueio NFS e monitor de status da rede
1016 inbound_4045-4046_udp	4045-4046 UDP	Qualquer a qualquer	Daemon de bloqueio NFS e monitor de status da rede
1017 inbound_10000	10000 TCP	Qualquer a qualquer	Backup usando NDMP
1018 inbound_11104-11105	11104-11105 TCP	Qualquer a qualquer	Transferência de dados SnapMirror
3000 inbound_deny _all_tcp	Qualquer porta TCP	Qualquer a qualquer	Bloquear todo o outro tráfego de entrada TCP
3001 inbound_deny _all_udp	Qualquer porta UDP	Qualquer a qualquer	Bloqueie todo o outro tráfego de entrada UDP

Prioridade e nome	Porta e protocolo	Origem e destino	Descrição
65000 AllowVnetInBound	Qualquer porta de qualquer protocolo	VirtualNetwork para VirtualNetwork	Tráfego de entrada de dentro da VNet
65001 AllowAzureLoad BalancerInBound	Qualquer porta de qualquer protocolo	AzureLoadBalancer para qualquer	Tráfego de dados do Azure Standard Load Balancer
65500 DenyAllInBound	Qualquer porta de qualquer protocolo	Qualquer a qualquer	Bloquear todo o outro tráfego de entrada

Regras de entrada para sistemas HA

As regras listadas abaixo permitem tráfego, a menos que a descrição observe que bloqueia tráfego de entrada específico.

Os SISTEMAS HA têm menos regras de entrada do que os sistemas de nó único porque o tráfego de dados de entrada passa pelo Azure Standard Load Balancer. Devido a isso, o tráfego do Load Balancer deve estar aberto, como mostrado na regra "AllowAzureLoadBalancerInBound".

Prioridade e nome	Porta e protocolo	Origem e destino	Descrição
100 inbound_443	443 qualquer protocolo	Qualquer a qualquer	Acesso HTTPS ao console da Web do System Manager usando o endereço IP do LIF de gerenciamento de cluster
101 inbound_111_tcp	111 qualquer protocolo	Qualquer a qualquer	Chamada de procedimento remoto para NFS
102 inbound_2049_tcp	2049 qualquer protocolo	Qualquer a qualquer	Daemon do servidor NFS
111 inbound_ssh	22 qualquer protocolo	Qualquer a qualquer	Acesso SSH ao endereço IP do LIF de gerenciamento de cluster ou um LIF de gerenciamento de nó
121 inbound_53	53 qualquer protocolo	Qualquer a qualquer	DNS e CIFS
65000 AllowVnetInBound	Qualquer porta de qualquer protocolo	VirtualNetwork para VirtualNetwork	Tráfego de entrada de dentro da VNet
65001 AllowAzureLoad BalancerInBound	Qualquer porta de qualquer protocolo	AzureLoadBalancer para qualquer	Tráfego de dados do Azure Standard Load Balancer
65500 DenyAllInBound	Qualquer porta de qualquer protocolo	Qualquer a qualquer	Bloquear todo o outro tráfego de entrada

Regras de saída

O grupo de segurança predefinido para o Cloud Volumes ONTAP abre todo o tráfego de saída. Se isso for

aceitável, siga as regras básicas de saída. Se 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.

Porta	Protocolo	Finalidade
Tudo	Todo o TCP	Todo o tráfego de saída
Tudo	Todos os UDP	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	Porta	Protocolo	Fonte	Destino	Finalidade
Ative Directory					

Serviço	Porta	Protocolo	Fonte	Destino	Finalidade
	389	TCP E UDP	DATA LIF (NFS, CIFS)	Floresta do ative Directory	LDAP
	445	TCP	DATA LIF (NFS, CIFS)	Floresta do ative Directory	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
	464	TCP	DATA LIF (NFS, CIFS)	Floresta do ative Directory	Kerberos V alterar e definir senha (SET_CHANGE)
	464	UDP	DATA LIF (NFS, CIFS)	Floresta do ative Directory	Administração de chaves Kerberos
	749	TCP	DATA LIF (NFS, CIFS)	Floresta do ative Directory	Palavra-passe de alteração e definição Kerberos V (RPCSEC_GSS)
DHCP	68	UDP	LIF de gerenciamento de nós	DHCP	Cliente DHCP para configuração pela primeira vez
DHCPS	67	UDP	LIF de gerenciamento de nós	DHCP	Servidor DHCP
DNS	53	UDP	LIF e LIF de dados de gerenciamento de nós (NFS, CIFS)	DNS	DNS
NDMP	18600–18699	TCP	LIF de gerenciamento de nós	Servidores de destino	Cópia NDMP
SMTP	25	TCP	LIF de gerenciamento de nós	Servidor de correio	Alertas SMTP, podem ser usados para AutoSupport
SNMP	161	TCP	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
	161	UDP	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
	162	TCP	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
	162	UDP	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
SnapMirror	11104	TCP	LIF entre clusters	LIFs ONTAP entre clusters	Gestão de sessões de comunicação entre clusters para SnapMirror
	11105	TCP	LIF entre clusters	LIFs ONTAP entre clusters	Transferência de dados SnapMirror
Syslog	514	UDP	LIF de gerenciamento de nós	Servidor syslog	Mensagens de encaminhamento do syslog

Regras do grupo de segurança 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.

Porta	Protocolo	Finalidade
22	SSH	Fornece acesso SSH ao host do conetor
80	HTTP	Fornece acesso HTTP a partir de navegadores da Web cliente para a interface de usuário local
443	HTTPS	Fornece acesso HTTPS a partir de navegadores da Web cliente para a interface de usuário local

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.

Porta	Protocolo	Finalidade
Tudo	Todo o TCP	Todo o tráfego de saída
Tudo	Todos os UDP	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	Porta	Protocolo	Destino	Finalidade
Ative Directory	88	TCP	Floresta do ative Directory	Autenticação Kerberos V.
	139	TCP	Floresta do ative Directory	Sessão de serviço NetBIOS
	389	TCP	Floresta do ative Directory	LDAP
	445	TCP	Floresta do ative Directory	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
	464	TCP	Floresta do ative Directory	Kerberos V alterar e definir senha (SET_CHANGE)
	749	TCP	Floresta do ative Directory	Palavra-passe de alteração e definição Kerberos V do ative Directory (RPCSEC_GSS)
	137	UDP	Floresta do ative Directory	Serviço de nomes NetBIOS
	138	UDP	Floresta do ative Directory	Serviço de datagrama NetBIOS
	464	UDP	Floresta do ative Directory	Administração de chaves Kerberos
Chamadas de API e AutoSupport	443	HTTPS	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	3000	TCP	LIF de gerenciamento de clusters ONTAP	Chamadas de API para ONTAP
DNS	53	UDP	DNS	Usado para resolução de DNS pelo Cloud Manager

Iniciar o Cloud Volumes ONTAP no Azure

Você pode iniciar um sistema de nó único ou um par de HA no Azure criando um ambiente de trabalho do Cloud Volumes ONTAP no Cloud Manager.

Antes de começar

- Você deve ter um "Conetor associado ao workspace".

Você deve ser um administrador de conta para criar um conetor. Quando você cria seu primeiro ambiente de trabalho do Cloud Volumes ONTAP, o Cloud Manager solicita que você crie um conetor se ainda não tiver um.

- "Você deve estar preparado para deixar o conetor funcionando o tempo todo".
- Você deve ter escolhido uma configuração e obtido informações de rede do Azure do administrador. Para obter detalhes, "Planejando sua configuração do Cloud Volumes ONTAP"consulte .
- Para implantar um sistema BYOL, você precisa do número de série de 20 dígitos (chave de licença) para cada nó.

Sobre esta tarefa

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

Potencial para perda de dados

A implantação do Cloud Volumes ONTAP em um grupo de recursos compartilhados existente não é recomendada devido ao risco de perda de dados. Embora a reversão esteja atualmente desativada por padrão ao usar a API para implantar em um grupo de recursos existente, excluir o Cloud Volumes ONTAP potencialmente excluirá outros recursos desse grupo compartilhado.

A prática recomendada é usar um novo grupo de recursos dedicado para o Cloud Volumes ONTAP. Essa é a opção padrão e recomendada somente ao implantar o Cloud Volumes ONTAP no Azure a partir do Gerenciador de nuvem.

Passos

1. Na página ambientes de trabalho, clique em **Adicionar ambiente de trabalho** e siga as instruções.
2. **Escolha um local**: Selecione **Microsoft Azure** e **nó único Cloud Volumes ONTAP** ou **alta disponibilidade Cloud Volumes ONTAP**.
3. **Detalhes e credenciais**: Opcionalmente, altere as credenciais e a assinatura do Azure, especifique um nome de cluster e um nome de grupo de recursos, adicione tags se necessário e especifique credenciais.

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

Campo	Descrição
Nome do ambiente de trabalho	O Cloud Manager usa o nome do ambiente de trabalho para nomear o sistema Cloud Volumes ONTAP e a máquina virtual do Azure. Ele também usa o nome como prefixo para o grupo de segurança predefinido, se você selecionar essa opção.
Nome Grupo recursos	Mantenha o nome padrão para o novo grupo de recursos ou desmarque **usar padrão** e insira seu próprio nome para o novo grupo de recursos. A prática recomendada é usar um novo grupo de recursos dedicado para o Cloud Volumes ONTAP. Embora seja possível implantar o Cloud Volumes ONTAP em um grupo de recursos compartilhado existente usando a API, isso não é recomendado devido ao risco de perda de dados. Consulte o aviso acima para obter mais detalhes.

Campo	Descrição
Tags	As tags são metadados para seus recursos do Azure. Quando você insere tags neste campo, o Cloud Manager as adiciona ao grupo de recursos associado ao sistema Cloud Volumes ONTAP. Você pode adicionar até quatro tags da interface do usuário ao criar um ambiente de trabalho e, em seguida, você pode adicionar mais após a criação. Observe que a API não limita a quatro tags ao criar um ambiente de trabalho. Para obter informações sobre tags, "Documentação do Microsoft Azure: Usando tags para organizar seus recursos do Azure" consulte .
Nome de utilizador e palavra-passe	Essas são as credenciais da conta de administrador do cluster do Cloud Volumes ONTAP. Você pode usar essas credenciais para se conetar ao Cloud Volumes ONTAP por meio do OnCommand System Manager ou da CLI.
Editar credenciais	Você pode escolher diferentes credenciais do Azure e uma assinatura diferente do Azure para usar com este sistema Cloud Volumes ONTAP. Você precisa associar uma assinatura do Azure Marketplace à assinatura do Azure selecionada para implantar um sistema Cloud Volumes ONTAP pay-as-you-go. "Saiba como adicionar credenciais".

O vídeo a seguir mostra como associar uma assinatura do Marketplace a uma assinatura do Azure:

► https://docs.netapp.com/pt-br/occm38//media/video_subscribing_azure.mp4 *(video)*

4. **Serviços**: Mantenha os serviços ativados ou desative os serviços individuais que você não deseja usar com o Cloud Volumes ONTAP.
   - "Saiba mais sobre o Cloud Compliance".
   - "Saiba mais sobre o Backup to Cloud".
5. **Localização e conetividade**: Selecione um local e um grupo de segurança e marque a caixa de seleção para confirmar a conetividade de rede entre o Cloud Manager e o local de destino.
6. **Conta do site de suporte e licença**: Especifique se você deseja usar o pagamento conforme o uso ou o BYOL e especifique uma conta do site de suporte da NetApp.

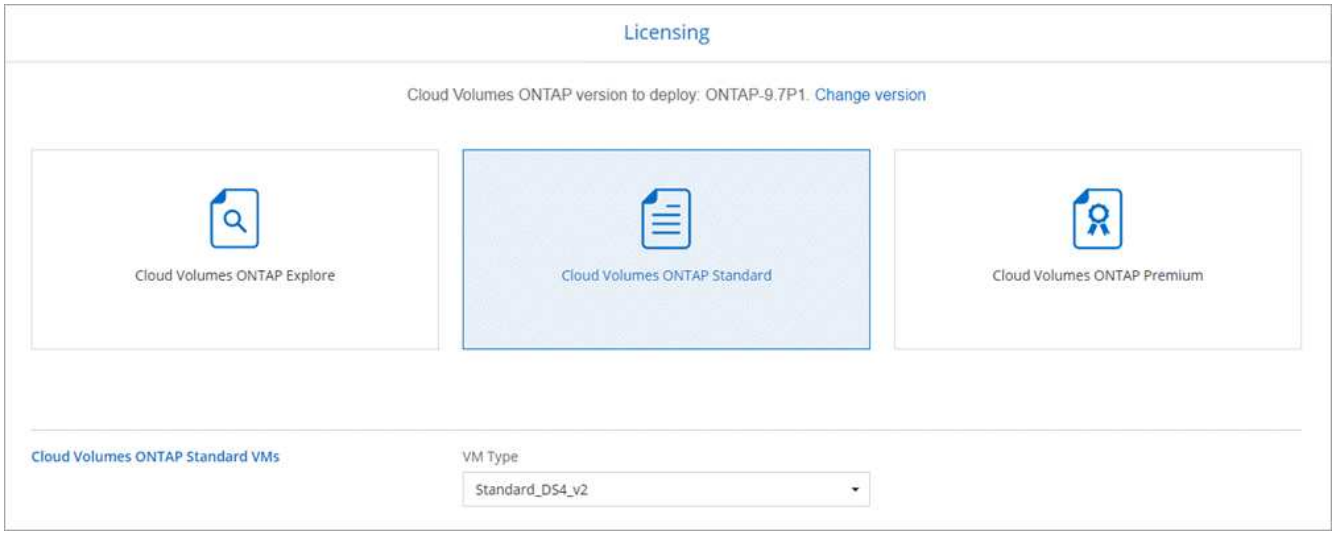
   Para entender como as licenças funcionam, "Licenciamento"consulte .

   Uma conta do site de suporte da NetApp é opcional para pagamento conforme o uso, mas necessária para sistemas BYOL. "Saiba como adicionar contas do site de suporte da NetApp".

7. **Pacotes pré-configurados**: Selecione um dos pacotes para implantar rapidamente um sistema Cloud Volumes ONTAP ou clique em **criar minha própria configuração**.

   Se você escolher um dos pacotes, você só precisa especificar um volume e, em seguida, revisar e aprovar a configuração.

8. **Licenciamento**: Altere a versão do Cloud Volumes ONTAP conforme necessário, selecione uma licença e selecione um tipo de máquina virtual.



Se suas necessidades mudarem depois de iniciar o sistema, você poderá modificar a licença ou o tipo de máquina virtual mais tarde.

> Se uma versão mais recente do Release Candidate, General Availability ou patch estiver disponível para a versão selecionada, o Cloud Manager atualizará o sistema para essa versão ao criar o ambiente de trabalho. Por exemplo, a atualização ocorre se você selecionar Cloud Volumes ONTAP 9,6 RC1 e 9,6 GA estiver disponível. A atualização não ocorre de uma versão para outra, por exemplo, de 9,6 a 9,7.

9. **Assine no Azure Marketplace**: Siga as etapas se o Cloud Manager não puder habilitar implantações programáticas do Cloud Volumes ONTAP.
10. **Recursos de armazenamento subjacentes**: Escolha configurações para o agregado inicial: Um tipo de disco, um tamanho para cada disco e se a disposição de dados em camadas para armazenamento Blob deve ser ativada.

    Observe o seguinte:

    - O tipo de disco é para o volume inicial. Você pode escolher um tipo de disco diferente para volumes subsequentes.
    - O tamanho do disco é para todos os discos no agregado inicial e para quaisquer agregados adicionais criados pelo Cloud Manager quando você usa a opção de provisionamento simples. Você pode criar agregados que usam um tamanho de disco diferente usando a opção Alocação avançada.

      Para obter ajuda sobre como escolher um tipo e tamanho de disco, "Dimensionamento do seu sistema no Azure"consulte .

    - Você pode escolher uma política específica de disposição em categorias de volume ao criar ou editar um volume.
    - Se você desativar a disposição de dados em categorias, poderá ativá-la em agregados subsequentes.

      "Saiba mais sobre categorização de dados".

11. **Velocidade de gravação e WORM** (somente sistemas de nó único): Escolha a velocidade de gravação **normal** ou **alta** e ative o armazenamento WORM (write once, read many), se desejado.

    A escolha de uma velocidade de gravação é compatível apenas com sistemas de nó único.

"Saiba mais sobre a velocidade de escrita".

O WORM não pode ser ativado se a disposição de dados em camadas estiver ativada.

"Saiba mais sobre o armazenamento WORM".

12. **Comunicação segura com armazenamento e WORM** (somente HA): Escolha se deseja habilitar uma conexão HTTPS a contas de storage do Azure e ative o armazenamento WORM (write once, read many), se desejado.

    A conexão HTTPS é de um par de HA do Cloud Volumes ONTAP 9,7 para contas de storage do Azure. Observe que ativar essa opção pode afetar o desempenho de gravação. Não é possível alterar a configuração depois de criar o ambiente de trabalho.

    "Saiba mais sobre o armazenamento WORM".

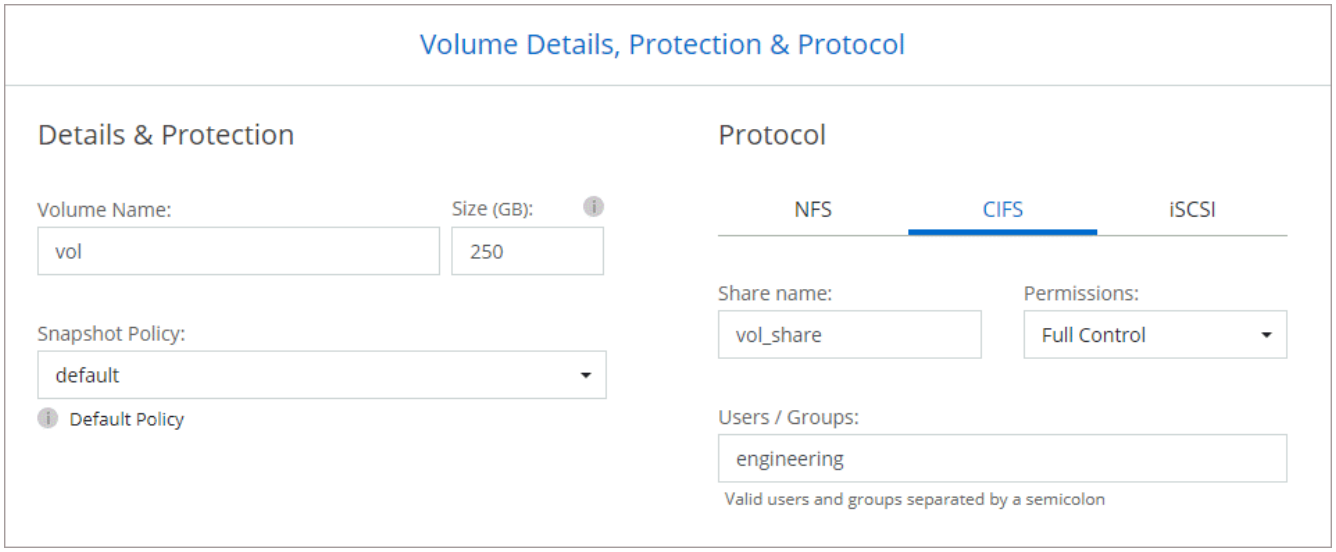
13. **Criar volume**: Insira os detalhes do novo volume ou clique em **Ignorar**.

    Alguns dos campos desta página são auto-explicativos. 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, em grande parte, se você ativar o provisionamento de thin, o que permite criar um volume maior do que o armazenamento físico atualmente disponível para ele.
Controle de acesso (somente para NFS)	Uma política de exportação define os clientes na sub-rede que podem acessar o volume. Por padrão, o Cloud Manager insere um valor que fornece acesso a todas as instâncias na sub-rede.
Permissões e utilizadores/grupos (apenas para CIFS)	Esses campos permitem controlar 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 do Windows locais ou de domínio, ou usuários ou grupos UNIX. Se você especificar um nome de usuário do domínio do Windows, você deve incluir o domínio do usuário usando o nome de domínio do formato.
Política de instantâneos	Uma política de cópia Snapshot especifica a frequência e o número de cópias snapshot do NetApp criadas automaticamente. Uma cópia Snapshot do NetApp é uma imagem pontual do sistema de arquivos que não afeta a performance e exige o mínimo de storage. 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 NFS para o volume: NFSv3 ou NFSv4.

Campo	Descrição
Grupo de iniciadores e IQN (apenas 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 conetam à rede por meio de adaptadores de rede Ethernet (NICs) padrão, placas de mecanismo de descarga TCP (TOE) com iniciadores de software, adaptadores de rede convergidos (CNAs) ou adaptadores de barramento de host dedicados (HBAs) e são identificados por IQNs (iSCSI Qualified Names). Quando você cria um volume iSCSI, o Cloud Manager cria automaticamente um LUN para você. Simplificamos a criação de apenas um LUN por volume, para que não haja gerenciamento envolvido. Depois de criar o volume, "Use o IQN para se conetar ao LUN a partir de seus hosts".

A imagem seguinte mostra a página volume preenchida para o protocolo CIFS:



14. **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 ative Directory e os controladores de domínio para o domínio em que o servidor CIFS irá ingressar.
Ative Directory Domain para aderir	O FQDN do domínio do ative Directory (AD) ao qual você deseja que o servidor CIFS se associe.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores à unidade organizacional especificada (ou) dentro do domínio do AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio AD.

Campo	Descrição
Unidade organizacional	A unidade organizacional dentro do domínio AD a associar ao servidor CIFS. A predefinição é computadores. Para configurar os Serviços de domínio do Azure AD como o servidor AD para o Cloud Volumes ONTAP, você deve inserir **computadores AADDC** ou **usuários AADDC** neste campo. "Documentação do Azure: Crie uma unidade organizacional (ou) em um domínio gerenciado dos Serviços de domínio do Azure AD"
Domínio DNS	O domínio DNS da máquina virtual de storage (SVM) do Cloud Volumes ONTAP. Na maioria dos casos, o domínio é o mesmo que o domínio AD.
NTP Server	Selecione **Use ative Directory Domain** para configurar um servidor NTP usando o DNS do ative Directory. Se você precisa configurar um servidor NTP usando um endereço diferente, então você deve usar a API. Consulte "Guia do desenvolvedor de API do Cloud Manager"para obter detalhes.

15. **Perfil de uso, tipo de disco e Política de disposição em categorias**: Escolha se você deseja habilitar os recursos de eficiência de storage e alterar a política de disposição em categorias de volume, se necessário.

    Para obter mais informações, "Compreender os perfis de utilização de volume"consulte e "Visão geral de categorização de dados".

16. **Rever & aprovar**: Revise e confirme suas seleções.
    a. Reveja os detalhes sobre a configuração.
    b. Clique em **mais informações** para analisar detalhes sobre o suporte e os recursos do Azure que o Cloud Manager adquirirá.
    c. Selecione as caixas de verificação **I understand…**.
    d. Clique em **Go**.

Resultado

O Cloud Manager implanta o sistema Cloud Volumes ONTAP. Você pode acompanhar o progresso na linha do tempo.

Se você tiver algum problema na implantação do sistema Cloud Volumes ONTAP, revise a mensagem de falha. Você também pode selecionar o ambiente de trabalho e clicar em **Re-create environment**.

Para obter ajuda adicional, vá "Suporte à NetApp Cloud Volumes ONTAP" para .

Depois de terminar

- Se você provisionou um compartilhamento CIFS, dê 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 a volumes, use o System Manager ou a CLI.

  As cotas permitem restringir ou rastrear o espaço em disco e o número de arquivos usados por um usuário, grupo ou qtree.

Informações sobre direitos autorais

Informações sobre marcas comerciais