



## **Comece no Microsoft Azure**

### **Cloud Volumes ONTAP**

NetApp  
February 17, 2026

This PDF was generated from <https://docs.netapp.com/pt-br/storage-management-cloud-volumes-ontap/concept-azure-mktplace-direct.html> on February 17, 2026. Always check docs.netapp.com for the latest.

# Índice

Comece no Microsoft Azure .....	1
Saiba mais sobre as opções de implantação do Cloud Volumes ONTAP no Azure .....	1
Introdução ao NetApp Console .....	2
Início rápido para Cloud Volumes ONTAP no Azure .....	2
Planeje sua configuração do Cloud Volumes ONTAP no Azure .....	3
Configurar a rede do Azure para o Cloud Volumes ONTAP .....	6
Configurar o Cloud Volumes ONTAP para usar uma chave gerenciada pelo cliente no Azure .....	17
Configurar o licenciamento do Cloud Volumes ONTAP no Azure .....	22
Habilitar o modo de alta disponibilidade para o Cloud Volumes ONTAP no Azure .....	28
Habilitar VMOrchestratorZonalMultiFD para Cloud Volumes ONTAP no Azure .....	30
Inicie o Cloud Volumes ONTAP no Azure .....	31
Verificar imagem da plataforma Azure .....	44
Implantar o Cloud Volumes ONTAP no marketplace do Azure .....	55
Solucionar problemas de implantação .....	57
Descubra os sistemas implantados no Console .....	57

# Comece no Microsoft Azure

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

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

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

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

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

	Mercado do Azure	NetApp Console
<b>Integração</b>	Mais curto e fácil, com preparação mínima necessária para implantação direta	Processo de integração mais longo, incluindo a instalação do agente do Console
<b>Tipos de máquinas virtuais (VM) suportados</b>	Tipos de instância Eds_v5 e Ls_v3	Gama completa de tipos de VM. <a href="https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-azure.html">https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-azure.html</a> ["Configurações com suporte no Azure"]
<b>Licença</b>	Licença gratuita	Qualquer licença baseada em capacidade. <a href="#">"Licenciamento do Cloud Volumes ONTAP"</a>
* Suporte NetApp *	Não incluído	Disponível, com base no tipo de licença
<b>Capacidade</b>	Até 500 GiB	Expansível por configuração
<b>Modelo de implantação</b>	Implantação do modo de alta disponibilidade (HA) em zona de disponibilidade única (AZ)	Todas as configurações suportadas, incluindo modos de nó único e HA, implantações de AZ únicas e múltiplas

	<b>Mercado do Azure</b>	<b>NetApp Console</b>
<b>Tipo de disco suportado</b>	Discos gerenciados SSD v2 premium	Suporte mais amplo. <a href="#">"Configuração padrão para Cloud Volumes ONTAP"</a>
<b>Velocidade de gravação (modo de gravação rápida)</b>	Não suportado	Suportado, com base na sua configuração. <a href="#">"Saiba mais sobre velocidades de gravação no Cloud Volumes ONTAP"</a> .
<b>Capacidade de orquestração</b>	Não disponível	Disponível por meio do NetApp Console, com base no tipo de licença
<b>Número de VMs de armazenamento suportadas</b>	Um por implantação	Várias VMs de armazenamento, com base na sua configuração. <a href="#">"Número suportado de VMs de armazenamento"</a>
<b>Alterando o tipo de instância</b>	Não suportado	Suportado
* Hierarquização do FabricPool *	Não suportado	Suportado

#### Links relacionados

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

## Introdução ao NetApp Console

### Início rápido para Cloud Volumes ONTAP no Azure

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

1

#### Criar um agente de console

Se você não tem um ["Agente de console"](#) no entanto, você precisa criar um. ["Aprenda a criar um agente de console no Azure"](#)

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

2

#### Planeje sua configuração

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

### 3

#### Configure sua rede

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

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

["Saiba mais sobre os requisitos de rede"](#) .

### 4

#### Inicie o Cloud Volumes ONTAP

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

#### Links relacionados

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

## Planeje sua configuração do Cloud Volumes ONTAP no Azure

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

#### Escolha uma licença do Cloud Volumes ONTAP

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

- ["Saiba mais sobre as opções de licenciamento do Cloud Volumes ONTAP"](#)
- ["Aprenda como configurar o licenciamento"](#)

#### Escolha uma região com suporte

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

#### Escolha um tipo de VM compatível

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

["Configurações com suporte para Cloud Volumes ONTAP no Azure"](#)

## Entenda os limites de armazenamento

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

["Limites de armazenamento para Cloud Volumes ONTAP no Azure"](#)

## Dimensione seu sistema no Azure

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

### Tipo de máquina virtual

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

- ["Documentação do Azure: Tamanhos de máquinas virtuais de uso geral"](#)
- ["Documentação do Azure: tamanhos de máquinas virtuais otimizados para memória"](#)

### Tipo de disco do Azure com sistemas de nó único

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

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

- *Discos SSD gerenciados premium* oferecem alto desempenho para cargas de trabalho com uso intensivo de E/S a um custo mais alto.
- *Discos gerenciados SSD v2 Premium* oferecem maior desempenho com menor latência e menor custo, em comparação aos discos gerenciados SSD Premium.
- *Discos gerenciados SSD padrão* fornecem desempenho consistente para cargas de trabalho que exigem IOPS baixo.
- *Discos gerenciados de HDD padrão* são uma boa escolha se você não precisa de IOPS alto e quer reduzir seus custos.

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

### Tipo de disco do Azure com pares de alta disponibilidade

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

### Tamanho do disco do Azure

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



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

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

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

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

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

- ["Microsoft Azure: preços de discos gerenciados"](#)
- ["Microsoft Azure: preços de Page Blobs"](#)

### Exibir discos de sistema padrão

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

["Exibir os discos padrão para dados do sistema Cloud Volumes ONTAP no Azure"](#) .



O agente do Console também requer um disco do sistema. ["Exibir detalhes sobre a configuração padrão do agente do Console"](#) .

### Coletar informações de rede

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

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

### Escolha uma velocidade de gravação

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

["Saiba mais sobre velocidade de gravação"](#) .

## **Escolha um perfil de uso de volume**

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

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

### **Provisionamento fino**

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

### **Desduplicação**

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

### **Compressão**

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

## **Configurar a rede do Azure para o Cloud Volumes ONTAP**

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

### **Requisitos para o Cloud Volumes ONTAP**

Os seguintes requisitos de rede devem ser atendidos no Azure.

#### **Acesso de saída à Internet**

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

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

### **Pontos de extremidade Cloud Volumes ONTAP**

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



Pontos finais	Aplicável para	Propósito	Modos de implantação	Impacto se indisponível
\ <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	Autenticação	Usado para autenticação no Console.	Modos padrão e restrito.	A autenticação do usuário falha e os seguintes serviços permanecem indisponíveis: <ul style="list-style-type: none"> <li>• Serviços Cloud Volumes ONTAP</li> <li>• Serviços ONTAP</li> <li>• Protocolos e serviços de proxy</li> </ul>
<a href="https://vault.azure.net">https://vault.azure.net</a>	Cofre de Chaves	Usado para recuperar chaves secretas do cliente do Azure Key Vault ao usar chaves gerenciadas pelo cliente (CMK).	Modos padrão, restrito e privado.	Os serviços do Cloud Volumes ONTAP não estão disponíveis.
\ <a href="https://api.blueexp.net/app.com/tenancy">https://api.blueexp.net/app.com/tenancy</a>	Arrendamento	Usado para recuperar os recursos Cloud Volumes ONTAP do Console para autorizar recursos e usuários.	Modos padrão e restrito.	Os recursos do Cloud Volumes ONTAP e os usuários não estão autorizados.
\ <a href="https://mysupport.netapp.com/aods/asupmessage">https://mysupport.netapp.com/aods/asupmessage</a> \ <a href="https://mysupport.netapp.com/asupprod/post/1.0/postAsup">https://mysupport.netapp.com/asupprod/post/1.0/postAsup</a>	AutoSupport	Usado para enviar dados de telemetria do AutoSupport para o suporte da NetApp.	Modos padrão e restrito.	As informações do AutoSupport continuam não entregues.
\ <a href="https://management.azure.com">https://management.azure.com</a> \ <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a> \ <a href="https://blueexpinfraproduct.eastus2.data.azurecr.io">https://blueexpinfraproduct.eastus2.data.azurecr.io</a> \ <a href="https://core.windows.net">https://core.windows.net</a>	Regiões públicas	Comunicação com serviços do Azure.	Modos padrão, restrito e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço do Azure para executar operações específicas para o Console no Azure.

Pontos finais	Aplicável para	Propósito	Modos de implantação	Impacto se indisponível
<a href="https://management.chinacloudapi.cn">https://management.chinacloudapi.cn</a> \ <a href="https://login.chinacloudapi.cn">https://login.chinacloudapi.cn</a> \ <a href="https://blob.core.chinacloudapi.cn">https://blob.core.chinacloudapi.cn</a> \ <a href="https://core.chinacloudapi.cn">https://core.chinacloudapi.cn</a>	Região da China	Comunicação com serviços do Azure.	Modos padrão, restrito e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço do Azure para executar operações específicas para o Console no Azure.
<a href="https://management.microsoftazure.de">https://management.microsoftazure.de</a> \ <a href="https://login.microsoftonline.de">https://login.microsoftonline.de</a> \ <a href="https://blob.core.cloudapi.de">https://blob.core.cloudapi.de</a> \ <a href="https://core.cloudapi.de">https://core.cloudapi.de</a>	Região da Alemanha	Comunicação com serviços do Azure.	Modos padrão, restrito e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço do Azure para executar operações específicas para o Console no Azure.
<a href="https://management.usgovcloudapi.net">https://management.usgovcloudapi.net</a> \ <a href="https://login.microsoftonline.us">https://login.microsoftonline.us</a> \ <a href="https://blob.core.usgovcloudapi.net">https://blob.core.usgovcloudapi.net</a> \ <a href="https://core.usgovcloudapi.net">https://core.usgovcloudapi.net</a>	Regiões governamentais	Comunicação com serviços do Azure.	Modos padrão, restrito e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço do Azure para executar operações específicas para o Console no Azure.
<a href="https://management.azure.microsoft.scloud">https://management.azure.microsoft.scloud</a> \ <a href="https://login.microsoftonline.microsoft.scloud">https://login.microsoftonline.microsoft.scloud</a> \ <a href="https://blob.core.microsoft.scloud">https://blob.core.microsoft.scloud</a> \ <a href="https://core.microsoft.scloud">https://core.microsoft.scloud</a>	Regiões do DoD do governo	Comunicação com serviços do Azure.	Modos padrão, restrito e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço do Azure para executar operações específicas para o Console no Azure.

### Configuração de proxy de rede do agente do NetApp Console

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

- **Proxy explícito:** O tráfego de saída do Cloud Volumes ONTAP usa o endereço HTTP do servidor proxy especificado durante a configuração de proxy do agente do Console. O administrador também pode ter configurado credenciais de usuário e certificados de CA raiz para autenticação adicional. Se um certificado de CA raiz estiver disponível para o proxy explícito, certifique-se de obter e carregar o mesmo certificado para o seu sistema Cloud Volumes ONTAP usando o ["ONTAP CLI: instalação do certificado de segurança"](#) comando.

- **Proxy transparente:** A rede está configurada para rotear automaticamente o tráfego de saída do Cloud Volumes ONTAP por meio do proxy para o agente do Console. Ao configurar um proxy transparente, o administrador precisa fornecer apenas um certificado de CA raiz para conectividade do Cloud Volumes ONTAP, não o endereço HTTP do servidor proxy. Certifique-se de obter e carregar o mesmo certificado de CA raiz para o seu sistema Cloud Volumes ONTAP usando o ["ONTAP CLI: instalação do certificado de segurança"](#) comando.

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

## Endereços IP

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

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



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

## Endereços IP para um sistema de nó único

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

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



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

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

## Endereços IP para pares HA

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

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

## NIC0

- IP de gerenciamento de nó
- IP intercluster

- IP iSCSI



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

### NIC1

- IP de rede de cluster

### NIC2

- IP de interconexão de cluster (HA IC)

### NIC3

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



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

Os endereços IP acima não migram em eventos de failover.

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

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

### Conexões seguras com serviços do Azure

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

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

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

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

### Rede para criptografia do Azure VNet

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

Você só precisa garantir que a Rede Acelerada esteja habilitada nas NICs da VM e revisar os requisitos e

limitações de criptografia da VNet do Azure antes de habilitar o recurso. Você não deve modificar os objetos do balanceador de carga gerenciado pela NetApp.

["Documentação do Azure: criptografia VNet e Accelerated Networking"](#).

### Conexões com outros sistemas ONTAP

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

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

### Porta para a interconexão HA

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

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

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

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

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

### Regras do grupo de segurança

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

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

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

### Regras de entrada para sistemas de nó único

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

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

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

Prioridade e nome	Porta e protocolo	Origem e destino	Descrição
1000 entrada_ssh	22 TCP	Qualquer para Qualquer	Acesso SSH ao endereço IP do LIF de gerenciamento de cluster ou de um LIF de gerenciamento de nó
1001 entrada_http	80 TCP	Qualquer para Qualquer	Acesso HTTP ao console da web do ONTAP System Manager usando o endereço IP do LIF de gerenciamento do cluster
1002 entrada_111_tcp	111 TCP	Qualquer para Qualquer	Chamada de procedimento remoto para NFS
1003 entrada_111_udp	111 UDP	Qualquer para Qualquer	Chamada de procedimento remoto para NFS
1004 entrada_139	139 TCP	Qualquer para Qualquer	Sessão de serviço NetBIOS para CIFS
1005 entrada_161-162_tcp	161-162 TCP	Qualquer para Qualquer	Protocolo simples de gerenciamento de rede
1006 entrada_161-162_udp	161-162 UDP	Qualquer para Qualquer	Protocolo simples de gerenciamento de rede
1007 entrada_443	443 TCP	Qualquer para Qualquer	Conectividade com o agente do Console e acesso HTTPS ao console da Web do ONTAP System Manager usando o endereço IP do LIF de gerenciamento do cluster
1008 entrada_445	445 TCP	Qualquer para Qualquer	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
1009 entrada_635_tcp	635 TCP	Qualquer para Qualquer	Montagem NFS
1010 entrada_635_udp	635 UDP	Qualquer para Qualquer	Montagem NFS
1011 entrada_749	749 TCP	Qualquer para Qualquer	Kerberos
1012 entrada_2049_tcp	2049 TCP	Qualquer para Qualquer	Daemon do servidor NFS
1013 entrada_2049_udp	2049 UDP	Qualquer para Qualquer	Daemon do servidor NFS

Prioridade e nome	Porta e protocolo	Origem e destino	Descrição
1014 entrada_3260	3260 TCP	Qualquer para Qualquer	Acesso iSCSI através do LIF de dados iSCSI
1015 entrada_4045-4046_tcp	4045-4046 TCP	Qualquer para Qualquer	Daemon de bloqueio NFS e monitor de status de rede
1016 entrada_4045-4046_udp	4045-4046 UDP	Qualquer para Qualquer	Daemon de bloqueio NFS e monitor de status de rede
1017 entrada_10000	10000 TCP	Qualquer para Qualquer	Backup usando NDMP
1018 entrada_11104-11105	11104-11105 TCP	Qualquer para Qualquer	Transferência de dados do SnapMirror
3000 negação de entrada_todos_tcp	Qualquer porta TCP	Qualquer para Qualquer	Bloquear todo o outro tráfego de entrada TCP
3001 negação de entrada_todos_udp	Qualquer porta UDP	Qualquer para Qualquer	Bloquear todo o outro tráfego de entrada UDP
65000 Permitir entrada de Vnet	Qualquer porta Qualquer protocolo	Rede Virtual para Rede Virtual	Tráfego de entrada de dentro da VNet
65001 Permitir entrada do balanceador de carga do Azure	Qualquer porta Qualquer protocolo	AzureLoadBalancer para qualquer	Tráfego de dados do Azure Standard Load Balancer
65500 NegarAllInBound	Qualquer porta Qualquer protocolo	Qualquer para Qualquer	Bloqueie todo o outro tráfego de entrada

## Regras de entrada para sistemas HA

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

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



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

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

Prioridade e nome	Porta e protocolo	Origem e destino	Descrição
100 entrada_443	443 Qualquer protocolo	Qualquer para Qualquer	Conectividade com o agente do Console e acesso HTTPS ao console da Web do ONTAP System Manager usando o endereço IP do LIF de gerenciamento do cluster
101 entrada_111_tcp	111 Qualquer protocolo	Qualquer para Qualquer	Chamada de procedimento remoto para NFS
102 entrada_2049_tcp	2049 Qualquer protocolo	Qualquer para Qualquer	Daemon do servidor NFS
111 entrada_ssh	22 Qualquer protocolo	Qualquer para Qualquer	Acesso SSH ao endereço IP do LIF de gerenciamento de cluster ou de um LIF de gerenciamento de nó
121 entrada_53	53 Qualquer protocolo	Qualquer para Qualquer	DNS e CIFS
65000 Permitir entrada de Vnet	Qualquer porta Qualquer protocolo	Rede Virtual para Rede Virtual	Tráfego de entrada de dentro da VNet
65001 Permitir entrada do balanceador de carga do Azure	Qualquer porta Qualquer protocolo	AzureLoadBalancer para qualquer	Tráfego de dados do Azure Standard Load Balancer
65500 NegarAllInBound	Qualquer porta Qualquer protocolo	Qualquer para Qualquer	Bloqueie todo o outro tráfego de entrada

## Regras de saída

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

### Regras básicas de saída

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

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

### Regras avançadas de saída

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



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



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

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

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

### Requisitos para o agente do console

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

- ["Exibir requisitos de rede para o agente do Console"](#)
- ["Regras de grupo de segurança no Azure"](#)

### Tópicos relacionados

- ["Verifique a configuração do AutoSupport para o Cloud Volumes ONTAP"](#)
- ["Saiba mais sobre as portas internas do ONTAP"](#) .

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

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

### Visão geral da criptografia de dados

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

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

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

### Como os dados são criptografados

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

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

Configuração do Cloud Volumes ONTAP	Discos do sistema usados para criptografia de chaves	Discos de dados usados para criptografia de chaves
Nó único	<ul style="list-style-type: none"> <li>• Bota</li> <li>• Essencial</li> <li>• NVRAM</li> </ul>	<ul style="list-style-type: none"> <li>• Raiz</li> <li>• Dados</li> </ul>
Zona de disponibilidade única do Azure HA com blobs de página	<ul style="list-style-type: none"> <li>• Bota</li> <li>• Essencial</li> <li>• NVRAM</li> </ul>	Nenhum
Zona de disponibilidade única do Azure HA com discos gerenciados compartilhados	<ul style="list-style-type: none"> <li>• Bota</li> <li>• Essencial</li> <li>• NVRAM</li> </ul>	<ul style="list-style-type: none"> <li>• Raiz</li> <li>• Dados</li> </ul>
Várias zonas de disponibilidade do Azure HA com discos gerenciados compartilhados	<ul style="list-style-type: none"> <li>• Bota</li> <li>• Essencial</li> <li>• NVRAM</li> </ul>	<ul style="list-style-type: none"> <li>• Raiz</li> <li>• Dados</li> </ul>

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

## Rotação de chaves no Cloud Volumes ONTAP

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

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

- ["Configurar a rotação automática da chave criptográfica no Azure Key Vault"](#)
- ["Azure PowerShell - Habilitar chaves gerenciadas pelo cliente"](#)



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

## Crie uma identidade gerenciada atribuída pelo usuário

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

O recurso tem o seguinte ID: `userassignedidentity` .

### Passos

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

## Crie um cofre de chaves e gere uma chave

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

Se você [criou uma identidade gerenciada atribuída pelo usuário](#) , ao criar o cofre de chaves, você também deve criar uma política de acesso para o cofre de chaves.

### Passos

1. "[Crie um cofre de chaves na sua assinatura do Azure](#)" .

Observe os seguintes requisitos para o cofre de chaves:

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



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

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

a. Selecione as seguintes permissões:

- pegar
- lista
- decifrar
- criptografar
- desembrulhar chave
- chave de envoltório
- verificar
- sinal

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

c. Revise e crie a política de acesso.

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

Observe os seguintes requisitos para a chave:

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

## Crie um sistema que use a chave de criptografia

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

### Permissões necessárias

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

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

["Veja a lista mais recente de permissões"](#)

### Passos

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

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

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

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

["Saiba mais sobre esta chamada de API"](#) .

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

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

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

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

["Saiba mais sobre esta chamada de API"](#) .

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

- a. Para um par HA:

POST /azure/ha/working-environments

O corpo da solicitação deve incluir os seguintes campos:

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



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

["Saiba mais sobre esta chamada de API"](#) .

- b. Para um sistema de nó único:

POST /azure/vsa/working-environments

O corpo da solicitação deve incluir os seguintes campos:

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



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

["Saiba mais sobre esta chamada de API"](#) .

## Resultado

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

para criptografia de dados.

## Configurar o licenciamento do Cloud Volumes ONTAP no Azure

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

### Freemium

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

### Passos

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

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

**Edit Credentials & Add Subscription**

**Associate Subscription to Credentials** ⓘ

Credentials

Managed Service Identity ▼

Azure Subscription

OCCM Dev (Default) ▼

Marketplace Subscription

ⓘ A marketplace subscription isn't associated with the selected Azure subscription.

+ Add Subscription

Apply Cancel

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



Select Charging Method

<input type="radio"/> Professional	By capacity	▼
<input type="radio"/> Essential	By capacity	▼
<input checked="" type="radio"/> Freemium (Up to 500 GiB)	By capacity	▼
<input type="radio"/> Per Node	By node	▼

["Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP no Azure"](#) .

### Licença baseada em capacidade

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

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

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

["Saiba mais sobre licenciamento baseado em capacidade"](#) .

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

#### Traga sua própria bebida

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



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

### Passos

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

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

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

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

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

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

The screenshot shows a dialog box titled "Edit Credentials & Add Subscription". It has a section "Associate Subscription to Credentials" with a help icon. Below this are two dropdown menus: "Credentials" with "Managed Service Identity" selected, and "Azure Subscription" with "OCCM Dev (Default)" selected. A message box states: "Marketplace Subscription" followed by an orange icon and the text "A marketplace subscription isn't associated with the selected Azure subscription." Below the message is a blue link "+ Add Subscription". At the bottom are two buttons: "Apply" (blue) and "Cancel" (gray).

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

Select Charging Method

☒ Professional

By capacity

▼

☐ Essential

By capacity

▼

☐ Freemium (Up to 500 GiB)

By capacity

▼

☐ Per Node

By node

▼

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

### Assinatura PAYGO

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

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

### Passos

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

### Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev (Default)

Marketplace Subscription

ⓘ A marketplace subscription isn't associated with the selected Azure subscription.

+ Add Subscription

Apply Cancel

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

### Select Charging Method

<input checked="" type="radio"/> Professional	By capacity	▼
<input type="radio"/> Essential	By capacity	▼
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity	▼
<input type="radio"/> Per Node	By node	▼

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



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

## Contrato anual

Pague pelo Cloud Volumes ONTAP anualmente comprando um contrato anual.

### Passos

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

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

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

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

Select Charging Method	
<input checked="" type="radio"/> Professional	By capacity
<input type="radio"/> Essential	By capacity
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity
<input type="radio"/> Per Node	By node

["Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP no Azure"](#) .

## Assinatura Keystone

Uma assinatura Keystone é um serviço baseado em assinatura com pagamento conforme o crescimento.

["Saiba mais sobre as assinaturas do NetApp Keystone"](#) .

### Passos

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

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

Select Charging Method

☒ Keystone By capacity ^

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1 v

☐ Professional By capacity v

☐ Essential By capacity v

☐ Freemium (Up to 500 GiB) By capacity v

☐ Per Node By node v

["Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP no Azure"](#) .

### Licença baseada em nó

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

- ["Fim da disponibilidade de licenças baseadas em nós"](#)
- ["Fim da disponibilidade de licenças baseadas em nós"](#)
- ["Converter uma licença baseada em nós para uma licença baseada em capacidade."](#)

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

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

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

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

### Sobre esta tarefa

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

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

### Passos

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

1. ["Acesse o Azure Cloud Shell pelo Portal do Azure"](#)
2. Registre o recurso de modo de alta disponibilidade:

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

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

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

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

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

### Links relacionados

1. ["Microsoft Azure documentação: Visão geral das portas de alta disponibilidade"](#)
2. ["Microsoft Azure documentação: introdução à CLI do Azure"](#)

## Habilitar VMOrchestratorZonalMultiFD para Cloud Volumes ONTAP no Azure

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

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

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

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

### Passos

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

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

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



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

## Inicie o Cloud Volumes ONTAP no Azure

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

### Antes de começar

Você precisa do seguinte antes de começar.

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

Você deve ter uma configuração planejada e os detalhes necessários da rede do Azure fornecidos pelo seu administrador. Para mais informações, consulte ["Planejando sua configuração do Cloud Volumes ONTAP"](#) .

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

["Aprenda como configurar o licenciamento"](#) .

### Sobre esta tarefa

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

#### Potencial de perda de dados

A prática recomendada é usar um novo grupo de recursos dedicado para cada sistema Cloud Volumes ONTAP .



Não é recomendado implantar o Cloud Volumes ONTAP em um grupo de recursos compartilhados existente devido ao risco de perda de dados. Embora o Console possa remover recursos do Cloud Volumes ONTAP de um grupo de recursos compartilhados em caso de falha de implantação ou exclusão, um usuário do Azure pode excluir acidentalmente recursos do Cloud Volumes ONTAP de um grupo de recursos compartilhados.

## Inicie um sistema Cloud Volumes ONTAP de nó único no Azure

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

### Passos

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

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

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

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

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



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


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



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

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

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

Campo	Descrição
Grupo de Recursos	<p>Crie um novo grupo de recursos para o Cloud Volumes ONTAP ou use um grupo de recursos existente. A prática recomendada é usar um novo grupo de recursos dedicado para o Cloud Volumes ONTAP. Embora seja possível implantar o Cloud Volumes ONTAP em um grupo de recursos compartilhados existente, isso não é recomendado devido ao risco de perda de dados. Veja o aviso acima para mais detalhes.</p> <div><p>Se a conta do Azure que você está usando tiver o "<a href="#">permissões necessárias</a>", o Console remove os recursos do Cloud Volumes ONTAP de um grupo de recursos, em caso de falha de implantação ou exclusão.</p></div>
Grupo de segurança gerado	<p>Se você deixar o Console gerar o grupo de segurança para você, precisará escolher como permitirá o tráfego:</p> <ul style="list-style-type: none"><li>• Se você escolher <b>Somente VNet selecionada</b>, a origem do tráfego de entrada será o intervalo de sub-redes da VNet selecionada e o intervalo de sub-redes da VNet onde o agente do Console reside. Esta é a opção recomendada.</li><li>• Se você escolher <b>Todas as VNets</b>, a origem do tráfego de entrada será o intervalo de IP 0.0.0.0/0.</li></ul>
Use existente	<p>Se você escolher um grupo de segurança existente, ele deverá atender aos requisitos do Cloud Volumes ONTAP . "<a href="#">Exibir o grupo de segurança padrão</a>" .</p>

9. **Métodos de cobrança e conta NSS:** especifique qual opção de cobrança você gostaria de usar com este sistema e, em seguida, especifique uma conta do site de suporte da NetApp .

- "[Saiba mais sobre as opções de licenciamento do Cloud Volumes ONTAP](#)" .
- "[Aprenda como configurar o licenciamento](#)" .

10. **Pacotes pré-configurados:** selecione um dos pacotes para implantar rapidamente um sistema Cloud Volumes ONTAP ou clique em **Criar minha própria configuração**.

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

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



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

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

Observe o seguinte:

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

Para obter ajuda na escolha do tipo e tamanho do disco, consulte ["Dimensionando seu sistema no Azure"](#) .

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

["Saiba mais sobre camadas de dados"](#) .

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

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

["Saiba mais sobre velocidade de gravação"](#) .

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

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

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

["Saiba mais sobre o armazenamento WORM"](#) .

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

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

["Saiba mais sobre os protocolos e versões de clientes suportados"](#) .

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

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

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



**Volume Details & Protection**

Volume Name i

ABDcv5689

Volume Size i

100

Storage VM (SVM)

svm\_...CVO1 ▼

Unit

GiB ▼

Snapshot Policy

default ▼

default policy i

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

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

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

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

Para mais informações, consulte ["Compreendendo os perfis de uso de volume"](#) e ["Visão geral da hierarquização de dados"](#).

18. **Revisar e aprovar:** revise e confirme suas seleções.

- a. Revise os detalhes sobre a configuração.
- b. Clique em **Mais informações** para revisar detalhes sobre o suporte e os recursos do Azure que o Console comprará.
- c. Selecione as caixas de seleção **Eu entendo....**
- d. Clique em **Ir**.

## Resultado

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

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

Para obter ajuda adicional, acesse ["Suporte NetApp Cloud Volumes ONTAP"](#) .



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

## Depois que você terminar

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

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

## Inicie um par de Cloud Volumes ONTAP HA no Azure

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

## Passos

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

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

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

5. **Serviços:** habilite ou desabilite os serviços individuais com base na sua vontade de usá-los com o Cloud Volumes ONTAP.

- ["Saiba mais sobre a NetApp Data Classification"](#)
- ["Saiba mais sobre o NetApp Backup and Recovery"](#)



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

## 6. Modelos de implantação de HA:

a. Selecione **Zona de disponibilidade única** ou **Zona de disponibilidade múltipla**.

- Para zonas de disponibilidade únicas, selecione uma região do Azure, uma zona de disponibilidade, uma VNet e uma sub-rede.

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


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

b. Marque a caixa de seleção **Verifiquei a conectividade de rede...**

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



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

Campo	Descrição
Grupo de Recursos	<p>Crie um novo grupo de recursos para o Cloud Volumes ONTAP ou use um grupo de recursos existente. A prática recomendada é usar um novo grupo de recursos dedicado para o Cloud Volumes ONTAP. Embora seja possível implantar o Cloud Volumes ONTAP em um grupo de recursos compartilhados existente, isso não é recomendado devido ao risco de perda de dados. Veja o aviso acima para mais detalhes.</p> <p>Você deve usar um grupo de recursos dedicado para cada par de Cloud Volumes ONTAP HA implantado no Azure. Somente um par de HA é suportado em um grupo de recursos. O Console terá problemas de conexão se você tentar implantar um segundo par de Cloud Volumes ONTAP HA em um grupo de recursos do Azure.</p> <div>  <p>Se a conta do Azure que você está usando tiver o "<a href="#">permissões necessárias</a>", o Console remove os recursos do Cloud Volumes ONTAP de um grupo de recursos, em caso de falha de implantação ou exclusão.</p> </div>
Grupo de segurança gerado	<p>Se você deixar o Console gerar o grupo de segurança para você, precisará escolher como permitirá o tráfego:</p> <ul style="list-style-type: none"> <li>• Se você escolher <b>Somente VNet selecionada</b>, a origem do tráfego de entrada será o intervalo de sub-redes da VNet selecionada e o intervalo de sub-redes da VNet onde o agente do Console reside. Esta é a opção recomendada.</li> <li>• Se você escolher <b>Todas as VNets</b>, a origem do tráfego de entrada será o intervalo de IP 0.0.0.0/0.</li> </ul>
Use existente	<p>Se você escolher um grupo de segurança existente, ele deverá atender aos requisitos do Cloud Volumes ONTAP. "<a href="#">Exibir o grupo de segurança padrão</a>".</p>

8. **Métodos de cobrança e conta NSS:** especifique qual opção de cobrança você gostaria de usar com este sistema e, em seguida, especifique uma conta do site de suporte da NetApp.

- "[Saiba mais sobre as opções de licenciamento do Cloud Volumes ONTAP](#)".
- "[Aprenda como configurar o licenciamento](#)".

9. **Pacotes pré-configurados:** selecione um dos pacotes para implantar rapidamente um sistema Cloud Volumes ONTAP ou clique em **Alterar configuração**.

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

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



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

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

Observe o seguinte:

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

Para obter ajuda na escolha do tamanho do disco, consulte ["Dimensione seu sistema no Azure"](#) .

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

["Saiba mais sobre camadas de dados"](#) .

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

["Saiba mais sobre as configurações com suporte no Azure"](#) .

### 13. Velocidade de gravação e WORM:

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

["Saiba mais sobre velocidade de gravação"](#) .

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

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

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

["Saiba mais sobre o armazenamento WORM"](#) .

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

14. **Comunicação segura com armazenamento e WORM:** escolha se deseja habilitar uma conexão HTTPS com contas de armazenamento do Azure e ative o armazenamento WORM (gravação única e leitura múltipla), se desejar.

A conexão HTTPS é de um par de HA do Cloud Volumes ONTAP 9.7 para contas de armazenamento de blobs de páginas do Azure. Observe que habilitar esta opção pode afetar o desempenho da gravação. Você não pode alterar a configuração depois de criar o sistema.

["Saiba mais sobre o armazenamento WORM"](#) .

O WORM não pode ser habilitado se a hierarquização de dados estiver habilitada.

["Saiba mais sobre o armazenamento WORM"](#) .

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

["Saiba mais sobre os protocolos e versões de clientes suportados"](#) .

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

Campo	Descrição
Tamanho	O tamanho máximo que você pode inserir depende muito se você habilita o provisionamento fino, que permite criar um volume maior que o armazenamento físico disponível atualmente.
Controle de acesso (somente para NFS)	Uma política de exportação define os clientes na sub-rede que podem acessar o volume. Por padrão, o Console insere um valor que fornece acesso a todas as instâncias na sub-rede.
Permissões e usuários/grupos (somente para CIFS)	Esses campos permitem que você controle o nível de acesso a um compartilhamento para usuários e grupos (também chamados de listas de controle de acesso ou ACLs). Você pode especificar usuários ou grupos locais ou de domínio do Windows, ou usuários ou grupos do UNIX. Se você especificar um nome de usuário de domínio do Windows, deverá incluir o domínio do usuário usando o formato domínio\nome de usuário.
Política de Snapshot	Uma política de cópia de instantâneo especifica a frequência e o número de cópias de instantâneo do NetApp criadas automaticamente. Uma cópia do NetApp Snapshot é uma imagem do sistema de arquivos de um momento específico que não tem impacto no desempenho e requer armazenamento mínimo. Você pode escolher a política padrão ou nenhuma. Você pode escolher nenhum para dados transitórios: por exemplo, tempdb para Microsoft SQL Server.
Opções avançadas (somente para NFS)	Selecione uma versão do NFS para o volume: NFSv3 ou NFSv4.

Campo	Descrição
Grupo iniciador e IQN (somente para iSCSI)	Os destinos de armazenamento iSCSI são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Os grupos de iniciadores são tabelas de nomes de nós de host iSCSI e controlam quais iniciadores têm acesso a quais LUNs. Os destinos iSCSI se conectam à rede por meio de adaptadores de rede Ethernet padrão (NICs), placas de mecanismo de descarregamento TCP (TOE) com iniciadores de software, adaptadores de rede convergentes (CNAs) ou adaptadores de bust de host dedicados (HBAs) e são identificados por nomes qualificados iSCSI (IQNs). Quando você cria um volume iSCSI, o Console cria automaticamente um LUN para você. Simplificamos criando apenas um LUN por volume, portanto não há gerenciamento envolvido. Depois de criar o volume, <a href="#">"use o IQN para conectar-se ao LUN de seus hosts"</a> .

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

The screenshot displays the 'Volume Details & Protection' configuration interface. It includes the following fields and options:

- Volume Name:** A text input field containing 'ABDcv5689'.
- Storage VM (SVM):** A dropdown menu showing 'svm\_c...CVO1'.
- Volume Size:** A text input field containing '100'.
- Unit:** A dropdown menu showing 'GiB'.
- Snapshot Policy:** A dropdown menu showing 'default'.
- default policy:** A label with an information icon (i) located below the Snapshot Policy dropdown.

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

Campo	Descrição
Endereço IP primário e secundário do DNS	Os endereços IP dos servidores DNS que fornecem resolução de nomes para o servidor CIFS. Os servidores DNS listados devem conter os registros de localização de serviço (SRV) necessários para localizar os servidores LDAP do Active Directory e os controladores de domínio para o domínio ao qual o servidor CIFS se juntará.
Domínio do Active Directory para ingressar	O FQDN do domínio do Active Directory (AD) ao qual você deseja que o servidor CIFS ingresse.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com privilégios suficientes para adicionar computadores à Unidade Organizacional (UO) especificada dentro do domínio do AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio do AD.

Campo	Descrição
Unidade Organizacional	A unidade organizacional dentro do domínio do AD a ser associada ao servidor CIFS. O padrão é CN=Computadores. Para configurar o Azure AD Domain Services como o servidor AD para o Cloud Volumes ONTAP, você deve inserir <b>OU=AADDCC Computers</b> ou <b>OU=AADDCC Users</b> neste campo. <a href="https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou">https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou</a> ["Documentação do Azure: Criar uma Unidade Organizacional (UO) em um domínio gerenciado do Azure AD Domain Services"^]
Domínio DNS	O domínio DNS para a máquina virtual de armazenamento (SVM) do Cloud Volumes ONTAP . Na maioria dos casos, o domínio é o mesmo que o domínio do AD.
Servidor NTP	Selecione <b>Usar domínio do Active Directory</b> para configurar um servidor NTP usando o DNS do Active Directory. Se você precisar configurar um servidor NTP usando um endereço diferente, use a API. Consulte o <a href="#">"Documentação de automação do NetApp Console"</a> para mais detalhes. Observe que você só pode configurar um servidor NTP ao criar um servidor CIFS. Não é configurável depois de criar o servidor CIFS.

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

Para mais informações, consulte ["Escolha um perfil de uso de volume"](#) , ["Visão geral da hierarquização de dados"](#) , e ["KB: Quais recursos de eficiência de armazenamento em linha são suportados pelo CVO?"](#)

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

## Resultado

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

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

Para obter ajuda adicional, acesse ["Suporte NetApp Cloud Volumes ONTAP"](#) .

## Depois que você terminar

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

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



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

### Links relacionados

[\\*\\*Planejando sua configuração do Cloud Volumes ONTAP no Azure](#) [\\*\\*Implantar o Cloud Volumes ONTAP no Azure a partir do Azure Marketplace](#)

## Verificar imagem da plataforma Azure

### Verificação de imagem do Azure Marketplace para Cloud Volumes ONTAP

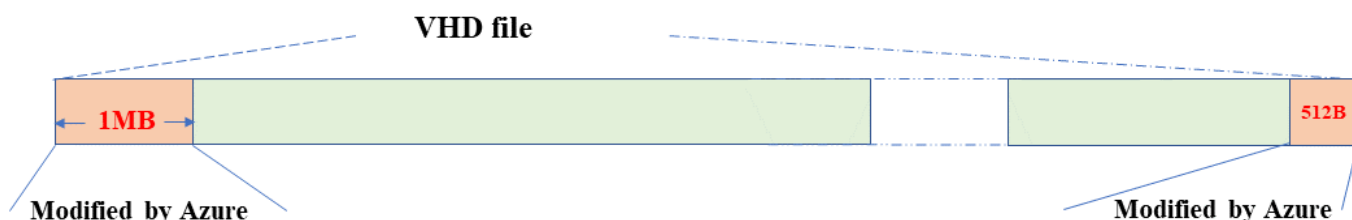
A verificação de imagem do Azure está em conformidade com os requisitos de segurança aprimorados da NetApp. Verificar um arquivo de imagem é um processo simples. No entanto, a verificação da assinatura da imagem do Azure requer considerações específicas para o arquivo de imagem VHD do Azure porque ele é alterado no marketplace do Azure.



A verificação de imagem do Azure é compatível com o Cloud Volumes ONTAP 9.15.0 e posteriores.

### Alteração de arquivos VHD publicados pelo Azure

O 1 MB (1048576 bytes) no início e 512 bytes no final do arquivo VHD são modificados pelo Azure. O NetApp assina o arquivo VHD restante.



No exemplo, o arquivo VHD tem 10 GB. A parte que a NetApp assinou está marcada em verde (10 GB - 1 MB - 512 bytes).

### Links relacionados

- ["Blog de falhas de página: como assinar e verificar usando OpenSSL"](#)
- ["Use a imagem do Azure Marketplace para criar uma imagem de VM para sua GPU Azure Stack Edge Pro | Microsoft Learn"](#)
- ["Exportar/Copiar um disco gerenciado para uma conta de armazenamento usando a CLI do Azure | Microsoft Learn"](#)
- ["Início rápido do Azure Cloud Shell - Bash | Microsoft Learn"](#)
- ["Como instalar o Azure CLI | Microsoft Learn"](#)
- ["cópia do blob de armazenamento az | Microsoft Learn"](#)
- ["Sign in com a CLI do Azure — Login e Autenticação | Microsoft Learn"](#)



## Baixe o arquivo de imagem do Azure para o Cloud Volumes ONTAP

Você pode baixar o arquivo de imagem do Azure em "[Site de suporte da NetApp](#)".

O arquivo *tar.gz* contém os arquivos necessários para verificação da assinatura da imagem. Junto com o arquivo *tar.gz*, você também deve baixar o arquivo *checksum* da imagem. O arquivo de soma de verificação contém o md5 e sha256 somas de verificação do arquivo *tar.gz*.

### Passos

1. Vá para o "[Página do produto Cloud Volumes ONTAP no site de suporte da NetApp](#)" e baixe a versão do software necessária na seção **Downloads**.
2. Na página de download do Cloud Volumes ONTAP, clique no arquivo para download da imagem do Azure e baixe o arquivo *tar.gz*.

## Cloud Volumes ONTAP 9.15.0P1

Date Posted : 17-May-2024

### Cloud Volumes ONTAP

#### Non-Restricted Countries

If you are upgrading to ONTAP 9.15.0P1, and you are in "Non-restricted Countries", please download the image with NetApp Volume Encryption.

**DOWNLOAD 9150P1\_V\_IMAGE.TGZ [2.58 GB]**

[View and download checksums](#)

**DOWNLOAD 9150P1\_V\_IMAGE.TGZ.PEM [451 B]**

[View and download checksums](#)

**DOWNLOAD 9150P1\_V\_IMAGE.TGZ.SIG [256 B]**

[View and download checksums](#)

### Cloud Volumes ONTAP

#### Restricted Countries

If you are unsure whether your company complied with all applicable legal requirements on encryption technology, download the image without NetApp Volume Encryption.

**DOWNLOAD 9150P1\_V\_NODAR\_IMAGE.TGZ [2.58 GB]**

[View and download checksums](#)

**DOWNLOAD 9150P1\_V\_NODAR\_IMAGE.TGZ.PEM [451 B]**

[View and download checksums](#)

**DOWNLOAD 9150P1\_V\_NODAR\_IMAGE.TGZ.SIG [256 B]**

[View and download checksums](#)

### Cloud Volumes ONTAP

**DOWNLOAD GCP-9-15-0P1\_PKG.TAR.GZ [7.49 KB]**

[View and download checksums](#)

**DOWNLOAD AZURE-9-15-0P1\_PKG.TAR.GZ [7.64 KB]**

[View and download checksums](#)

3. No Linux, execute `md5sum AZURE-<version>_PKG.TAR.GZ`.

No macOS, execute `sha256sum AZURE-<version>_PKG.TAR.GZ`.

4. Verifique se o `md5sum` e `sha256sum` os valores correspondem aos da imagem do Azure baixada.
5. No Linux e macOS, extraia o arquivo *tar.gz* usando o `tar -xzf` comando.

O arquivo *tar.gz* extraído contém o arquivo de resumo (*.sig*), o arquivo de certificado de chave pública (*.pem*) e o arquivo de certificado de cadeia (*.pem*).

**Exemplo de saída após extrair o arquivo *tar.gz*:**

```
$ ls cert/ -l
-rw-r----- 1 netapp netapp 384 May 13 13:00 9.15.0P1_azure_digest.sig
-rw-r----- 1 netapp netapp 2365 May 13 13:00 Certificate-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May 13 13:00 Certificate-Chain-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May 13 13:00 version_readme
```

## Exportar imagens VHD para o Cloud Volumes ONTAP do marketplace do Azure

Depois que a imagem VHD é publicada na nuvem do Azure, ela não é mais gerenciada pelo NetApp. Em vez disso, a imagem publicada é colocada no marketplace do Azure. Quando a imagem é preparada e publicada no marketplace do Azure, o Azure modifica 1 MB no início e 512 bytes no final do VHD. Para verificar a assinatura do arquivo VHD, você precisa exportar a imagem VHD modificada pelo Azure do marketplace do Azure.

### Antes de começar

Certifique-se de que a CLI do Azure esteja instalada no seu sistema ou que o Azure Cloud Shell esteja disponível no portal do Azure. Para obter mais informações sobre como instalar o Azure CLI, consulte o ["Documentação da Microsoft: Como instalar o Azure CLI"](#).

### Passos

1. Mapeie a versão do Cloud Volumes ONTAP no seu sistema para a versão da imagem do Azure Marketplace usando o conteúdo do arquivo *version\_readme*. A versão Cloud Volumes ONTAP é representada por *buildname* e a versão da imagem do marketplace do Azure é representada por *version* nos mapeamentos de versão.

No exemplo a seguir, a versão do Cloud Volumes ONTAP 9.15.0P1 é mapeado para a versão da imagem do Azure Marketplace 9150.01000024.05090105. Esta versão da imagem do Azure Marketplace é usada posteriormente para definir o URN da imagem.

```
[
  "buildname": "9.15.0P1",
  "publisher": "netapp",
  "version": "9150.01000024.05090105"
]
```

2. Identifique a região onde você deseja criar as VMs. O nome da região é usado como valor para o *locName* variável ao definir a URN da imagem do marketplace. Para listar as regiões disponíveis, execute este comando:

```
az account list-locations -o table
```

Nesta tabela, o nome da região aparece no *Name* campo.



```
$ az account list-locations -o table
DisplayName          Name          RegionalDisplayName
-----
East US              eastus        (US) East US
East US 2            eastus2       (US) East US 2
South Central US     southcentralus (US) South Central US
...
```

3. Revise os nomes de SKU para as versões correspondentes do Cloud Volumes ONTAP e os tipos de implantação de VM na tabela abaixo. O nome do SKU é usado como valor para o `skuName` variável ao definir o URN da imagem do marketplace.

Por exemplo, todas as implantações de nó único com Cloud Volumes ONTAP 9.15.0 devem usar `ontap_cloud_byol` como o nome do SKU.

* Versão Cloud Volumes ONTAP *	Implantação de VM por meio de	Nome do SKU
9.17.1 e posterior	O mercado do Azure	ontap_cloud_direct_gen2
9.17.1 e posterior	O NetApp Console	ontap_cloud_gen2
9.16.1	O mercado do Azure	ontap_cloud_direct
9.16.1	O Console	ontap_cloud
9.15.1	O Console	ontap_cloud
9.15.0	O Console, implantações de nó único	ontap_cloud_byol
9.15.0	O Console, implantações de alta disponibilidade (HA)	ontap_cloud_byol_ha

4. Após mapear a versão do ONTAP e a imagem do Azure Marketplace, exporte o arquivo VHD do Azure Marketplace usando o Azure Cloud Shell ou o Azure CLI.

#### Exportar arquivo VHD usando o Azure Cloud Shell no Linux

No Azure Cloud Shell, exporte a imagem do marketplace para o arquivo VHD (por exemplo, `9150.01000024.05090105.vhd`) e baixe-a para o seu sistema Linux local. Execute estas etapas para obter a imagem VHD do marketplace do Azure.

#### Passos

1. Defina o URN e outros parâmetros da imagem do marketplace. O formato URN é `<publisher>:<offer>:<sku>:<version>`. Opcionalmente, você pode listar imagens do NetApp Marketplace para confirmar a versão correta da imagem.

```

PS /home/user1> $urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
PS /home/user1> $locName="eastus2"
PS /home/user1> $pubName="netapp"
PS /home/user1> $offerName="netapp-ontap-cloud"
PS /home/user1> $skuName="ontap_cloud_byol"
PS /home/user1> Get-AzVMImage -Location $locName -PublisherName $pubName
-Offer $offerName -Sku $skuName |select version
...
141.20231128
9.141.20240131
9.150.20240213
9150.01000024.05090105
...

```

2. Crie um novo disco gerenciado a partir da imagem do marketplace com a versão da imagem correspondente:

```

PS /home/user1> $diskName = "9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = "fnf1"
PS /home/user1> az disk create -g $diskRG -n $diskName --image-reference
$urn
PS /home/user1> $sas = az disk grant-access --duration-in-seconds 3600
--access-level Read --name $diskName --resource-group $diskRG
PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-Json)[0].accessSas

```

3. Exporte o arquivo VHD do disco gerenciado para o Armazenamento do Azure. Crie um contêiner com o nível de acesso apropriado. Neste exemplo, usamos um contêiner chamado `vm-images` com `Container` nível de acesso. Obtenha a chave de acesso da conta de armazenamento no portal do Azure: **Contas de armazenamento > *examplesaname* > Chave de acesso > *key1* > key > Mostrar > <cópia>**

```

PS /home/user1> $storageAccountName = "examplesaname"
PS /home/user1> $containerName = "vm-images"
PS /home/user1> $storageAccountKey = "<replace with the above access
key>"
PS /home/user1> $destBlobName = "9150.01000024.05090105.vhd"
PS /home/user1> $destContext = New-AzureStorageContext
-StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri $diskAccessSAS
-DestContainer $containerName -DestContext $destContext -DestBlob
$destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState -Container $containerName
-Context $destContext -Blob $destBlobName

```

4. Baixe a imagem gerada para o seu sistema Linux. Use o `wget` comando para baixar o arquivo VHD:

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

O URL segue um formato padrão. Para automação, você pode derivar a sequência de URL conforme mostrado abaixo. Como alternativa, você pode usar o Azure CLI `az` comando para obter a URL. URL de exemplo: `https://examplesaname.bluelxpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]`

5. Limpe o disco gerenciado

```

PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName
$diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName

```

### Exportar arquivo VHD usando a CLI do Azure no Linux

Exporte a imagem do marketplace para um arquivo VHD usando a CLI do Azure de um sistema Linux local.

#### Passos

1. Efetue login na CLI do Azure e liste as imagens do marketplace:

```
% az login --use-device-code
```

2. Para fazer login, use um navegador da web para abrir a página <https://microsoft.com/devicelogin> e digite o código de autenticação.

```
% az vm image list --all --publisher netapp --offer netapp-ontap-cloud
--sku ontap_cloud_byol
...
{
  "architecture": "x64",
  "offer": "netapp-ontap-cloud",
  "publisher": "netapp",
  "sku": "ontap_cloud_byol",
  "urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
  "version": "9150.01000024.05090105"
},
...
```

3. Crie um novo disco gerenciado a partir da imagem do marketplace com a versão da imagem correspondente.

```
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level Read
--name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.bluepinfraprod.eastus2.data.azurecr.io/xxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluepinfraprod.eastus2.data.azurecr.io/xxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
```

Para automatizar o processo, o SAS precisa ser extraído da saída padrão. Consulte os documentos apropriados para obter orientação.

4. Exporte o arquivo VHD do disco gerenciado.
  - a. Crie um contêiner com o nível de acesso apropriado. Neste exemplo, um contêiner chamado `vm-images` com Container nível de acesso é usado.
  - b. Obtenha a chave de acesso da conta de armazenamento no portal do Azure: **Contas de armazenamento > *examplesaname* > Chave de acesso > *key1* > *key* > Mostrar > <cópia>**

Você também pode usar o `az` comando para esta etapa.

```
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS --destination
--container $containerName --account-name $storageAccountName --account
--key $storageAccountKey --destination-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xxxxxxxxxxxxxxxxxxxx\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

##### 5. Verifique o status da cópia do blob.

```
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
  "copy": {
    "completionTime": null,
    "destinationSnapshot": null,
    "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx",
    "incrementalCopy": null,
    "progress": "10737418752/10737418752",
    "source": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "status": "success",
    "statusDescription": null
  },
....
```

##### 6. Baixe a imagem gerada para o seu servidor Linux.

```
wget <URL of file examplesaname/Containers/vm-  
images/9150.01000024.05090105.vhd>
```

O URL segue um formato padrão. Para automação, você pode derivar a sequência de URL conforme mostrado abaixo. Como alternativa, você pode usar o Azure CLI `az` comando para obter a URL. URL de exemplo: `https://examplesaname.bluelxpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]`

## 7. Limpe o disco gerenciado

```
az disk revoke-access --name $diskName --resource-group $diskRG  
az disk delete --name $diskName --resource-group $diskRG --yes
```

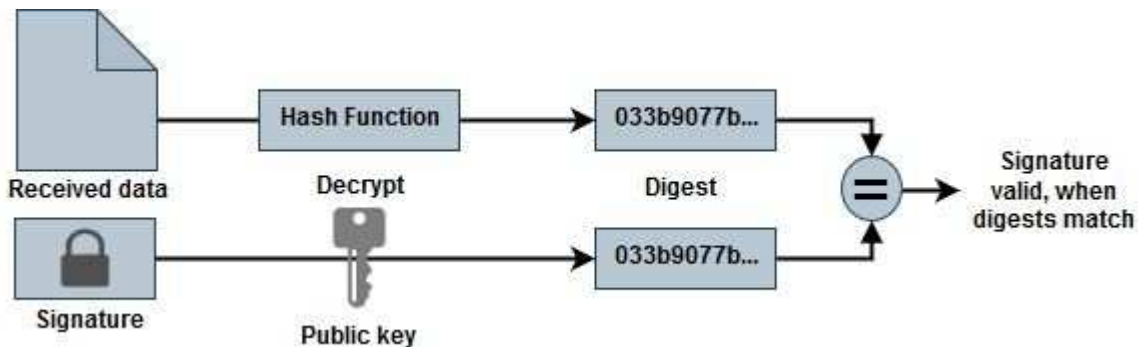
## Verificar assinatura do arquivo

### Verificação de assinatura de imagem do Azure Marketplace para Cloud Volumes ONTAP

O processo de verificação de imagem do Azure gera um arquivo de resumo a partir do arquivo VHD, retirando 1 MB no início e 512 bytes no final e, em seguida, aplicando uma função de hash. Para corresponder ao procedimento de assinatura, *sha256* é usado para hash.

### Resumo do fluxo de trabalho de verificação de assinatura de arquivo

A seguir, uma visão geral do processo de fluxo de trabalho de verificação de assinatura de arquivo.



- Baixando a imagem do Azure do ["Site de suporte da NetApp"](#) e extrair o arquivo digest (.sig), o arquivo de certificado de chave pública (.pem) e o arquivo de certificado de cadeia (.pem). Consulte ["Baixe o arquivo de resumo da imagem do Azure"](#) para maiores informações.
- Verificação da cadeia de confiança.
- Extraíndo a chave pública (.pub) do certificado de chave pública (.pem).
- Descriptografando o arquivo de resumo usando a chave pública extraída.
- Comparando o resultado com um resumo recém-gerado de um arquivo temporário criado a partir do arquivo de imagem após remover 1 MB no início e 512 bytes no final. Esta etapa é realizada usando a ferramenta de linha de comando OpenSSL. A ferramenta OpenSSL CLI exibe mensagens apropriadas sobre sucesso ou falha na correspondência dos arquivos.

```
openssl dgst -verify <public_key> -keyform <form> <hash_function>
-signature <digest_file> -binary <temporary_file>
```

### Verificar assinatura de imagem do Azure Marketplace para Cloud Volumes ONTAP no Linux

A verificação da assinatura de um arquivo VHD exportado no Linux inclui a validação da cadeia de confiança, a edição do arquivo e a verificação da assinatura.

#### Passos

1. Baixe o arquivo de imagem do Azure em "[Site de suporte da NetApp](#)" e extraia o arquivo digest (.sig), o arquivo de certificado de chave pública (.pem) e o arquivo de certificado de cadeia (.pem).

Consulte "[Baixe o arquivo de resumo da imagem do Azure](#)" para maiores informações.

2. Verifique a cadeia de confiança.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. Remova 1 MB (1.048.576 bytes) no início e 512 bytes no final do arquivo VHD. Ao usar `tail`, o `-c +K` opção gera bytes a partir do K-ésimo byte do arquivo. Portanto, ele passa 1048577 para `tail -c`.

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. Use o OpenSSL para extrair a chave pública do certificado e verificar o arquivo removido (sign.tmp) com o arquivo de assinatura e a chave pública.

O prompt de comando exibe mensagens indicando sucesso ou falha com base na verificação.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verification OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. Limpe o espaço de trabalho.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

### Verificar assinatura de imagem do Azure Marketplace para Cloud Volumes ONTAP no macOS

A verificação da assinatura de um arquivo VHD exportado no Linux inclui a validação da cadeia de confiança, a edição do arquivo e a verificação da assinatura.

#### Passos

1. Baixe o arquivo de imagem do Azure em "[Site de suporte da NetApp](#)" e extraia o arquivo digest (.sig), o arquivo de certificado de chave pública (.pem) e o arquivo de certificado de cadeia (.pem).

Consulte "[Baixe o arquivo de resumo da imagem do Azure](#)" para maiores informações.

2. Verifique a cadeia de confiança.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. Remova 1 MB (1.048.576 bytes) no início e 512 bytes no final do arquivo VHD. Ao usar `tail`, o `-c +K` opção gera bytes a partir do K-ésimo byte do arquivo. Portanto, ele passa 1048577 para `tail -c`. Observe que no macOS, o comando `tail` pode levar cerca de dez minutos para ser concluído.

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. Use o OpenSSL para extrair a chave pública do certificado e verificar o arquivo removido (sign.tmp) com o arquivo de assinatura e a chave pública. O prompt de comando exibe mensagens indicando sucesso ou falha com base na verificação.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. Limpe o espaço de trabalho.



```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

## Implantar o Cloud Volumes ONTAP no marketplace do Azure

Você pode usar a implantação direta do Azure Marketplace para implantar o Cloud Volumes ONTAP de forma rápida e fácil. No marketplace do Azure, você pode implantar rapidamente o Cloud Volumes ONTAP em apenas alguns cliques e explorar seus principais recursos e funcionalidades em seu ambiente.

Para mais informações sobre esta oferta, consulte ["Saiba mais sobre as ofertas do Cloud Volumes ONTAP no NetApp Console e no marketplace"](#).

### Sobre esta tarefa

O sistema Cloud Volumes ONTAP implantado usando a implantação direta do Azure Marketplace tem essas propriedades. Observe que os recursos de uma instância autônoma implantada por meio do marketplace do Azure mudam quando ela é descoberta no NetApp Console.

- A versão mais recente do Cloud Volumes ONTAP (9.16.1 ou posterior).
- Uma licença gratuita para o Cloud Volumes ONTAP limitada a 500 GiB de capacidade provisionada. Esta licença não inclui suporte NetApp e não tem data de expiração.
- Dois nós configurados em modo de alta disponibilidade (HA) em uma única zona de disponibilidade (AZ), provisionados com números de série padrão. As máquinas virtuais de armazenamento (VMs de armazenamento) são implantadas em um ["modo de orquestração flexível"](#).
- Um agregado para a instância criada por padrão.
- Um disco gerenciado SSD v2 Premium com capacidade provisionada de 500 GiB, além de um disco raiz e um disco de dados.
- Uma VM de armazenamento de dados implantada, com serviços de dados NFS, CIFS, iSCSI e NVMe/TCP. Não é possível adicionar nenhuma VM de armazenamento de dados adicional.
- Licenças instaladas para NFS, CIFS (SMB), iSCSI, Autonomous Ransomware Protection (ARP), SnapLock e SnapMirror.
- ["Eficiência de armazenamento sensível à temperatura \(TSSE\) ONTAP"](#), criptografia de volume e gerenciamento de chaves externas habilitados por padrão.
- Os seguintes recursos não são suportados:
  - Hierarquização do FabricPool
  - Alterando o tipo de VM de armazenamento
  - Modo de gravação rápida

### Antes de começar

- Certifique-se de ter uma assinatura válida do Azure Marketplace.
- Certifique-se de atender aos requisitos de rede para um ["Implantação de HA em uma única AZ"](#) no Azure. Consulte ["Configurar a rede do Azure para o Cloud Volumes ONTAP"](#).

- Você precisa ter uma destas funções do Azure atribuídas para implantar o Cloud Volumes ONTAP:
  - O `contributor` função com as permissões padrão. Para mais informações, consulte o ["Documentação do Microsoft Azure: funções integradas do Azure"](#) .
  - Uma função RBAC personalizada com as seguintes permissões. Para mais informações, consulte o ["Documentação do Azure: Funções personalizadas do Azure"](#) .

```
"permissões": [ { "ações": [ "Microsoft.AAD/register/action",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Network/loadBalancers/write", "Microsoft.ClassicCompute/virtualMachines/write",
"Microsoft.Compute/capacityReservationGroups/deploy/action",
"Microsoft.ClassicCompute/virtualMachines/networkInterfaces/associatedNetworkSecurityGroups/
write", "Microsoft.Network/networkInterfaces/write", "Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Network/virtualNetworks/write", "Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/read", "Microsoft.Compute/disks/write",
"Microsoft.Compute/virtualMachineScaleSets/write", "Microsoft.Resources/deployments/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/subnets/write" ], "notActions": [], "dataActions": [],
"notDataActions": [] } ]
```



Se você registrou o provedor de recursos "Microsoft.storage" em sua assinatura, não precisará do `Microsoft.AAD/register/action` permissão. Para mais informações, consulte o ["Documentação do Azure: Permissões do Azure para Armazenamento"](#) .

## Passos

1. No site do marketplace do Azure, pesquise por produtos NetApp .
2. Selecione \* NetApp Cloud Volumes ONTAP direct\*.
3. Clique em **Criar** para iniciar o assistente de implantação.
4. Selecione um plano. A lista **Plano** normalmente exibe as versões mais recentes do Cloud Volumes ONTAP.
5. Na aba **Básico**, forneça estes detalhes:
  - **Assinatura**: Selecione uma assinatura. A implantação será vinculada ao número de assinatura.
  - **Grupo de recursos**: use um grupo de recursos existente ou crie um novo. Os grupos de recursos ajudam a alocar todos os recursos, como discos e VMs de armazenamento, dentro de um único grupo para um sistema Cloud Volumes ONTAP .
  - **Região**: selecione uma região que ofereça suporte à implantação de HA do Azure em uma única AZ. Você vê apenas as regiões disponíveis na lista.
  - **Tamanho**: Selecione um tamanho de VM de armazenamento para o Disco gerenciado Premium SSD v2 compatível.
  - **Zona**: Selecione uma zona para a região selecionada.
  - **Senha do administrador**: Defina uma senha. Use esta senha de administrador para efetuar login no sistema após a implantação.

- **Confirmar senha:** Digite novamente a mesma senha para confirmação.
  - Na aba **Rede**, adicione uma rede virtual e uma sub-rede ou selecione-as nas listas.



Para cumprir com as restrições do Microsoft Azure, você deve criar uma nova sub-rede ao configurar uma nova rede virtual. Da mesma forma, se você escolher uma rede existente, deverá selecionar uma sub-rede existente.

- Para selecionar um grupo de segurança de rede predefinido, selecione **Sim**. Selecione **Não** para atribuir um grupo de segurança de rede predefinido do Azure com as regras de tráfego necessárias. Para mais informações, consulte ["Regras de grupo de segurança para o Azure"](#) .
- Na guia **Avançado**, confirme se os dois recursos do Azure necessários para esta implantação foram definidos. Consulte ["Habilitar um recurso do Azure para implantações de AZ únicas do Cloud Volumes ONTAP"](#) e ["Habilitar o modo de alta disponibilidade para o Cloud Volumes ONTAP no Azure"](#) .
- Você pode definir pares de nomes e valores para os recursos ou grupos de recursos na guia **Tags**.
- Na aba **Revisar + criar**, revise os detalhes e inicie a implantação.

### Depois que você terminar

Selecione o ícone de notificação para visualizar o progresso da sua implantação. Após a implantação do Cloud Volumes ONTAP , você pode visualizar a VM de armazenamento listada para operações.

Uma vez acessível, use o ONTAP System Manager ou o ONTAP CLI para efetuar login na VM de armazenamento com as credenciais de administrador que você definiu. Depois disso, você pode criar volumes, LUNs ou compartilhamentos e começar a utilizar os recursos de armazenamento do Cloud Volumes ONTAP.

## Solucionar problemas de implantação

Os sistemas Cloud Volumes ONTAP implantados diretamente pelo marketplace do Azure não incluem suporte da NetApp. Caso surjam problemas durante a implantação, você pode solucioná-los e resolvê-los de forma independente.

### Passos

1. No site do marketplace do Azure, acesse **Diagnóstico de inicialização > Log serial**.
2. Baixe e investigue os logs serials.
3. Consulte a documentação do produto e os artigos da base de conhecimento (KB) para solução de problemas.
  - ["Documentação do marketplace do Azure"](#)
  - ["Documentação da NetApp"](#)
  - ["Artigos da base de conhecimento da NetApp"](#)

## Descubra os sistemas implantados no Console

Você pode descobrir os sistemas Cloud Volumes ONTAP que você implantou usando a implantação direta do Azure Marketplace e gerenciá-los na página **Sistemas** no Console. O agente do Console descobre os sistemas, os adiciona e aplica as licenças necessárias, além de desbloqueia todos os recursos do Console para esses sistemas. A configuração HA original em uma única AZ com discos gerenciados PSSD v2 é mantida, e o sistema é registrado na mesma assinatura do Azure e no mesmo grupo de recursos da implantação original.

## Sobre esta tarefa

Ao descobrir os sistemas Cloud Volumes ONTAP implantados usando a implantação direta do Azure Marketplace, o agente do Console executa estas tarefas:

- Substitui as licenças gratuitas dos sistemas descobertos como licenças regulares baseadas em capacidade "[Licenças Freemium](#)".
- Mantém os recursos existentes dos sistemas implantados e adiciona recursos adicionais do Console, como proteção de dados, gerenciamento de dados e recursos de segurança.
- Substitui as licenças instaladas nos nós por novas licenças ONTAP para NFS, CIFS (SMB), iSCSI, ARP, SnapLock e SnapMirror.
- Converte os números de série dos nós genéricos em números de série exclusivos.
- Atribui novas tags de sistema aos recursos, conforme necessário.
- Converte os endereços IP dinâmicos da instância em endereços IP estáticos.
- Habilita as funcionalidades de "[Hierarquização do FabricPool](#)", "[AutoSupport](#)", e "[escrever uma vez e ler muitas vezes](#)" (WORM) armazenamento nos sistemas implantados. Você pode ativar esses recursos no Console quando precisar deles.
- Registra as instâncias nas contas NSS usadas para descobri-las.
- Habilita recursos de gerenciamento de capacidade em "[modos automático e manual](#)" para os sistemas descobertos.

## Antes de começar

Certifique-se de que a implantação esteja concluída no marketplace do Azure. O agente do Console pode descobrir os sistemas somente quando a implantação estiver concluída e eles estiverem disponíveis para descoberta.

## Passos

No Console, você segue o procedimento padrão para descobrir sistemas existentes. Consulte "[Adicionar um sistema Cloud Volumes ONTAP existente ao Console](#)".



Durante a descoberta, você poderá ver mensagens de falha, mas pode ignorá-las até que o processo de descoberta seja concluído. Não modifique as configurações do Cloud Volumes ONTAP geradas pelo sistema no portal do marketplace do Azure durante a descoberta, especialmente as tags do sistema. Quaisquer alterações feitas nessas configurações podem levar a um comportamento inesperado do sistema.

## Depois que você terminar

Após a conclusão da descoberta, você poderá visualizar os sistemas listados na página **Sistemas** no Console. Você pode executar várias tarefas de gerenciamento, como "[expandindo o agregado](#)", "[adicionando volumes](#)", "[provisionamento de VMs de armazenamento adicionais](#)", e "[alterando os tipos de instância](#)".

## Links relacionados

Consulte a documentação do ONTAP para obter mais informações sobre como criar armazenamento:

- "[Criar volumes para NFS](#)"
- "[Criar LUNs para iSCSI](#)"
- "[Criar compartilhamentos para CIFS](#)"

## **Informações sobre direitos autorais**

Copyright © 2026 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 SOBRESSAIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO 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.