



Documentação do Cloud Volumes ONTAP

Cloud Volumes ONTAP

NetApp
December 20, 2024

Índice

Documentação do Cloud Volumes ONTAP	1
Notas de lançamento	2
O que há de novo	2
Limitações conhecidas	36
Notas de versão do Cloud Volumes ONTAP	37
Comece agora	38
Saiba mais sobre o Cloud Volumes ONTAP	38
Versões ONTAP compatíveis para novas implantações	39
Comece a usar o Amazon Web Services	41
Comece a usar o Microsoft Azure	120
Comece a usar o Google Cloud	173
Use o Cloud Volumes ONTAP	227
Gerenciamento de licenças	227
Administração de volume e LUN	241
Administração de agregados	268
Administração da VM de storage	273
Segurança e criptografia de dados	309
Administração do sistema	324
Saúde do sistema e eventos	366
Conceitos	371
Licenciamento	371
Armazenamento	379
Pares de alta disponibilidade	402
Segurança	421
Desempenho	423
Gerenciamento de licenças para BYOL baseado em nós	424
AutoSupport e consultor digital	427
Configuração padrão para Cloud Volumes ONTAP	428
Conhecimento e apoio	433
Registre-se para obter suporte	433
Obtenha ajuda	437
Avisos legais	443
Direitos de autor	443
Marcas comerciais	443
Patentes	443
Política de privacidade	443
Código aberto	443

Documentação do Cloud Volumes ONTAP

Notas de lançamento

O que há de novo

Saiba o que há de novo com o gerenciamento de Cloud Volumes ONTAP no BlueXP .

Os aprimoramentos descritos nesta página são específicos dos recursos do BlueXP que permitem o gerenciamento do Cloud Volumes ONTAP. Para saber o que há de novo com o próprio software Cloud Volumes ONTAP, ["Vá para as Notas de versão do Cloud Volumes ONTAP"](#)

9 de dezembro de 2024

Lista de VMs com suporte atualizadas para o Azure para se alinhar às práticas recomendadas

As famílias de máquinas DS_v2 e ES_v3 não estão mais disponíveis para seleção no BlueXP ao implantar novas instâncias do Cloud Volumes ONTAP no Azure. Essas famílias serão mantidas e apoiadas apenas em sistemas antigos e existentes. Novas implantações do Cloud Volumes ONTAP são suportadas no Azure somente a partir da versão 9.12.1. Recomendamos que mude para ES_v4 ou qualquer outra série compatível com Cloud Volumes ONTAP 9.12.1 e posterior. No entanto, as máquinas das séries DS_v2 e ES_v3 estarão disponíveis para novas implantações feitas através da API.

["Configurações compatíveis no Azure"](#)

11 de novembro de 2024

Fim da disponibilidade para licenças baseadas em nós

A NetApp planejou o fim da disponibilidade (EOA) e o fim do suporte (EOS) do licenciamento baseado em nós da Cloud Volumes ONTAP. A partir de 11 de novembro de 2024, a disponibilidade limitada de licenças baseadas em nós foi encerrada. O suporte para licenciamento baseado em nós termina em 31 de dezembro de 2024. Após a EOA de suas licenças baseadas em nós, você deve fazer a transição para o licenciamento baseado em capacidade usando a ferramenta de conversão de licença do BlueXP .

Para compromissos anuais ou de longo prazo, a NetApp recomenda que você entre em Contato com seu representante da NetApp antes da data da EOA ou da data de expiração da licença para garantir que os pré-requisitos para a transição estejam em vigor. Se você não tiver um contrato de longo prazo para um nó Cloud Volumes ONTAP e executar seu sistema com uma assinatura paga conforme o uso (PAYGO) sob demanda, é importante Planejar sua conversão antes da data EOS. Para contratos de longo prazo e assinaturas PAYGO, você pode usar a ferramenta de conversão de licenças BlueXP para uma conversão perfeita.

["Término da disponibilidade de licenças baseadas em nós"](#) ["Converta licenças baseadas em nós em capacidade"](#)

Remoção de implantações baseadas em nós do BlueXP

A opção de implantar sistemas Cloud Volumes ONTAP usando licenças baseadas em nós é obsoleta no BlueXP . Exceto em alguns casos especiais, você não pode usar licenças baseadas em nós para implantações do Cloud Volumes ONTAP para nenhum provedor de nuvem.

A NetApp reconhece os seguintes requisitos exclusivos de licenciamento em conformidade com as obrigações contratuais e as necessidades operacionais, e continuará a dar suporte a licenças baseadas em nós nessas situações:

- Clientes do setor público dos EUA
- Implantações em modo privado
- Implementações da região da China do Cloud Volumes ONTAP na AWS
- Se você tiver um nó de by-node válido e não expirado, traga sua própria licença (licença BYOL)

["Término da disponibilidade de licenças baseadas em nós"](#)

Adição de uma categoria inativa de dados do Cloud Volumes ONTAP no storage Azure Blob

O BlueXP agora permite que você selecione uma categoria inativa para armazenar os dados da categoria de capacidade no storage Blob do Azure. Adicionar a camada fria às camadas quentes e frias existentes fornece uma opção de storage mais econômica e uma melhor economia.

["Categorização de dados no Azure"](#)

Opção para restringir o acesso público à conta de armazenamento do Azure

Agora você tem a opção de restringir o acesso público à sua conta de storage para sistemas Cloud Volumes ONTAP no Azure. Ao desativar o acesso, você pode proteger seu endereço IP privado da exposição mesmo dentro do mesmo VNet, caso haja necessidade de cumprir com as políticas de segurança da sua organização. Essa opção também desativa a disposição de dados em camadas dos sistemas Cloud Volumes ONTAP e se aplica a pares de nó único e alta disponibilidade.

["Regras do grupo de segurança"](#).

Habilitação DE WORM após a implantação do Cloud Volumes ONTAP

Agora, você pode ativar o storage WORM (uma gravação, muitas leituras) em um sistema Cloud Volumes ONTAP existente usando o BlueXP. Esse recurso oferece a flexibilidade de habilitar o WORM em um ambiente de trabalho, mesmo que o WORM não tenha sido ativado durante sua criação. Uma vez ativado, você não pode desativar WORM.

["Habilitando WORM em um ambiente de trabalho do Cloud Volumes ONTAP"](#)

25 de outubro de 2024

Lista de VMs com suporte atualizada para o Google Cloud para se alinhar às práticas recomendadas

As máquinas da série n1 não estão mais disponíveis para seleção no BlueXP ao implantar novas instâncias do Cloud Volumes ONTAP no Google Cloud. As máquinas da série n1 serão mantidas e suportadas apenas em sistemas existentes mais antigos. Novas implantações do Cloud Volumes ONTAP são suportadas no Google Cloud apenas a partir da versão 9,8. Recomendamos que mude para os tipos de máquinas da série n2 compatíveis com o Cloud Volumes ONTAP 9,8 e posterior. As máquinas da série n1, no entanto, estarão disponíveis para novas implantações realizadas através da API.

["Configurações compatíveis no Google Cloud"](#).

Suporte a zonas locais para Amazon Web Services em modo privado

O BlueXP agora oferece suporte a zonas locais da AWS para implantações de alta disponibilidade (HA) do Cloud Volumes ONTAP no modo privado. O suporte anteriormente limitado apenas ao modo padrão foi agora estendido para incluir o modo privado.



As zonas locais da AWS não são suportadas ao usar o BlueXP no modo restrito.

Para obter mais informações sobre zonas locais da AWS com implantações de HA, ["Zonas locais da AWS"](#) consulte .

7 de outubro de 2024

Experiência de usuário aprimorada na seleção de versão para atualização

A partir desta versão, quando você tentar atualizar o Cloud Volumes ONTAP usando a notificação BlueXP , você receberá orientações sobre as versões padrão, mais recentes e compatíveis a serem usadas. Além disso, agora você pode selecionar o patch mais recente ou a versão principal compatível com sua instância do Cloud Volumes ONTAP, ou inserir manualmente uma versão para atualização.

["Atualize o software Cloud Volumes ONTAP"](#)

9 de setembro de 2024

As funcionalidades WORM e ARP não são mais carregáveis

Os recursos de segurança e proteção de dados incorporados do WORM (Write Once Read many) e do ARP (Autonomous ransomware Protection) serão oferecidos com licenças do Cloud Volumes ONTAP sem custo adicional. O novo modelo de preços se aplica às assinaturas BYOL e PAYGO/Marketplace novas e existentes da AWS, Azure e Google Cloud. As licenças baseadas em capacidade e baseadas em nós contêm ARP e WORM para todas as configurações, incluindo nó único e pares de alta disponibilidade (HA), sem custo adicional.

O preço simplificado traz a você esses benefícios:

- As contas que atualmente incluem WORM e ARP não terão mais cobranças por esses recursos. No futuro, sua cobrança só terá cobranças pelo uso da capacidade, como foi antes dessa alteração. Worm e ARP não serão mais incluídos em suas contas futuras.
- Se suas contas atuais não incluírem esses recursos, agora você pode optar por WORM e ARP sem custo adicional.
- Todas as ofertas do Cloud Volumes ONTAP para quaisquer novas contas excluirão cobranças por WORM e ARP.

Saiba mais sobre esses recursos:

- ["Aumento da proteção contra ransomware"](#)
- ["STORAGE WORM"](#)

23 de agosto de 2024

A região oeste do Canadá agora é compatível com a AWS

A região Oeste do Canadá agora é suportada na AWS para Cloud Volumes ONTAP 9.12.1 GA e posterior.

Para obter uma lista de todas as regiões, consulte ["Mapa das regiões globais na AWS"](#).

22 de agosto de 2024

Cloud Volumes ONTAP 9.15.1 GA

Agora, o BlueXP pode implantar e gerenciar o lançamento de disponibilidade geral do Cloud Volumes ONTAP 9.15.1 na AWS, Azure e Google Cloud.

["Saiba mais sobre os novos recursos incluídos nesta versão do Cloud Volumes ONTAP"](#).

8 de agosto de 2024

Pacotes de licenciamento do Edge Cache descontinuados

Os pacotes de licenciamento baseados em capacidade do Edge Cache não estarão mais disponíveis para implantações futuras do Cloud Volumes ONTAP. No entanto, você pode usar a API para aproveitar essa funcionalidade.

Suporte de versão mínima para Flash Cache no Azure

A versão mínima do Cloud Volumes ONTAP necessária para configurar o Flash Cache no Azure é 9.13.1 GA. Você só pode usar o ONTAP 9.13,1 GA e versões posteriores para implantar o Flash Cache em sistemas Cloud Volumes ONTAP para Azure.

Para obter as configurações suportadas, ["Configurações compatíveis no Azure"](#) consulte .

Avaliações gratuitas para assinaturas de marketplace obsoletas

A avaliação gratuita automática de 30 dias para assinaturas de pagamento conforme o uso no mercado do provedor de nuvem não estará mais disponível no Cloud Volumes ONTAP. A cobrança de qualquer tipo de assinatura do mercado (PAYGO ou contrato anual) será ativada a partir da primeira utilização, sem qualquer período de teste gratuito.

10 de junho de 2024

Cloud Volumes ONTAP 9.15.0

Agora, o BlueXP pode implantar e gerenciar o Cloud Volumes ONTAP 9.15.0 na AWS, Azure e Google Cloud.

["Saiba mais sobre os novos recursos incluídos nesta versão do Cloud Volumes ONTAP"](#).

17 de maio de 2024

Suporte a zonas locais do Amazon Web Services

O suporte para zonas locais da AWS agora está disponível para implantações do Cloud Volumes ONTAP HA. As zonas locais da AWS são uma implantação de infraestrutura onde storage, computação, banco de dados e outros serviços selecionados da AWS estão localizados perto de grandes cidades e áreas do setor.



As zonas locais da AWS são suportadas ao usar o BlueXP no modo padrão. Neste momento, as zonas locais da AWS não são suportadas ao usar o BlueXP no modo restrito ou no modo privado.

Para obter mais informações sobre zonas locais da AWS com implantações de HA, ["Zonas locais da](#)

[AWS](#) consulte .

23 de abril de 2024

Novas regiões com suporte para implantações de várias zonas de disponibilidade no Azure

As seguintes regiões agora oferecem suporte a implantações de várias zonas de disponibilidade no Azure para Cloud Volumes ONTAP 9.12.1 GA e versões posteriores:

- Alemanha Central Ocidental
- Polónia Central
- West US 3
- Israel Central
- Itália Norte
- Canadá Central

Para obter uma lista de todas as regiões, consulte "[Mapa das Regiões globais no Azure](#)"a .

A região de Joanesburgo agora é compatível com o Google Cloud

A região de Joanesburgo(`africa-south1`) agora é compatível com o Google Cloud para Cloud Volumes ONTAP 9.12.1 GA e posterior.

Para obter uma lista de todas as regiões, consulte "[Mapa das regiões globais no Google Cloud](#)"a .

Modelos de volume e tags não são mais compatíveis

Você não pode mais criar um volume a partir de um modelo ou editar as tags de um volume. Essas ações foram associadas ao serviço de remediação do BlueXP , que não está mais disponível.

8 de março de 2024

Suporte ao Amazon Instant Metadata Service v2

Na AWS, o Cloud Volumes ONTAP, o Mediador e o conector agora oferecem suporte ao Amazon Instant Metadata Service v2 (IMDSv2) para todas as funções. O IMDSv2 fornece proteção aprimorada contra vulnerabilidades. Apenas IMDSv1 foi anteriormente suportado.

Se exigido por suas políticas de segurança, você pode configurar suas instâncias do EC2 para usar o IMDSv2. Para obter instruções, "[Documentação de configuração e administração do BlueXP para gerenciar conectores existentes](#)" consulte .

5 de março de 2024

Cloud Volumes ONTAP 9.14.1 GA

Agora, o BlueXP pode implantar e gerenciar o lançamento de disponibilidade geral do Cloud Volumes ONTAP 9.14.1 na AWS, Azure e Google Cloud.

["Saiba mais sobre os novos recursos incluídos nesta versão do Cloud Volumes ONTAP"](#).

2 de fevereiro de 2024

Suporte para VMs da série Edv5 no Azure

O Cloud Volumes ONTAP agora suporta as seguintes VMs da série Edv5, começando com a versão 9.14.1.

- E4ds_v5
- E8ds_v5
- E20s_v5
- E32ds_v5
- E48ds_v5
- E64ds_v5

["Configurações compatíveis no Azure"](#)

16 de janeiro de 2024

Patch Releases no BlueXP

As versões de patch estão disponíveis no BlueXP apenas para as três versões mais recentes do Cloud Volumes ONTAP.

["Atualize o Cloud Volumes ONTAP"](#)

8 de janeiro de 2024

Novas VMs para várias zonas de disponibilidade do Azure

A partir do Cloud Volumes ONTAP 9.13.1, os seguintes tipos de VM oferecem suporte a várias zonas de disponibilidade do Azure para implantações de pares de alta disponibilidade novas e existentes:

- L16s_v3
- L32s_v3
- L48s_v3
- L64s_v3

["Configurações compatíveis no Azure"](#)

6 de dezembro de 2023

Cloud Volumes ONTAP 9.14.1 RC1

Agora, o BlueXP pode implantar e gerenciar o Cloud Volumes ONTAP 9.14.1 na AWS, Azure e Google Cloud.

["Saiba mais sobre os novos recursos incluídos nesta versão do Cloud Volumes ONTAP"](#).

Limite máximo de 300 TIB FlexVol volume

Agora você pode criar um FlexVol volume até o tamanho máximo de 300 TIB com o Gerenciador de sistema e a CLI do ONTAP a partir do Cloud Volumes ONTAP 9.12.1 P2 e 9.13.0 P2, e no BlueXP a partir do Cloud

Volumes ONTAP 9.13.1.

- ["Limites de armazenamento na AWS"](#)
- ["Limites de armazenamento no Azure"](#)
- ["Limites de armazenamento no Google Cloud"](#)

5 de dezembro de 2023

As seguintes alterações foram introduzidas.

Suporte a nova região no Azure

Suporte de região de zona de disponibilidade única

As seguintes regiões agora oferecem suporte a implantações de zona de disponibilidade única altamente disponíveis no Azure para Cloud Volumes ONTAP 9.12.1 GA e versões posteriores:

- Tel Aviv
- Milão

Suporte a várias regiões de zona de disponibilidade

As seguintes regiões agora oferecem suporte a implantações de várias zonas de disponibilidade altamente disponíveis no Azure para Cloud Volumes ONTAP 9.12.1 GA e versões posteriores:

- Central India
- Leste da Noruega
- Suíça Norte
- África do Sul Norte
- Emirados Árabes Unidos Norte

Para obter uma lista de todas as regiões, consulte ["Mapa das Regiões globais no Azure"](#).

10 de novembro de 2023

A seguinte alteração foi introduzida com a versão 3.9.35 do conector.

Região de Berlim agora suportada no Google Cloud

A região de Berlim agora é suportada no Google Cloud para Cloud Volumes ONTAP 9.12.1 GA e posterior.

Para obter uma lista de todas as regiões, consulte ["Mapa das regiões globais no Google Cloud"](#).

8 de novembro de 2023

A seguinte alteração foi introduzida com a versão 3.9.35 do conector.

A região de Tel Aviv agora é compatível com a AWS

A região de Tel Aviv agora é suportada na AWS para Cloud Volumes ONTAP 9.12.1 GA e posterior.

Para obter uma lista de todas as regiões, consulte ["Mapa das regiões globais na AWS"](#).

1 de novembro de 2023

A seguinte alteração foi introduzida com a versão 3.9.34 do conetor.

A região da Arábia Saudita agora é compatível com o Google Cloud

A região da Arábia Saudita agora é suportada no Google Cloud para Cloud Volumes ONTAP e no conetor para Cloud Volumes ONTAP 9.12.1 GA e posterior.

Para obter uma lista de todas as regiões, consulte ["Mapa das regiões globais no Google Cloud"](#) .

23 de outubro de 2023

A seguinte alteração foi introduzida com a versão 3.9.34 do conetor.

Novas regiões com suporte para implantações de várias zonas de disponibilidade de HA no Azure

As seguintes regiões no Azure agora oferecem suporte a implantações de várias zonas de disponibilidade altamente disponíveis para o Cloud Volumes ONTAP 9.12.1 GA e versões posteriores:

- Leste da Austrália
- Leste da Ásia
- França Central
- Norte da Europa
- Qatar Central
- Suécia Central
- Europa Ocidental
- West US 2

Para obter uma lista de todas as regiões que suportam várias zonas de disponibilidade, consulte o ["Mapa das Regiões globais no Azure"](#).

6 de outubro de 2023

A seguinte alteração foi introduzida com a versão 3.9.34 do conetor.

Cloud Volumes ONTAP 9.14.0

Agora, o BlueXP pode implantar e gerenciar o lançamento de disponibilidade geral do Cloud Volumes ONTAP 9.14.0 na AWS, Azure e Google Cloud.

["Saiba mais sobre os novos recursos incluídos nesta versão do Cloud Volumes ONTAP"](#).

10 de setembro de 2023

A seguinte alteração foi introduzida com a versão 3.9.33 do conetor.

Suporte para VMs da série Lsv3 no Azure

Os tipos de instância L48s_v3 e L64s_v3 agora são compatíveis com o Cloud Volumes ONTAP no Azure para implantações de nó único e par de alta disponibilidade com discos gerenciados compartilhados em zonas de

disponibilidade única e múltipla, a partir da versão 9.13.1. Esses tipos de instância oferecem suporte ao Flash Cache.

["Veja as configurações compatíveis para o Cloud Volumes ONTAP no Azure"](#) ["Veja os limites de storage do Cloud Volumes ONTAP no Azure"](#)

30 de julho de 2023

As seguintes alterações foram introduzidas com a versão 3.9.32 do conector.

Flash Cache e suporte a alta velocidade de gravação no Google Cloud

O Flash Cache e a alta velocidade de gravação podem ser ativados separadamente no Google Cloud para Cloud Volumes ONTAP 9.13.1 e posterior. A alta velocidade de gravação está disponível em todos os tipos de instância compatíveis. O Flash Cache é compatível com os seguintes tipos de instância:

- n2-padrão-16
- n2-padrão-32
- n2-padrão-48
- n2-padrão-64

Você pode usar esses recursos separadamente ou em conjunto em implantações de nó único e par de alta disponibilidade.

["Inicie o Cloud Volumes ONTAP no Google Cloud"](#)

Melhorias nos relatórios de uso

Várias melhorias nas informações exibidas nos relatórios de uso estão agora disponíveis. A seguir estão os aprimoramentos dos relatórios de uso:

- A unidade TIB está agora incluída no nome das colunas.
- Um novo campo "node(s)" para números de série está agora incluído.
- Uma nova coluna "tipo de workload" agora está incluída no relatório de uso das VMs de storage.
- Nomes de ambientes de trabalho agora incluídos nos relatórios de uso de volume e VMs de storage.
- O tipo de volume "arquivo" agora é rotulado como "primário (leitura/gravação)".
- O tipo de volume "secundário" agora é rotulado como "secundário (DP)".

Para obter mais informações sobre relatórios de uso, ["Transfira relatórios de utilização"](#) consulte .

26 de julho de 2023

As seguintes alterações foram introduzidas com a versão 3.9.31 do conector.

Cloud Volumes ONTAP 9.13.1 GA

Agora, o BlueXP pode implantar e gerenciar o lançamento de disponibilidade geral do Cloud Volumes ONTAP 9.13.1 na AWS, Azure e Google Cloud.

["Saiba mais sobre os novos recursos incluídos nesta versão do Cloud Volumes ONTAP"](#).

2 de julho de 2023

As seguintes alterações foram introduzidas com a versão 3.9.31 do conetor.

Suporte para implantações de várias zonas de disponibilidade de HA no Azure

O Japão Leste e a Coreia Central no Azure agora oferecem suporte a implantações de várias zonas de disponibilidade de HA para Cloud Volumes ONTAP 9.12.1 GA e posterior.

Para obter uma lista de todas as regiões que suportam várias zonas de disponibilidade, consulte o ["Mapa das Regiões globais no Azure"](#).

Suporte à proteção autônoma contra ransomware

A proteção autônoma contra ransomware (ARP) agora é suportada no Cloud Volumes ONTAP. O suporte ARP está disponível no Cloud Volumes ONTAP versão 9.12.1 e posterior.

Para saber mais sobre ARP com Cloud Volumes ONTAP, ["Proteção autônoma contra ransomware"](#) consulte .

26 de junho de 2023

A seguinte alteração foi introduzida com a versão 3.9.30 do conetor.

Cloud Volumes ONTAP 9.13.1 RC1

Agora, o BlueXP pode implantar e gerenciar o Cloud Volumes ONTAP 9.13.1 na AWS, Azure e Google Cloud.

["Saiba mais sobre os novos recursos incluídos nesta versão do Cloud Volumes ONTAP"](#).

4 de junho de 2023

A seguinte alteração foi introduzida com a versão 3.9.30 do conetor.

Atualização do seletor da versão de atualização do Cloud Volumes ONTAP

Através da página Atualizar Cloud Volumes ONTAP, agora você pode optar por atualizar para a versão mais recente disponível do Cloud Volumes ONTAP ou uma versão mais antiga.

Para saber mais sobre como atualizar o Cloud Volumes ONTAP através do BlueXP , ["Atualize o Cloud Volumes ONTAP"](#) consulte .

7 de maio de 2023

As seguintes alterações foram introduzidas com a versão 3.9.29 do conetor.

A região do Qatar agora é compatível com o Google Cloud

A região do Qatar agora é compatível com o Google Cloud para Cloud Volumes ONTAP e o conetor para Cloud Volumes ONTAP 9.12.1 GA e posterior.

Suécia região Central agora suportada no Azure

A região Central da Suécia é agora suportada no Azure para Cloud Volumes ONTAP e no conetor para Cloud Volumes ONTAP 9.12.1 GA e posterior.

Suporte para implantações de várias zonas de disponibilidade de HA no Azure Australia East

A região Leste da Austrália no Azure agora oferece suporte a implantações de várias zonas de disponibilidade de HA para Cloud Volumes ONTAP 9.12.1 GA e versões posteriores.

Avaria na utilização de carregamento

Agora você pode descobrir o que você está sendo cobrado quando você está inscrito em licenças baseadas em capacidade. Os seguintes tipos de relatórios de utilização estão disponíveis para transferência a partir da carteira digital no BlueXP. Os relatórios de uso fornecem detalhes de capacidade de suas assinaturas e informam como você está sendo cobrado pelos recursos em suas assinaturas do Cloud Volumes ONTAP. Os relatórios transferíveis podem ser facilmente compartilhados com outras pessoas.

- Uso do pacote Cloud Volumes ONTAP
- Uso de alto nível
- Utilização de VMs de storage
- Utilização de volumes

Para obter mais informações, ["Gerenciar licenças baseadas em capacidade"](#) consulte .

A notificação agora é exibida ao acessar o BlueXP sem uma assinatura do mercado

Uma notificação agora é exibida sempre que você acessa o Cloud Volumes ONTAP no BlueXP sem uma assinatura do mercado. A notificação afirma que "uma assinatura de mercado para este ambiente de trabalho é necessária para estar em conformidade com os termos e condições da Cloud Volumes ONTAP."

4 de abril de 2023

A partir do Cloud Volumes ONTAP 9.12.1 GA, as regiões da China agora são suportadas na AWS da seguinte forma.

- Sistemas de nó único são compatíveis.
- As licenças adquiridas diretamente da NetApp são suportadas.

Para obter informações sobre a disponibilidade regional, consulte o ["Mapas de regiões globais para Cloud Volumes ONTAP"](#).

3 de abril de 2023

As seguintes alterações foram introduzidas com a versão 3.9.28 do conector.

Região de Turim agora suportada no Google Cloud

A região de Turim é agora suportada no Google Cloud para Cloud Volumes ONTAP e no conector para Cloud Volumes ONTAP 9.12.1 GA e posterior.

Aprimoramento da carteira digital BlueXP

A carteira digital BlueXP agora mostra a capacidade licenciada que você comprou com ofertas privadas do mercado.

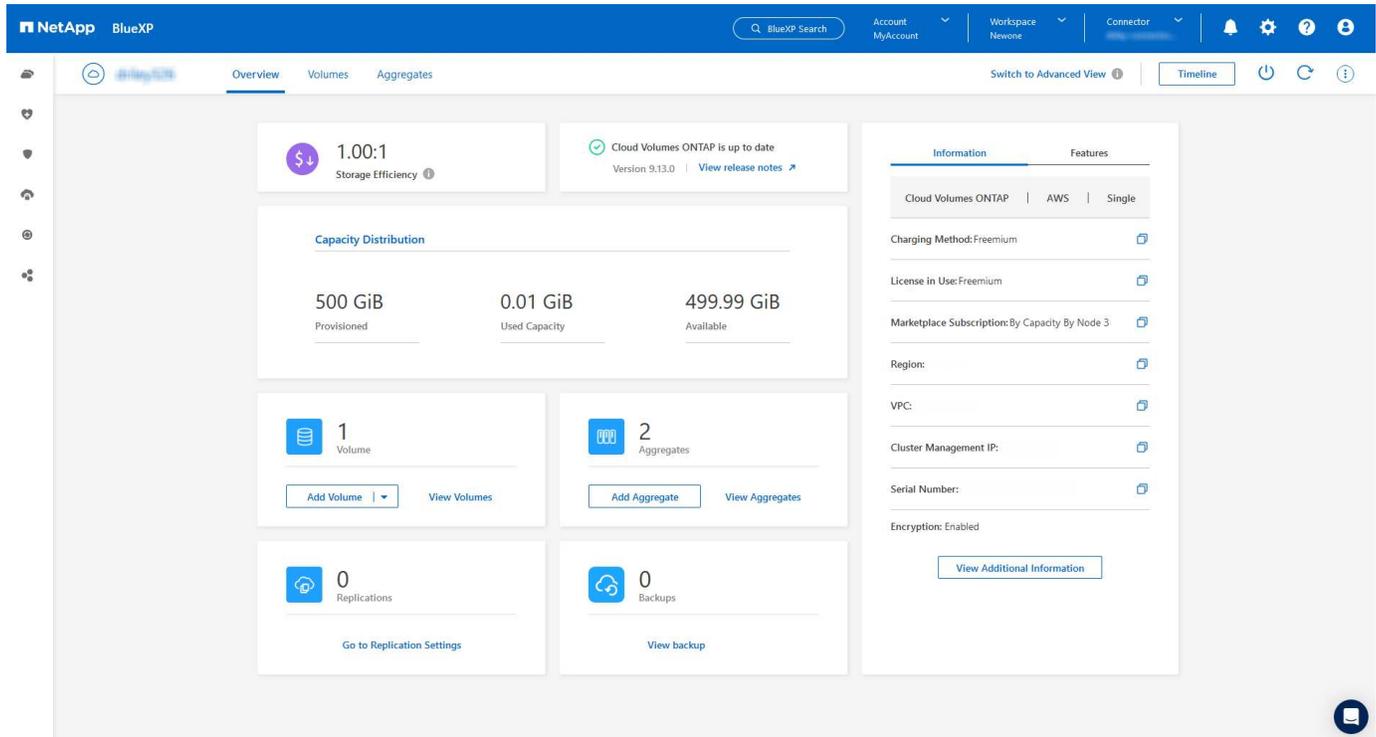
["Saiba como visualizar a capacidade consumida na sua conta"](#).

Suporte para comentários durante a criação de volume

Esta versão permite que você faça comentários ao criar um volume Cloud Volumes ONTAP FlexGroup ou FlexVol volume ao usar a API.

Redesign da interface de usuário do BlueXP para Cloud Volumes ONTAP Visão geral, volumes e páginas agregadas

O BlueXP agora tem uma interface de usuário redesenhada para a Visão geral do Cloud Volumes ONTAP, volumes e páginas agregadas. O design baseado em Azulejo apresenta informações mais abrangentes em cada bloco para uma melhor experiência do usuário.

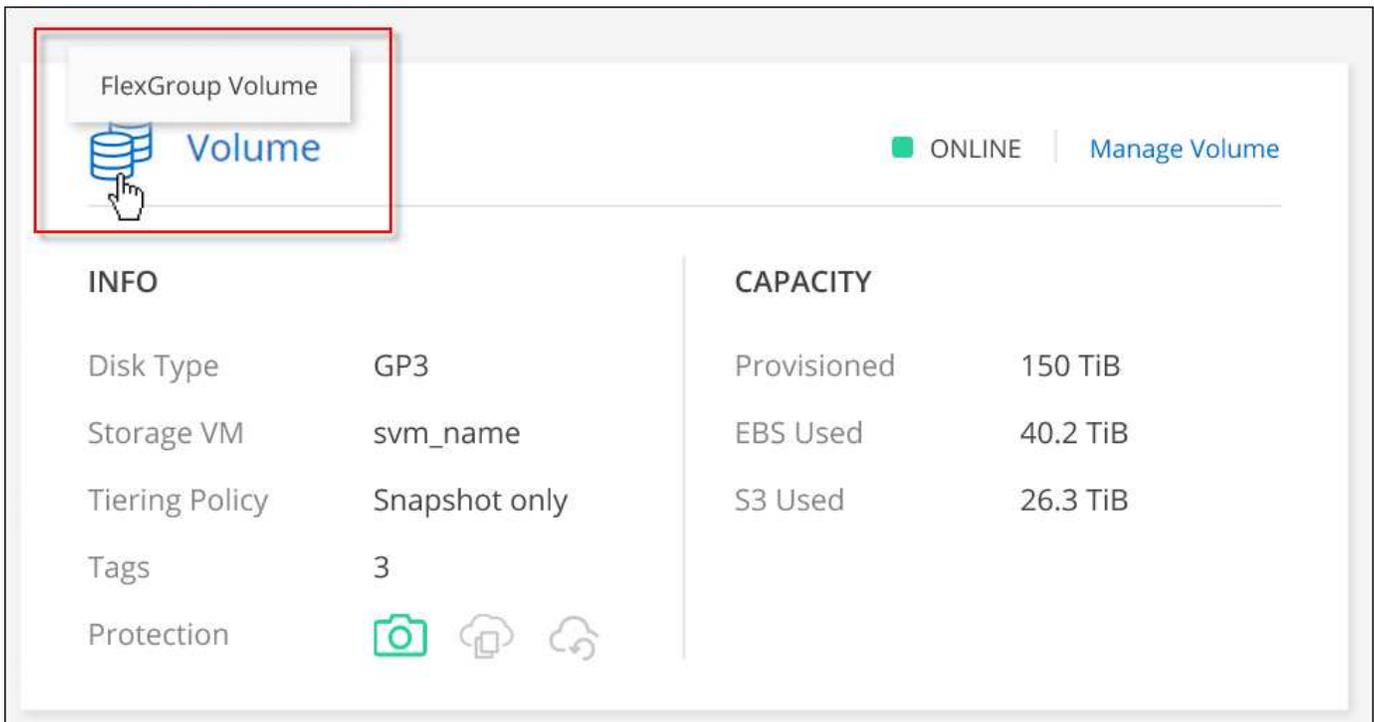


Volumes FlexGroup visíveis através do Cloud Volumes ONTAP

Os volumes do FlexGroup criados por meio do Gerenciador de sistemas do ONTAP ou da CLI do ONTAP agora podem ser visualizados diretamente por meio do bloco de volumes redesenhado no BlueXP. Idêntico às informações fornecidas para o FlexVol volumes, o BlueXP fornece informações detalhadas para volumes FlexGroup criados por meio de um bloco volumes dedicado.



Atualmente, você só pode exibir volumes FlexGroup existentes no BlueXP. A capacidade de criar volumes do FlexGroup no BlueXP não está disponível, mas planejada para um lançamento futuro.



"Saiba mais sobre como visualizar volumes FlexGroup criados."

13 de março de 2023

Apoio da região da China

A partir do Cloud Volumes ONTAP 9.12.1 GA, o suporte à região da China agora é suportado no Azure da seguinte forma.

- Cloud Volumes ONTAP é suportado na China Norte 3.
- Sistemas de nó único são compatíveis.
- As licenças adquiridas diretamente da NetApp são suportadas.

Para obter informações sobre a disponibilidade regional, consulte o "[Mapas de regiões globais para Cloud Volumes ONTAP](#)".

5 de março de 2023

As seguintes alterações foram introduzidas com a versão 3.9.27 do conector.

Cloud Volumes ONTAP 9.13.0

Agora, o BlueXP pode implantar e gerenciar o Cloud Volumes ONTAP 9.13.0 na AWS, Azure e Google Cloud.

"Saiba mais sobre os novos recursos incluídos nesta versão do Cloud Volumes ONTAP".

16 TIB e 32 Tib suporte no Azure

O Cloud Volumes ONTAP agora oferece suporte a tamanhos de disco TIB de 16 TIB e 32 TIB para implantações de alta disponibilidade executadas em discos gerenciados no Azure.

Saiba mais ["Tamanhos de disco compatíveis no Azure"](#) sobre o .

Licença MTEKM

A licença MTEKM (Gerenciamento de chaves de criptografia de vários locatários) agora está incluída em sistemas Cloud Volumes ONTAP novos e existentes que executam a versão 9.12.1 GA ou posterior.

O gerenciamento de chaves externas com alocação a vários clientes permite que as VMs de storage individuais (SVMs) mantenham suas próprias chaves por meio de um servidor KMIP ao usar o NetApp volume Encryption.

["Saiba como criptografar volumes com as soluções de criptografia NetApp"](#).

Suporte para ambientes sem internet

O Cloud Volumes ONTAP agora é compatível com qualquer ambiente de nuvem que tenha isolamento completo da Internet. Somente o licenciamento baseado em nó (BYOL) é compatível nesses ambientes. O licenciamento baseado em capacidade não é suportado. Para começar, instale manualmente o software Connector, faça login no console BlueXP que está sendo executado no conetor, adicione sua licença BYOL à carteira digital BlueXP e, em seguida, implante o Cloud Volumes ONTAP.

- ["Instale o conetor num local sem acesso à Internet"](#)
- ["Acesse o console do BlueXP no conetor"](#)
- ["Adicione uma licença não atribuída"](#)

Flash Cache e alta velocidade de gravação no Google Cloud

Suporte para cache Flash, alta velocidade de gravação e uma unidade de transmissão máxima (MTU) alta de 8.896 bytes agora está disponível para instâncias selecionadas com a versão Cloud Volumes ONTAP 9.13.0.

Saiba mais ["Configurações compatíveis com licença para o Google Cloud"](#) sobre o .

5 de fevereiro de 2023

As seguintes alterações foram introduzidas com a versão 3.9.26 do conetor.

Criação de grupos de posicionamento na AWS

Uma nova configuração agora está disponível para criação de grupo de posicionamento com implantações de zona de disponibilidade única (AZ) do AWS HA. Agora você pode optar por ignorar criações de grupos de colocação com falha e permitir que implantações de AZ únicas do AWS HA sejam concluídas com sucesso.

Para obter informações detalhadas sobre como configurar a configuração de criação do grupo de posicionamento, ["Configurar a criação do grupo de posicionamento para AWS HA Single AZ"](#) consulte .

Atualização de configuração de zona DNS privada

Uma nova configuração está agora disponível para que você possa evitar criar um link entre uma zona DNS privada e uma rede virtual ao usar o Azure Private Links. A criação está ativada por predefinição.

["Forneça ao BlueXP detalhes sobre o DNS Privado do Azure"](#)

STORAGE WORM e categorização de dados

Agora, você pode habilitar o storage WORM e disposição de dados em camadas ao criar um sistema Cloud Volumes ONTAP 9,8 ou posterior. Ao habilitar a disposição de dados em categorias com storage WORM, você pode categorizar os dados em um armazenamento de objetos na nuvem.

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

1 de janeiro de 2023

As seguintes alterações foram introduzidas com a versão 3.9.25 do conetor.

Pacotes de licenciamento disponíveis no Google Cloud

Pacotes de licenciamento otimizados e baseados em capacidade do Edge Cache estão disponíveis para o Cloud Volumes ONTAP no Google Cloud Marketplace como uma oferta de pagamento conforme o uso ou como um contrato anual.

["Licenciamento do Cloud Volumes ONTAP"](#)Consulte a .

Configuração padrão para Cloud Volumes ONTAP

A licença MTEKM (Gerenciamento de chave de criptografia de vários locatários) não está mais incluída nas novas implantações do Cloud Volumes ONTAP.

Para obter mais informações sobre as licenças de recursos do ONTAP instaladas automaticamente com o Cloud Volumes ONTAP, ["Configuração padrão para Cloud Volumes ONTAP"](#)consulte .

15 de dezembro de 2022

Cloud Volumes ONTAP 9.12.0

Agora, o BlueXP pode implantar e gerenciar o Cloud Volumes ONTAP 9.12.0 na AWS e no Google Cloud.

["Saiba mais sobre os novos recursos incluídos nesta versão do Cloud Volumes ONTAP"](#).

8 de dezembro de 2022

Cloud Volumes ONTAP 9.12.1

Agora, a BlueXP pode implantar e gerenciar o Cloud Volumes ONTAP 9.12.1, que inclui suporte a novos recursos e regiões de provedores de nuvem adicionais.

["Saiba mais sobre os novos recursos incluídos nesta versão do Cloud Volumes ONTAP"](#)

4 de dezembro de 2022

As seguintes alterações foram introduzidas com a versão 3.9.24 do conetor.

O WORM e o backup em nuvem agora estão disponíveis durante a criação do Cloud Volumes ONTAP

A capacidade de ativar os recursos WORM (uma gravação, muitas leituras) e do backup em nuvem agora está disponível durante o processo de criação do Cloud Volumes ONTAP.

Região de Israel agora suportada no Google Cloud

A região de Israel agora é compatível com o Google Cloud para Cloud Volumes ONTAP e o conector para o Cloud Volumes ONTAP 9.11.1 P3 e posterior.

15 de novembro de 2022

As seguintes alterações foram introduzidas com a versão 3.9.23 do conector.

Licença ONTAP S3 no Google Cloud

Uma licença do ONTAP S3 agora está incluída em sistemas Cloud Volumes ONTAP novos e existentes que executam a versão 9.12.1 ou posterior no Google Cloud Platform.

["Saiba como configurar e gerenciar serviços de armazenamento de objetos S3 no ONTAP"](#)

6 de novembro de 2022

As seguintes alterações foram introduzidas com a versão 3.9.23 do conector.

Mover grupos de recursos no Azure

Agora você pode mover um ambiente de trabalho de um grupo de recursos para um grupo de recursos diferente no Azure na mesma assinatura do Azure.

Para obter mais informações, ["Movendo grupos de recursos"](#) consulte .

Certificação NDMP-copy

Agora, a cópia NDMP é certificada para uso com o Cloud volume ONTAP.

Para obter informações sobre como configurar e usar o NDMP, ["Visão geral da configuração NDMP"](#) consulte .

Suporte a criptografia de disco gerenciado para Azure

Foi adicionada uma nova permissão do Azure que agora permite encriptar todos os discos geridos aquando da criação.

Para obter mais informações sobre esta nova funcionalidade, ["Configure o Cloud Volumes ONTAP para usar uma chave gerenciada pelo cliente no Azure"](#) consulte .

18 de setembro de 2022

As seguintes alterações foram introduzidas com a versão 3.9.22 do conector.

Melhorias na carteira digital

- A carteira digital agora mostra um resumo do pacote de licenciamento de e/S otimizado e da capacidade WORM provisionada para sistemas Cloud Volumes ONTAP em sua conta.

Esses detalhes podem ajudá-lo a entender melhor como você está sendo cobrado e se precisa comprar capacidade adicional.

["Saiba como visualizar a capacidade consumida na sua conta"](#).

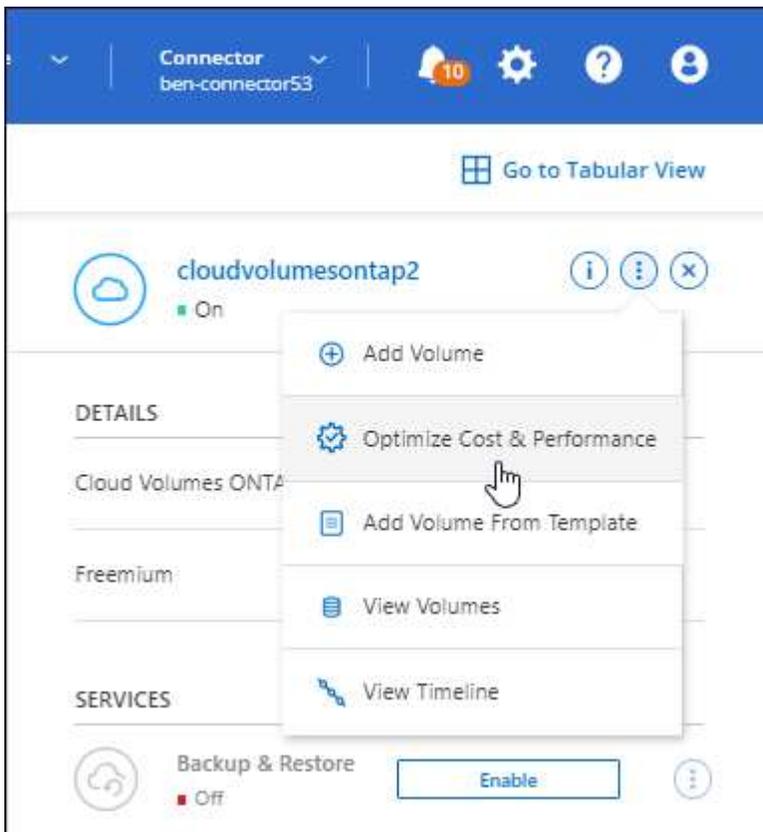
- Agora você pode mudar de um método de carregamento para o método de carregamento otimizado.

["Saiba como alterar os métodos de carregamento"](#).

Otimizar os custos e a performance

Agora você pode otimizar o custo e o desempenho de um sistema Cloud Volumes ONTAP diretamente a partir do Canvas.

Depois de selecionar um ambiente de trabalho, você pode escolher a opção **Otimizar Custo & Performance** para alterar o tipo de instância para o Cloud Volumes ONTAP. Escolher uma instância de menor porte pode ajudar a reduzir custos, ao mesmo tempo em que mudar para uma instância de maior porte pode ajudar a otimizar o desempenho.



Notificações do AutoSupport

O BlueXP irá agora gerar uma notificação se um sistema Cloud Volumes ONTAP não conseguir enviar mensagens AutoSupport. A notificação inclui um link para instruções que você pode usar para solucionar problemas de rede.

31 de julho de 2022

As seguintes alterações foram introduzidas com a versão 3.9.21 do conetor.

Licença MTEKM

A licença MTEKM (Gerenciamento de chaves de criptografia de vários locatários) agora está incluída em sistemas Cloud Volumes ONTAP novos e existentes que executam a versão 9.11.1 ou posterior.

O gerenciamento de chaves externas com alocação a vários clientes permite que as VMs de storage individuais (SVMs) mantenham suas próprias chaves por meio de um servidor KMIP ao usar o NetApp volume Encryption.

["Saiba como criptografar volumes com as soluções de criptografia NetApp"](#).

Servidor proxy

O BlueXP agora configura automaticamente seus sistemas Cloud Volumes ONTAP para usar o conector como um servidor proxy, se uma conexão de saída de Internet não estiver disponível para enviar mensagens AutoSupport.

O AutoSupport monitora proativamente a integridade do sistema e envia mensagens para o suporte técnico da NetApp.

O único requisito é garantir que o grupo de segurança do conector permita conexões *inbound* pela porta 3128. Você precisará abrir essa porta depois de implantar o conector.

Alterar o método de carregamento

Agora você pode alterar o método de carregamento de um sistema Cloud Volumes ONTAP que usa licenciamento baseado em capacidade. Por exemplo, se você implantou um sistema Cloud Volumes ONTAP com o pacote Essentials, poderá alterá-lo para o pacote Professional se a sua empresa precisar ser alterada. Este recurso está disponível na carteira digital.

["Saiba como alterar os métodos de carregamento"](#).

Aprimoramento do grupo de segurança

Quando você cria um ambiente de trabalho do Cloud Volumes ONTAP, a interface de usuário agora permite que você escolha se deseja que o grupo de segurança predefinido permita tráfego somente na rede selecionada (recomendado) ou em todas as redes.

Connectivity

Security Group

Generated security group Use existing security group

Allow traffic within:

The selected VPC only (recommended) ▾

SSH Authentication Method

Password Key Pair

18 de julho de 2022

Novos pacotes de licenciamento no Azure

Dois novos pacotes de licenciamento baseados em capacidade estão disponíveis para o Cloud Volumes ONTAP no Azure quando você paga por meio de uma assinatura do Azure Marketplace:

- **Otimizado:** Pague por capacidade provisionada e operações de e/S separadamente
- **Edge Cache:** Licenciamento para "[Cloud volumes Edge Cache](#)"

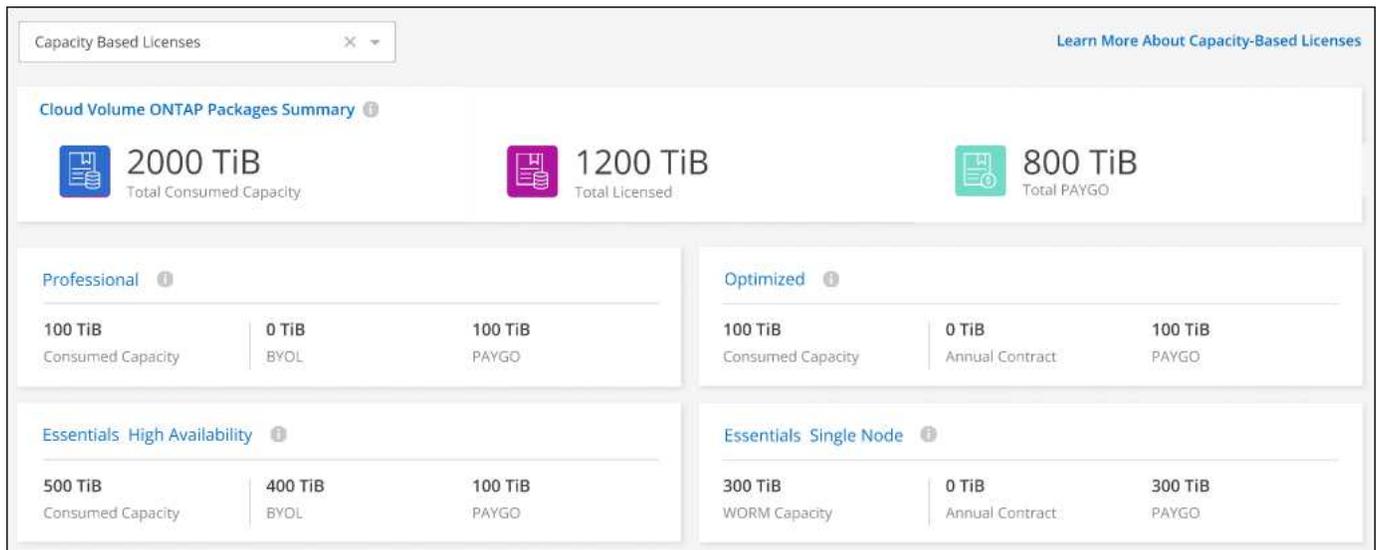
["Saiba mais sobre esses pacotes de licenciamento"](#).

3 de julho de 2022

As seguintes alterações foram introduzidas com a versão 3.9.20 do conector.

Carteira digital

A carteira Digital agora mostra a capacidade total consumida na sua conta e a capacidade consumida pelo pacote de licenciamento. Isso pode ajudá-lo a entender como você está sendo cobrado e se você precisa comprar capacidade adicional.



Aprimoramento de volumes elásticos

O BlueXP agora oferece suporte ao recurso volumes elásticos do Amazon EBS ao criar um ambiente de trabalho do Cloud Volumes ONTAP a partir da interface do usuário. O recurso volumes elásticos é habilitado por padrão ao usar discos GP3 ou IO1. Você pode escolher a capacidade inicial com base nas suas necessidades de storage e revisá-la após a implantação do Cloud Volumes ONTAP.

["Saiba mais sobre o suporte a volumes elásticos na AWS"](#).

Licença do ONTAP S3 na AWS

Uma licença do ONTAP S3 agora está incluída em sistemas Cloud Volumes ONTAP novos e existentes que executam a versão 9.11.0 ou posterior na AWS.

["Saiba como configurar e gerenciar serviços de armazenamento de objetos S3 no ONTAP"](#)

Novo suporte à região do Azure Cloud

A partir da versão 9.10.1, o Cloud Volumes ONTAP agora é suportado na região Azure West US 3.

["Veja a lista completa de regiões compatíveis com o Cloud Volumes ONTAP"](#)

Licença ONTAP S3 no Azure

Uma licença do ONTAP S3 agora está incluída em sistemas Cloud Volumes ONTAP novos e existentes que executam a versão 9.9.1 ou posterior no Azure.

["Saiba como configurar e gerenciar serviços de armazenamento de objetos S3 no ONTAP"](#)

7 de junho de 2022

As seguintes alterações foram introduzidas com a versão 3.9.19 do conetor.

Cloud Volumes ONTAP 9.11.1

Agora, a BlueXP pode implantar e gerenciar o Cloud Volumes ONTAP 9.11.1, que inclui suporte a novos recursos e regiões de provedores de nuvem adicionais.

["Saiba mais sobre os novos recursos incluídos nesta versão do Cloud Volumes ONTAP"](#)

Nova Vista Avançada

Se você precisar executar o gerenciamento avançado do Cloud Volumes ONTAP, pode fazê-lo usando o Gerenciador de sistemas do ONTAP, que é uma interface de gerenciamento fornecida com um sistema ONTAP. Incluímos a interface do Gerenciador de sistema diretamente no BlueXP para que você não precise sair do BlueXP para gerenciamento avançado.

Esta visualização avançada está disponível como pré-visualização com o Cloud Volumes ONTAP 9.10.0 e posterior. Planejamos refinar essa experiência e adicionar melhorias nos próximos lançamentos. Por favor, envie-nos feedback usando o chat no produto.

["Saiba mais sobre a visualização avançada"](#).

Suporte para volumes elásticos do Amazon EBS

O suporte ao recurso volumes elásticos do Amazon EBS com um agregado Cloud Volumes ONTAP fornece melhor desempenho e capacidade adicional, ao mesmo tempo que permite que o BlueXP aumente automaticamente a capacidade de disco subjacente conforme necessário.

O suporte para volumes elásticos está disponível a partir de *new* sistemas Cloud Volumes ONTAP 9.11.0 e com os tipos de disco EBS GP3 e IO1.

["Saiba mais sobre o suporte para volumes elásticos"](#).

Observe que o suporte a volumes elásticos requer novas permissões da AWS para o conetor:

```
"ec2:DescribeVolumesModifications",  
"ec2:ModifyVolume",
```

Certifique-se de fornecer essas permissões a cada conjunto de credenciais da AWS que você adicionou ao BlueXP. ["Veja a política de conetores mais recente da AWS"](#).

Suporte para a implantação de pares de HA em sub-redes compartilhadas da AWS

O Cloud Volumes ONTAP 9.11.1 inclui suporte ao compartilhamento de VPC da AWS. Esta versão do conetor permite implantar um par de HA em uma sub-rede compartilhada da AWS ao usar a API.

["Saiba como implantar um par de HA em uma sub-rede compartilhada"](#).

Acesso limitado à rede ao usar endpoints de serviço

O BlueXP agora limita o acesso à rede ao usar um endpoint de serviço VNet para conexões entre contas Cloud Volumes ONTAP e armazenamento. O BlueXP usa um endpoint de serviço se você desativar as conexões de link privado do Azure.

["Saiba mais sobre o Azure Private Link Connections com o Cloud Volumes ONTAP"](#).

Suporte para a criação de VMs de storage no Google Cloud

Várias VMs de storage agora são compatíveis com o Cloud Volumes ONTAP no Google Cloud, a partir da versão 9.11.1. A partir dessa versão do conetor, o BlueXP permite criar VMs de storage em pares de HA do

Cloud Volumes ONTAP usando a API.

O suporte para a criação de VMs de armazenamento requer novas permissões do Google Cloud para o conector:

- `compute.instanceGroups.get`
- `compute.addresses.get`

Observe que você deve usar a CLI ou o Gerenciador de sistema do ONTAP para criar uma VM de storage em um único sistema de nó.

- ["Saiba mais sobre os limites de VM de armazenamento no Google Cloud"](#)
- ["Saiba como criar VMs de armazenamento de fornecimento de dados para o Cloud Volumes ONTAP no Google Cloud"](#)

2 de maio de 2022

As seguintes alterações foram introduzidas com a versão 3.9.18 do conector.

Cloud Volumes ONTAP 9.11.0

Agora, o BlueXP pode implantar e gerenciar o Cloud Volumes ONTAP 9.11.0.

["Saiba mais sobre os novos recursos incluídos nesta versão do Cloud Volumes ONTAP"](#).

Aprimoramento das atualizações do mediador

Quando o BlueXP atualiza o mediador de um par de HA, ele agora valida que uma nova imagem de mediador está disponível antes de excluir o disco de inicialização. Esta alteração garante que o mediador possa continuar a funcionar com sucesso se o processo de atualização não for bem sucedido.

O separador K8s foi removido

A guia K8s foi obsoleta em uma versão anterior e agora foi removida.

Contrato anual no Azure

Os pacotes Essenciais e Professional estão agora disponíveis no Azure através de um contrato anual. Você pode entrar 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 o NetApp compartilhar a oferta privada com você, você pode selecionar o plano anual ao se inscrever no mercado Azure durante a criação do ambiente de trabalho.

["Saiba mais sobre licenciamento"](#).

S3 Glacier Instant Retrieval

Agora você pode armazenar dados em camadas na classe de armazenamento Amazon S3 Glacier Instant Retrieval.

["Saiba como alterar a classe de armazenamento para dados em camadas"](#).

Novas permissões da AWS necessárias para o conetor

As permissões a seguir agora são necessárias para criar um grupo de posicionamento de spread da AWS ao implantar um par de HA em uma única zona de disponibilidade (AZ):

```
"ec2:DescribePlacementGroups",  
"iam:GetRolePolicy",
```

Essas permissões agora são necessárias para otimizar a forma como o BlueXP cria o grupo de posicionamento.

Certifique-se de fornecer essas permissões a cada conjunto de credenciais da AWS que você adicionou ao BlueXP. ["Veja a política de conetores mais recente da AWS"](#).

Novo suporte à região do Google Cloud

O Cloud Volumes ONTAP agora é compatível com as seguintes regiões do Google Cloud começando com a versão 9.10.1:

- Delhi (Ásia-south2)
- Melbourne (austrália-southeast2)
- Milão (Europa-west8) - apenas nó único
- Santiago (américa do sul-west1) - único nó apenas

["Veja a lista completa de regiões compatíveis com o Cloud Volumes ONTAP"](#)

Suporte para n2-standard-16 no Google Cloud

O tipo de máquina n2-padrão-16 agora é compatível com o Cloud Volumes ONTAP no Google Cloud, começando com a versão 9.10.1.

["Veja as configurações compatíveis do Cloud Volumes ONTAP no Google Cloud"](#)

Melhorias nas políticas de firewall do Google Cloud

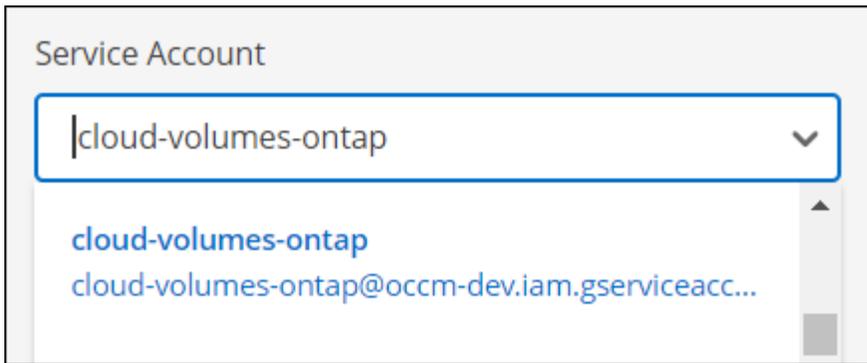
- Quando você cria um par de HA do Cloud Volumes ONTAP no Google Cloud, o BlueXP exibirá todas as políticas de firewall existentes em uma VPC.

Anteriormente, o BlueXP não exibia nenhuma política no VPC-1, VPC-2 ou VPC-3 que não tivesse uma tag de destino.

- Quando você cria um sistema de nó único do Cloud Volumes ONTAP no Google Cloud, agora você pode escolher se deseja que a política de firewall predefinida permita tráfego somente na VPC selecionada (recomendada) ou em todos os VPCs.

Aprimoramento das contas de serviço do Google Cloud

Quando você seleciona a conta de serviço do Google Cloud para usar com o Cloud Volumes ONTAP, o BlueXP agora exibe o endereço de e-mail associado a cada conta de serviço. A exibição do endereço de e-mail pode facilitar a distinção entre contas de serviço que compartilham o mesmo nome.



3 de abril de 2022

A ligação do Gestor do sistema foi removida

Removemos o link do Gerenciador de sistema que estava anteriormente disponível em um ambiente de trabalho do Cloud Volumes ONTAP.

Você ainda pode se conectar ao Gerenciador do sistema inserindo o endereço IP de gerenciamento de cluster em um navegador da Web que tenha uma conexão com o sistema Cloud Volumes ONTAP. ["Saiba mais sobre como conectar-se ao System Manager"](#).

Carregamento para armazenamento WORM

Agora que a taxa especial introdutória expirou, agora você será cobrado pelo uso de armazenamento WORM. O carregamento é feito por hora, de acordo com a capacidade total provisionada de volumes WORM. Isso se aplica a sistemas Cloud Volumes ONTAP novos e existentes.

["Saiba mais sobre os preços para storage WORM"](#).

27 de fevereiro de 2022

As seguintes alterações foram introduzidas com a versão 3.9.16 do conector.

Assistente de volume redesenhado

O assistente criar novo volume que introduzimos recentemente está agora disponível ao criar um volume em um agregado específico a partir da opção **Alocação avançada**.

["Saiba como criar volumes em um agregado específico"](#).

9 de fevereiro de 2022

Atualizações do mercado

- O pacote Essentials e Professional já estão disponíveis em todos os marketplaces de provedores de nuvem.

Esses métodos de cobrança por capacidade permitem que você pague por hora ou compre um contrato anual diretamente do seu provedor de nuvem. Você ainda tem a opção de comprar uma licença por capacidade diretamente da NetApp.

Se você já tiver uma assinatura em um mercado de nuvem, também estará automaticamente inscrito

nessas novas ofertas. Você pode escolher o carregamento por capacidade ao implantar um novo ambiente de trabalho do Cloud Volumes ONTAP.

Se você for um novo cliente, o BlueXP solicitará que você se inscreva quando você criar um novo ambiente de trabalho.

- O licenciamento por nó de todos os marketplaces de provedores de nuvem está obsoleto e não está mais disponível para novos assinantes. Isso inclui contratos anuais e assinaturas por hora (Explore, Standard e Premium).

Este método de carregamento ainda está disponível para clientes existentes que têm uma subscrição ativa.

["Saiba mais sobre as opções de licenciamento do Cloud Volumes ONTAP"](#).

6 de fevereiro de 2022

Troque licenças não atribuídas

Se você tiver uma licença não atribuída baseada em nó para o Cloud Volumes ONTAP que não tenha usado, agora poderá trocar a licença convertendo-a em uma licença do Cloud Backup, licença do Cloud Data Sense ou licença do Cloud Tiering.

Esta ação revoga a licença Cloud Volumes ONTAP e cria uma licença equivalente a dólar para o serviço com a mesma data de validade.

["Saiba como trocar licenças não atribuídas baseadas em nós"](#).

30 de janeiro de 2022

As seguintes alterações foram introduzidas com a versão 3.9.15 do conetor.

Seleção de licenciamento redesenhada

Redesenhamos a tela de seleção de licenciamento ao criar um novo ambiente de trabalho do Cloud Volumes ONTAP. As mudanças destacam os métodos de cobrança por capacidade introduzidos em julho de 2021 e oferecem suporte às próximas ofertas por meio dos marketplaces do provedor de nuvem.

Atualização da carteira digital

Atualizamos a **carteira digital** consolidando as licenças Cloud Volumes ONTAP em uma única guia.

2 de janeiro de 2022

As seguintes alterações foram introduzidas com a versão 3.9.14 do conetor.

Suporte para tipos adicionais de VM do Azure

O Cloud Volumes ONTAP agora é compatível com os seguintes tipos de VM no Microsoft Azure, começando com a versão 9.10.1:

- E4ds_v4
- E8ds_v4

- E32ds_v4
- E48ds_v4

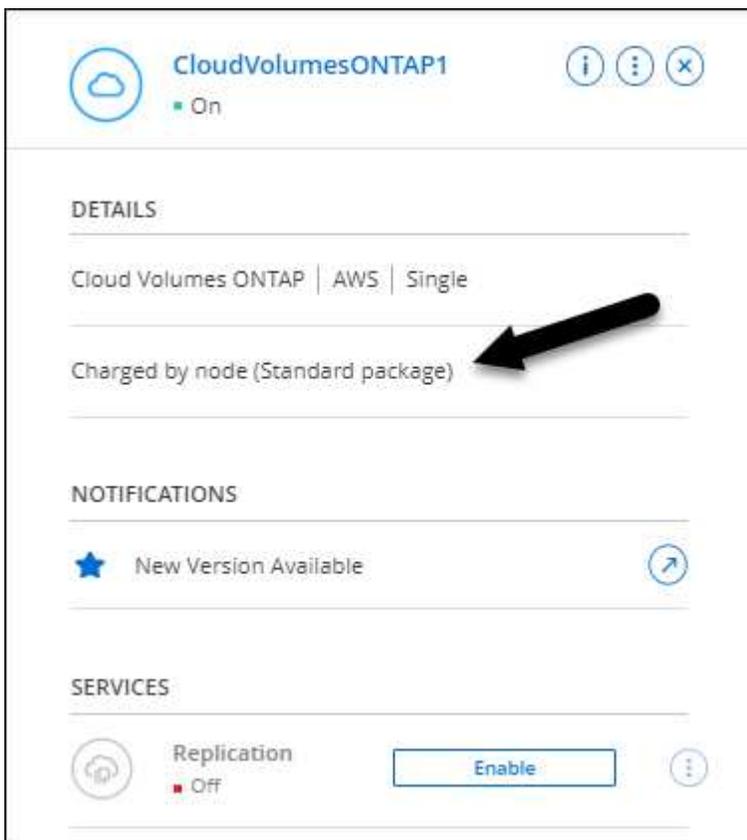
Aceda ao "[Notas de versão do Cloud Volumes ONTAP](#)" para obter mais detalhes sobre as configurações suportadas.

Atualização de carregamento do FlexClone

Se você usar um "[licença baseada em capacidade](#)" para Cloud Volumes ONTAP, não será mais cobrado pela capacidade usada pelo FlexClone volumes.

Método de carregamento agora apresentado

O BlueXP agora mostra o método de carregamento para cada ambiente de trabalho do Cloud Volumes ONTAP no painel direito da tela.



Escolha o seu nome de utilizador

Quando você cria um ambiente de trabalho do Cloud Volumes ONTAP, agora você tem a opção de inserir o nome de usuário preferido, em vez do nome de usuário padrão do administrador.

Credentials

User Name

Password

Confirm Password

Melhorias na criação de volume

Fizemos algumas melhorias na criação de volumes:

- Redesenhamos o assistente criar volume para facilitar o uso.
- Agora você pode escolher uma política de exportação personalizada para NFS.

1 Details, Protection & Tags 2 Protocol 3 Disk Type 4 Usage Profile & Tiering Policy 5 Review

Volumes Protocol

Select the volume's protocol: NFS Protocol CIFS Protocol iSCSI Protocol

Access Control

Custom export policy

Export Policy (1 rule defined)

[Manage volume's export policy](#)

28 de novembro de 2021

As seguintes alterações foram introduzidas com a versão 3.9.13 do conetor.

Cloud Volumes ONTAP 9.10.1

Agora, o BlueXP pode implantar e gerenciar o Cloud Volumes ONTAP 9.10.1.

["Saiba mais sobre os novos recursos incluídos nesta versão do Cloud Volumes ONTAP".](#)

Assinaturas do NetApp Keystone

Agora você pode usar as assinaturas do Keystone para pagar por pares de HA do Cloud Volumes ONTAP.

Uma subscrição do Keystone é um serviço baseado em subscrição com pagamento conforme o uso que oferece uma experiência de nuvem híbrida otimizada para quem prefere modelos de consumo de despesas operacionais para CapEx adiantado ou aluguel.

Uma assinatura do Keystone é compatível com todas as novas versões do Cloud Volumes ONTAP que você pode implantar na BlueXP .

- ["Saiba mais sobre as assinaturas do NetApp Keystone"](#).
- ["Saiba como começar a usar as assinaturas do Keystone no BlueXP "](#).

Novo suporte à região da AWS

O Cloud Volumes ONTAP agora é compatível com a região AWS Ásia-Pacífico (Osaka) (ap-nordeste-3).

Redução da porta

As portas 8023 e 49000 não estão mais abertas em sistemas Cloud Volumes ONTAP no Azure para sistemas de nó único e pares de HA.

Esta alteração aplica-se a *new* sistemas Cloud Volumes ONTAP começando com a versão 3.9.13 do conetor.

4 de outubro de 2021

As seguintes alterações foram introduzidas com a versão 3.9.11 do conetor.

Cloud Volumes ONTAP 9.10.0

Agora, o BlueXP pode implantar e gerenciar o Cloud Volumes ONTAP 9.10.0.

["Saiba mais sobre os novos recursos incluídos nesta versão do Cloud Volumes ONTAP"](#).

Tempo de implantação reduzido

Reduzimos o tempo necessário para implantar um ambiente de trabalho do Cloud Volumes ONTAP no Microsoft Azure ou no Google Cloud quando a velocidade de gravação normal está ativada. O tempo de implantação é agora 3-4 minutos mais curto, em média.

2 de setembro de 2021

As seguintes alterações foram introduzidas com a versão 3.9.10 do conetor.

Chave de criptografia gerenciada pelo cliente no Azure

Os dados são criptografados automaticamente no Cloud Volumes ONTAP no Azure usando ["Criptografia do Serviço de storage do Azure"](#) uma chave gerenciada pela Microsoft. Mas agora você pode usar sua própria chave de criptografia gerenciada pelo cliente, executando as seguintes etapas:

1. A partir do Azure, crie um cofre de chaves e, em seguida, gere uma chave nesse cofre.
2. No BlueXP , use a API para criar um ambiente de trabalho do Cloud Volumes ONTAP que use a chave.

["Saiba mais sobre estes passos"](#).

7 de julho de 2021

As seguintes alterações foram introduzidas com a versão 3.9.8 do conector.

Novos métodos de carregamento

Estão disponíveis novos métodos de carregamento para o Cloud Volumes ONTAP.

- **BYOL baseado em capacidade:** Uma licença baseada em capacidade permite que você pague por Cloud Volumes ONTAP por TIB de capacidade. A licença está associada à sua conta do NetApp e permite que você crie como vários sistemas Cloud Volumes ONTAP, contanto que a capacidade suficiente esteja disponível por meio de sua licença. O licenciamento baseado em capacidade está disponível na forma de um pacote, *Essentials* ou *Professional*.
- **Oferta de freemium:** O Freemium permite que você use todos os recursos do Cloud Volumes ONTAP gratuitamente da NetApp (taxas de provedor de nuvem ainda se aplicam). Você está limitado a 500 GiB de capacidade provisionada por sistema, e não há contrato de suporte. Você pode ter até 10 sistemas Freemium.

["Saiba mais sobre essas opções de licenciamento"](#).

Aqui está um exemplo dos métodos de carregamento que você pode escolher:

Cloud Volumes ONTAP Charging Methods

[Learn more about our charging methods](#)

 Pay-As-You-Go by the hour

 Bring your own license

Bring your own license type

Package

 Freemium (Up to 500GB)

Armazenamento WORM disponível para uso geral

O storage WORM (uma gravação, muitas leituras) não está mais no Preview e agora está disponível para uso geral com o Cloud Volumes ONTAP. ["Saiba mais sobre o armazenamento WORM"](#).

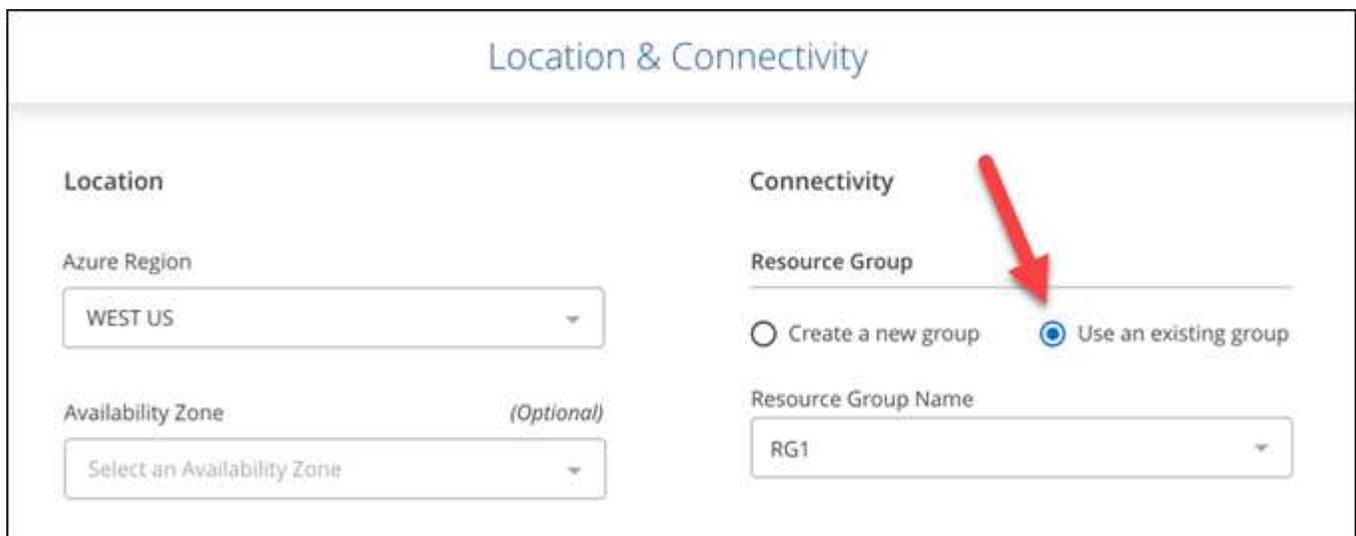
Suporte para m5dn.24xlarge na AWS

A partir da versão 9.9.1, o Cloud Volumes ONTAP agora suporta o tipo de instância m5dn.24xlarge com os seguintes métodos de carregamento: PAYGO Premium, bring Your own license (BYOL) e Freemium.

["Veja as configurações compatíveis do Cloud Volumes ONTAP na AWS"](#).

Selecione grupos de recursos existentes do Azure

Ao criar um sistema Cloud Volumes ONTAP no Azure, agora você tem a opção de selecionar um grupo de recursos existente para a VM e seus recursos associados.



The screenshot shows the 'Location & Connectivity' configuration page. On the left, under 'Location', 'Azure Region' is set to 'WEST US' and 'Availability Zone' is set to 'Select an Availability Zone (Optional)'. On the right, under 'Connectivity', 'Resource Group' is set to 'RG1'. The 'Use an existing group' radio button is selected, with a red arrow pointing to it.

As permissões a seguir permitem que o BlueXP remova recursos do Cloud Volumes ONTAP de um grupo de recursos, em caso de falha ou exclusão da implantação:

```
"Microsoft.Network/privateEndpoints/delete",  
"Microsoft.Compute/availabilitySets/delete",
```

Certifique-se de fornecer essas permissões a cada conjunto de credenciais do Azure que você adicionou ao BlueXP. ["Veja a política de conetores mais recente para o Azure"](#).

Blob acesso público agora desativado no Azure

Como um aprimoramento de segurança, o BlueXP agora desabilita **Acesso público Blob** ao criar uma conta de armazenamento para o Cloud Volumes ONTAP.

Aprimoramento do Azure Private Link

Por padrão, o BlueXP agora habilita uma conexão de link privado do Azure na conta de armazenamento de diagnósticos de inicialização para novos sistemas Cloud Volumes ONTAP.

Isso significa que as contas de armazenamento *all* do Cloud Volumes ONTAP agora usarão um link privado.

["Saiba mais sobre como usar um link privado do Azure com o Cloud Volumes ONTAP"](#).

Discos persistentes balanceados no Google Cloud

A partir da versão 9.9.1, o Cloud Volumes ONTAP agora oferece suporte a discos persistentes balanceados (pd-Balanced).

Esses SSDs equilibram performance e custo fornecendo IOPS mais baixo por GiB.

Custom-4-16384 não é mais compatível com o Google Cloud

O tipo de máquina personalizado-4-16384 não é mais suportado com novos sistemas Cloud Volumes ONTAP.

Se tiver um sistema existente a funcionar neste tipo de máquina, pode continuar a utilizá-lo, mas recomendamos que mude para o tipo de máquina n2-standard-4.

["Veja as configurações compatíveis com o Cloud Volumes ONTAP no GCP"](#).

30 de maio de 2021

As seguintes alterações foram introduzidas com a versão 3.9.7 do conector.

Novo pacote profissional na AWS

Um novo pacote profissional permite que você agrupe o Cloud Volumes ONTAP e o Cloud Backup Service usando um contrato anual do AWS Marketplace. O pagamento é por TIB. Essa assinatura não permite fazer backup dos dados no local.

Se você escolher essa opção de pagamento, poderá provisionar até 2 PIB por sistema Cloud Volumes ONTAP por meio de discos EBS e disposição em camadas em storage de objetos S3 (nó único ou HA).

Aceda ao ["Página do AWS Marketplace"](#) para ver os detalhes de preços e aceda ao ["Notas de versão do Cloud Volumes ONTAP"](#) para saber mais sobre esta opção de licenciamento.

Tags em volumes do EBS na AWS

O BlueXP agora adiciona tags aos volumes do EBS quando cria um novo ambiente de trabalho do Cloud Volumes ONTAP. As tags foram criadas anteriormente após a implantação do Cloud Volumes ONTAP.

Esta alteração pode ajudar se a sua organização utilizar políticas de controlo de serviço (SCPs) para gerir permissões.

Período mínimo de resfriamento para política de disposição automática em categorias

Se você ativou a disposição de dados em categorias em um volume usando a política de disposição em camadas *auto*, agora é possível ajustar o período mínimo de resfriamento usando a API.

["Saiba como ajustar o período mínimo de arrefecimento."](#)

Aprimoramento para políticas de exportação personalizadas

Quando você cria um novo volume NFS, o BlueXP agora exibe políticas de exportação personalizadas em ordem crescente, facilitando a localização da política de exportação de que você precisa.

Exclusão de snapshots antigos da nuvem

O BlueXP agora exclui snapshots de nuvem mais antigos de discos raiz e de inicialização que são criados quando um sistema Cloud Volumes ONTAP é implantado e sempre que ele é desligado. Apenas os dois snapshots mais recentes são retidos para os volumes raiz e de inicialização.

Esse aprimoramento ajuda a reduzir os custos do fornecedor de nuvem removendo snapshots que não são mais necessários.

Observe que um conector requer uma nova permissão para excluir snapshots do Azure. ["Veja a política de conectores mais recente para o Azure"](#).

```
"Microsoft.Compute/snapshots/delete"
```

24 de maio de 2021

Cloud Volumes ONTAP 9.9.1

Agora, o BlueXP pode implantar e gerenciar o Cloud Volumes ONTAP 9,9.1.

["Saiba mais sobre os novos recursos incluídos nesta versão do Cloud Volumes ONTAP"](#).

11 Abr 2021

As seguintes alterações foram introduzidas com a versão 3.9.5 do conector.

Relatórios de espaço lógico

O BlueXP agora permite a geração de relatórios de espaço lógico na VM de storage inicial criada para o Cloud Volumes ONTAP.

Quando o espaço é relatado logicamente, o ONTAP relata o espaço de volume de modo que todo o espaço físico salvo pelos recursos de eficiência de storage também seja reportado como usado.

Suporte para GP3 discos na AWS

O Cloud Volumes ONTAP agora oferece suporte a discos *SSD de uso geral (GP3)*, começando com a versão 9,7.GP3. Os discos são os SSDs de menor custo que equilibram custo e desempenho para uma ampla variedade de cargas de trabalho.

["Saiba mais sobre como usar discos GP3 com o Cloud Volumes ONTAP"](#).

Discos rígidos frios não são mais compatíveis com a AWS

O Cloud Volumes ONTAP não suporta mais discos rígidos frios (SC1).

TLS 1,2 para contas de armazenamento do Azure

Quando o BlueXP cria contas de armazenamento no Azure para Cloud Volumes ONTAP, a versão TLS para a conta de armazenamento agora é a versão 1,2.

8 de março de 2021

As seguintes alterações foram introduzidas com a versão 3.9.4 do conector.

Cloud Volumes ONTAP 9.9.0

Agora, o BlueXP pode implantar e gerenciar o Cloud Volumes ONTAP 9,9.0.

["Saiba mais sobre os novos recursos incluídos nesta versão do Cloud Volumes ONTAP"](#).

Suporte para o ambiente AWS C2S

Agora você pode implantar o Cloud Volumes ONTAP 9,8 no ambiente de Serviços de nuvem comerciais da AWS (C2S).

["Saiba como começar em C2S"](#).

Criptografia AWS com CMKs gerenciados pelo cliente

O BlueXP sempre permitiu que você criptografasse dados do Cloud Volumes ONTAP usando o AWS Key Management Service (KMS). A partir do Cloud Volumes ONTAP 9,9.0, os dados em discos EBS e dados dispostos em camadas em S3 são criptografados se você selecionar um CMK gerenciado pelo cliente. Anteriormente, apenas os dados do EBS seriam criptografados.

Observe que você precisará fornecer à função Cloud Volumes ONTAP IAM acesso para usar o CMK.

["Saiba mais sobre como configurar o AWS KMS com o Cloud Volumes ONTAP"](#).

Suporte para Azure DoD

Agora você pode implantar o Cloud Volumes ONTAP 9,8 no nível de impacto do Departamento de Defesa do Azure (DoD) 6 (IL6).

Redução de endereço IP no Google Cloud

Reduzimos o número de endereços IP necessários para o Cloud Volumes ONTAP 9,8 e posterior no Google Cloud. Por padrão, um endereço IP a menos é necessário (nós unificamos o LIF entre clusters com o LIF de gerenciamento de nós). Você também tem a opção de ignorar a criação do LIF de gerenciamento de SVM ao usar a API, o que reduziria a necessidade de um endereço IP adicional.

["Saiba mais sobre os requisitos de endereço IP no Google Cloud"](#).

Aceita VPC compartilhada no Google Cloud

Ao implantar um par de HA do Cloud Volumes ONTAP no Google Cloud, você pode escolher VPCs compartilhados para VPC-1, VPC-2 e VPC-3. Anteriormente, apenas a VPC-0 poderia ser uma VPC compartilhada. Esta alteração é suportada com o Cloud Volumes ONTAP 9,8 e posterior.

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

4 Jan 2021

As seguintes alterações foram introduzidas com a versão 3.9.2 do conector.

AWS Outposts

Há alguns meses, anunciamos que a Cloud Volumes ONTAP alcançou a designação de Outposts Ready da Amazon Web Services (AWS). Hoje, temos o prazer de anunciar que validamos o BlueXP e o Cloud Volumes ONTAP com o AWS Outposts.

Se você tiver um AWS Outpost, você poderá implantar o Cloud Volumes ONTAP nesse Outpost selecionando a VPC Outpost no assistente ambiente de trabalho. A experiência é a mesma que qualquer outra VPC que reside na AWS. Observe que você precisará primeiro implantar um conector no AWS Outpost.

Existem algumas limitações a apontar:

- No momento, apenas sistemas Cloud Volumes ONTAP de nó único são compatíveis
- As instâncias EC2 que você pode usar com o Cloud Volumes ONTAP estão limitadas ao que está disponível em seu Outpost
- Somente SSDs de uso geral (GP2) são suportados no momento

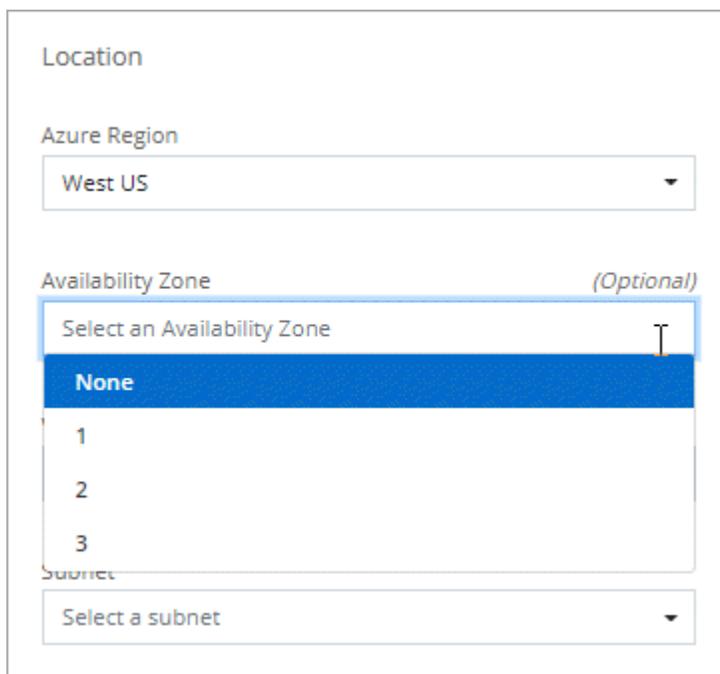
VNVRAM Ultra SSD em regiões Azure suportadas

Agora, o Cloud Volumes ONTAP pode usar um SSD Ultra como VNVRAM quando você usa o tipo de VM E32s_v3 com um sistema de nó único "[Em qualquer região do Azure suportada](#)".

A VNVRAM proporciona um melhor desempenho de gravação.

Escolha uma zona de disponibilidade no Azure

Agora você pode escolher a zona de disponibilidade na qual deseja implantar um sistema Cloud Volumes ONTAP de nó único. Se você não selecionar uma AZ, o BlueXP selecionará uma para você.



The screenshot shows a configuration form for an Azure resource. Under the 'Location' section, the 'Azure Region' dropdown menu is open, showing 'West US' as the selected option. Below it, the 'Availability Zone' dropdown menu is also open, showing 'None' as the selected option. A list of options '1', '2', and '3' is visible below the 'None' option. The 'Subnet' dropdown menu is set to 'Select a subnet'.

Discos maiores no Google Cloud

O Cloud Volumes ONTAP agora oferece suporte a discos de 64 TB no GCP.



A capacidade máxima do sistema somente com discos permanece em 256 TB devido aos limites do GCP.

Novos tipos de máquina no Google Cloud

O Cloud Volumes ONTAP agora suporta os seguintes tipos de máquina:

- N2-standard-4 com a licença Explore e com BYOL
- N2-standard-8 com a licença Standard e com BYOL
- N2-standard-32 com a licença Premium e com BYOL

3 Nov 2020

As seguintes alterações foram introduzidas com a versão 3.9.0 do conector.

Link privado do Azure para Cloud Volumes ONTAP

Por padrão, o BlueXP agora habilita uma conexão do Azure Private Link entre o Cloud Volumes ONTAP e suas contas de armazenamento associadas. Um link privado protege conexões entre endpoints no Azure.

- ["Saiba mais sobre os links privados do Azure"](#)
- ["Saiba mais sobre como usar um link privado do Azure com o Cloud Volumes ONTAP"](#)

Limitações conhecidas

As limitações conhecidas identificam plataformas, dispositivos ou funções que não são suportadas por esta versão do produto ou que não interoperam corretamente com ele. Revise essas limitações com cuidado.

Essas limitações são específicas para o gerenciamento de Cloud Volumes ONTAP no BlueXP. Para visualizar limitações com o próprio software Cloud Volumes ONTAP, ["Vá para as Notas de versão do Cloud Volumes ONTAP"](#)

O BlueXP não oferece suporte à criação de volumes do FlexGroup

Embora o Cloud Volumes ONTAP ofereça suporte ao FlexGroup volumes, o BlueXP não oferece suporte à criação de volumes do FlexGroup no momento. Se você criar um volume do FlexGroup a partir do Gerenciador de sistemas do ONTAP ou da CLI do ONTAP, defina o modo de gerenciamento de capacidade do BlueXP como Manual. O modo automático pode não funcionar corretamente com volumes FlexGroup.



A capacidade de criar volumes do FlexGroup no BlueXP está planejada para um lançamento futuro.

BlueXP não suporta S3 com Cloud Volumes ONTAP

Embora o Cloud Volumes ONTAP ofereça suporte ao S3 como opção para storage com escalabilidade horizontal, o BlueXP não oferece recursos de gerenciamento para esse recurso. Usar a CLI é a melhor prática para configurar o acesso de cliente S3 a partir do Cloud Volumes ONTAP. Para obter mais informações, consulte ["S3 Guia de Energia de Configuração"](#).

["Saiba mais sobre o suporte do Cloud Volumes ONTAP para S3 e outros protocolos de cliente"](#).

O BlueXP não oferece suporte à recuperação de desastres para VMs de storage

O BlueXP não oferece qualquer configuração ou suporte de orquestração para recuperação de desastres de VM de storage (SVM). Use o Gerenciador de sistemas do ONTAP ou a CLI do ONTAP.

["Saiba mais sobre a recuperação de desastres do SVM"](#).

Notas de versão do Cloud Volumes ONTAP

As Notas de versão para Cloud Volumes ONTAP fornecem informações específicas para a versão. Novidades na versão, configurações suportadas, limites de armazenamento e quaisquer limitações ou problemas conhecidos que possam afetar a funcionalidade do produto.

["Vá para as Notas de versão do Cloud Volumes ONTAP"](#)

Comece agora

Saiba mais sobre o Cloud Volumes ONTAP

Com o Cloud Volumes ONTAP, você otimiza seus custos e performance de storage de nuvem, além de aprimorar a proteção, a segurança e a conformidade dos dados.

O Cloud Volumes ONTAP é um dispositivo de storage somente de software que executa o software de gerenciamento de dados ONTAP na nuvem. Ele fornece storage de nível empresarial com os seguintes principais recursos:

- Eficiência de storage

Utilize deduplicação de dados incorporada, compressão, thin Provisioning e clonagem para minimizar os custos de storage.

- Alta disponibilidade

Garanta a confiabilidade empresarial e as operações contínuas em caso de falhas em seu ambiente de nuvem.

- Proteção de dados

A Cloud Volumes ONTAP utiliza o SnapMirror, a tecnologia de replicação líder do setor da NetApp para replicar dados no local para a nuvem de modo que seja fácil ter cópias secundárias disponíveis para vários casos de uso.

O Cloud Volumes ONTAP também se integra ao backup e recuperação do BlueXP para oferecer recursos de backup e restauração para proteção e arquivamento a longo prazo de seus dados de nuvem.

["Saiba mais sobre backup e recuperação do BlueXP "](#)

- Categorização de dados

Alterne entre pools de armazenamento de alto e baixo desempenho sob demanda sem colocar os aplicativos offline.

- Consistência de aplicativos

Garanta a consistência das cópias Snapshot do NetApp usando o NetApp SnapCenter.

["Saiba mais sobre o SnapCenter"](#)

- Segurança dos dados

O Cloud Volumes ONTAP é compatível com a criptografia de dados e oferece proteção contra vírus e ransomware.

- Controles de conformidade de privacidade

A integração com a classificação BlueXP ajuda você a entender o contexto dos dados e identificar dados confidenciais.

["Saiba mais sobre a classificação BlueXP"](#)



As licenças para os recursos do ONTAP estão incluídas no Cloud Volumes ONTAP.

["Veja as configurações do Cloud Volumes ONTAP compatíveis"](#)

["Saiba mais sobre o Cloud Volumes ONTAP"](#)

Versões ONTAP compatíveis para novas implantações

O BlueXP permite que você escolha entre várias versões diferentes do ONTAP ao criar um novo ambiente de trabalho do Cloud Volumes ONTAP.

Versões do Cloud Volumes ONTAP diferentes das listadas aqui não estão disponíveis para novas implantações. Para obter informações sobre a atualização, ["Caminhos de atualização suportados"](#) consulte .

AWS

Nó único

- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8
- 9,7 P5
- 9,5 P6

Par de HA

- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1

- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8
- 9,7 P5
- 9,5 P6

Azure

Nó único

- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9,8 P10
- 9,7 P6
- 9,5 P6

Par de HA

- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8

- 9.9.1 P7
- 9,8 P10
- 9,7 P6

Google Cloud

Nó único

- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8
- 9,7 P5

Par de HA

- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8

Comece a usar o Amazon Web Services

Início rápido do Cloud Volumes ONTAP na AWS

Comece a usar o Cloud Volumes ONTAP na AWS em alguns passos.

1

Crie um conetor

Se você ainda não tem um "Conetor", você precisa criar um. ["Saiba como criar um conetor na AWS"](#)

Observe que, se você quiser implantar o Cloud Volumes ONTAP em uma sub-rede onde não há acesso à Internet disponível, precisará instalar manualmente o conetor e acessar a interface de usuário do BlueXP que está sendo executada nesse conetor. ["Saiba como instalar manualmente o conetor em um local sem acesso à Internet"](#)

2

Planeje sua configuração

O BlueXP oferece pacotes pré-configurados que atendem aos requisitos de carga de trabalho ou você pode criar sua própria configuração. Se você escolher sua própria configuração, você deve entender as opções disponíveis para você. ["Saiba mais"](#).

3

Configure a rede

1. Certifique-se de que a VPC e as sub-redes suportem a conectividade entre o conetor e o Cloud Volumes ONTAP.
2. Ative o acesso de saída à Internet a partir da VPC de destino para NetApp AutoSupport.

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

3. Configure um endpoint de VPC para o serviço S3.

Um endpoint de VPC é necessário se você quiser categorizar dados inativos do Cloud Volumes ONTAP para storage de objetos de baixo custo.

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

4

Configure o AWS KMS

Se você quiser usar a criptografia do Amazon com o Cloud Volumes ONTAP, você precisa garantir que existe uma chave mestra do cliente (CMK) ativa. Você também precisa modificar a política de chave para cada CMK adicionando a função do IAM que fornece permissões ao conetor como um *usuário de chave*. ["Saiba mais"](#).

5

Inicie o Cloud Volumes ONTAP usando o BlueXP

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

Links relacionados

- ["Crie um conetor na AWS a partir do BlueXP "](#)

- ["Crie um conector no AWS Marketplace"](#)
- ["Instale e configure um conector no local"](#)
- ["Permissões da AWS para o conector"](#)

Planeje sua configuração do Cloud Volumes ONTAP na AWS

Ao implantar o Cloud Volumes ONTAP na AWS, você pode escolher um sistema pré-configurado que corresponda aos requisitos de workload ou criar sua própria configuração. Se você escolher sua própria configuração, você deve entender as opções disponíveis para você.

Escolha uma licença 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 para o Cloud Volumes ONTAP"](#)
- ["Saiba como configurar o licenciamento"](#)

Escolha uma região suportada

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

As regiões mais recentes da AWS devem estar habilitadas para que você possa criar e gerenciar recursos nessas regiões. ["Saiba como habilitar uma região"](#).

Escolha uma zona local suportada

Selecionar uma zona local é opcional. O Cloud Volumes ONTAP é compatível com algumas zonas locais da AWS, incluindo Singapura. O Cloud Volumes ONTAP na AWS suporta apenas o modo de alta disponibilidade (HA) em uma única zona de disponibilidade. Implantações de nó único não são compatíveis.



O Cloud Volumes ONTAP não é compatível com categorização de dados e disposição em camadas na nuvem nas zonas locais da AWS. Além disso, as zonas locais com instâncias que não foram qualificadas para Cloud Volumes ONTAP não são suportadas. Um exemplo disso é Miami, que não está disponível como uma zona local, porque tem apenas Gen6 instâncias que são não suportadas e não qualificadas.

["Veja a lista completa de zonas locais"](#). As zonas locais têm de estar ativadas antes de poder criar e gerir recursos nessas zonas.

["Saiba como ativar uma zona local"](#).

Escolha uma instância suportada

O Cloud Volumes ONTAP suporta vários tipos de instância, dependendo do tipo de licença escolhido.

["Configurações compatíveis com o Cloud Volumes ONTAP na AWS"](#)

Entenda os limites de armazenamento

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

["Limites de storage para Cloud Volumes ONTAP na AWS"](#)

Dimensione seu sistema na AWS

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

Tipo de instância

- Faça a correspondência dos requisitos de workload com a taxa de transferência máxima e IOPS para cada tipo de instância do EC2.
- Se vários usuários gravarem no sistema ao mesmo tempo, escolha um tipo de instância que tenha CPUs suficientes para gerenciar as solicitações.
- Se você tem um aplicativo que é principalmente lido, então escolha um sistema com RAM suficiente.
 - ["Documentação da AWS: Tipos de instância do Amazon EC2"](#)
 - ["Documentação da AWS: Instâncias otimizadas do Amazon EBS"](#)

Tipo de disco EBS

A um nível elevado, as diferenças entre os tipos de discos EBS são as seguintes. Para saber mais sobre os casos de uso de discos EBS, ["Documentação da AWS: Tipos de volume do EBS"](#) consulte .

- *Discos SSD de uso geral (GP3)* são os SSDs de menor custo que equilibram custo e desempenho para uma ampla variedade de cargas de trabalho. O desempenho é definido em termos de IOPS e taxa de transferência. Os discos de GP3 tb são compatíveis com o Cloud Volumes ONTAP 9,7 e posterior.

Quando você seleciona um disco de GP3 tb, o BlueXP preenche os valores de IOPS e taxa de transferência padrão que fornecem desempenho equivalente a um disco de GP2 tb com base no tamanho de disco selecionado. Você pode aumentar os valores para obter um melhor desempenho a um custo mais alto, mas não apoiamos valores mais baixos porque pode resultar em desempenho inferior. Em suma, mantenha os valores padrão ou aumente-os. Não os abaixe. ["Saiba mais sobre discos GP3 e seu desempenho"](#).

Observe que o Cloud Volumes ONTAP suporta o recurso volumes elásticos do Amazon EBS com discos GP3. ["Saiba mais sobre o suporte ao Elastic volumes"](#).

- *Discos SSD de uso geral (GP2)* equilibram custo e desempenho para uma ampla variedade de cargas de trabalho. A performance é definida em termos de IOPS.
- *Os discos SSD IOPS provisionados (IO1)* são para aplicativos críticos que exigem o mais alto desempenho a um custo mais alto.

Observe que o Cloud Volumes ONTAP suporta o recurso volumes elásticos do Amazon EBS com discos IO1. ["Saiba mais sobre o suporte ao Elastic volumes"](#).

- *Discos HDD otimizado para throughput (st1)* são para cargas de trabalho acessadas com frequência que exigem taxa de transferência rápida e consistente a um preço menor.



A disposição de dados em categorias para o AWS S3 não está disponível nas zonas locais da AWS devido à falta de conectividade.

Tamanho do disco EBS

Se você escolher uma configuração que não suporte o ["Recurso de volumes elásticos do Amazon EBS"](#), precisará escolher um tamanho de disco inicial ao iniciar um sistema Cloud Volumes ONTAP. Depois disso, você pode ["Deixe o BlueXP gerenciar a capacidade de um sistema para você"](#), mas se quiser ["crie agregados você mesmo"](#), estar ciente do seguinte:

- Todos os discos em um agregado devem ter o mesmo tamanho.
- O desempenho dos discos EBS está ligado ao tamanho do disco. O tamanho determina o IOPS de linha de base e a duração máxima de intermitência para discos SSD e a taxa de transferência de linha de base e de intermitência para discos HDD.
- Em última análise, você deve escolher o tamanho do disco que lhe dá o *desempenho sustentado* que você precisa.
- Mesmo que você escolha discos maiores (por exemplo, seis discos TIB de 4 TB), talvez você não tenha todos os IOPS porque a instância do EC2 pode atingir seu limite de largura de banda.

Para obter mais detalhes sobre o desempenho do disco EBS, ["Documentação da AWS: Tipos de volume do EBS"](#) consulte .

Como observado acima, a escolha de um tamanho de disco não é suportada com configurações do Cloud Volumes ONTAP que suportam o recurso volumes elásticos do Amazon EBS. ["Saiba mais sobre o suporte ao Elastic volumes"](#).

Exibir discos do sistema padrão

Além do storage para dados de usuário, a BlueXP também compra storage de nuvem para dados de sistema do Cloud Volumes ONTAP (dados de inicialização, dados de raiz, dados básicos e NVRAM). Para fins de Planejamento, pode ajudar você a analisar esses detalhes antes de implantar o Cloud Volumes ONTAP.

["Exibir os discos padrão para os dados do sistema Cloud Volumes ONTAP na AWS"](#).



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

Prepare-se para implantar o Cloud Volumes ONTAP em um AWS Outpost

Se você tiver um AWS Outpost, você poderá implantar o Cloud Volumes ONTAP nesse Outpost selecionando a VPC Outpost no assistente ambiente de trabalho. A experiência é a mesma que qualquer outra VPC que reside na AWS. Observe que você precisará primeiro implantar um conector no AWS Outpost.

Existem algumas limitações a apontar:

- No momento, apenas sistemas Cloud Volumes ONTAP de nó único são compatíveis
- As instâncias EC2 que você pode usar com o Cloud Volumes ONTAP estão limitadas ao que está disponível em seu Outpost
- Somente SSDs de uso geral (GP2) são suportados no momento

Colete informações de rede

Ao iniciar o Cloud Volumes ONTAP na AWS, você precisa especificar detalhes sobre sua rede VPC. Você pode usar uma Planilha para coletar as informações do administrador.

Nó único ou par de HA em uma única AZ

Informações da AWS	O seu valor
Região	
VPC	
Sub-rede	
Grupo de segurança (se estiver usando o seu próprio)	

Par HA em várias AZs

Informações da AWS	O seu valor
Região	
VPC	
Grupo de segurança (se estiver usando o seu próprio)	
Zona de disponibilidade do nó 1	
Sub-rede do nó 1	
Zona de disponibilidade do nó 2	
Sub-rede do nó 2	
Zona de disponibilidade do mediador	
Sub-rede do mediador	
Par de chaves para o mediador	
Endereço IP flutuante para porta de gerenciamento de cluster	
Endereço IP flutuante para dados no nó 1	
Endereço IP flutuante para dados no nó 2	
Tabelas de rota para endereços IP flutuantes	

Escolha uma velocidade de gravação

O BlueXP 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 e os riscos e recomendações ao usar alta velocidade de gravação. ["Saiba mais sobre a velocidade de escrita"](#).

Escolha um perfil de uso de volume

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

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

Thin Provisioning

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

Deduplicação

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

Compactação

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

Configure a rede

Requisitos de rede para o Cloud Volumes ONTAP na AWS

O BlueXP lida com a configuração de componentes de rede para Cloud Volumes ONTAP, como endereços IP, máscaras de rede e rotas. Você precisa se certificar de que o acesso de saída à Internet está disponível, que endereços IP privados suficientes estão disponíveis, que as conexões certas estão em vigor e muito mais.

Requisitos gerais

Os requisitos a seguir devem ser atendidos na AWS.

Acesso de saída à Internet para nós Cloud Volumes ONTAP

Os nós do Cloud Volumes ONTAP requerem acesso de saída à Internet para contactar os seguintes pontos finais para operações diárias.

Pontos de extremidade Cloud Volumes ONTAP

O Cloud Volumes ONTAP requer acesso de saída à Internet para contactar vários endpoints para operações diárias.

Os seguintes endpoints são específicos do Cloud Volumes ONTAP. O conetor também entra em Contato com vários endpoints para operações diárias, bem como com o console baseado na Web do BlueXP . ["Veja os pontos finais contactados a partir do conetor"](#)Consulte e ["Prepare a rede para usar o console BlueXP "](#).

Endpoints	Aplicável para	Finalidade	Modos de implantação do BlueXP	Impacto se o endpoint não estiver disponível
https://NetApp-cloud-account.auth0.com	Autenticação	Usado para autenticação BlueXP .	Modos padrão e restritos.	A autenticação do usuário falha e os seguintes serviços permanecem indisponíveis: <ul style="list-style-type: none"> • Serviços da Cloud Volumes ONTAP • Serviços da ONTAP • Protocolos e serviços proxy
https://keyvault-production-aks.vault.azure.net	Cofre de chaves	Usado para recuperar a chave secreta do cliente do Azure Key Vault para se comunicar com buckets do S3 para manipulação de metadados. O serviço Cloud Volumes ONTAP usa esse componente internamente.	Modos padrão, restrito e privado.	Os serviços Cloud Volumes ONTAP não estão disponíveis.
https://cloudmanager.cloud.NetApp.com/locação	Alocação	Usado para recuperar os recursos do Cloud Volumes ONTAP da BlueXP Locancy para autorizar recursos e usuários.	Modos padrão e restritos.	Os recursos do Cloud Volumes ONTAP e os usuários não estão autorizados.
https://support.NetApp.com/aods/asupmessage https://support.NetApp.com/asupprod/post/1,0/postAsup	AutoSupport	Usado para enviar dados de telemetria do AutoSupport para o suporte do NetApp.	Modos padrão e restritos.	As informações do AutoSupport permanecem não entregues.

Endpoints	Aplicável para	Finalidade	Modos de implantação do BlueXP	Impacto se o endpoint não estiver disponível
O endpoint comercial exato para o serviço AWS (sufixo com <code>amazonaws.com</code>) depende da região da AWS que você está usando. Consulte a "Documentação da AWS para obter detalhes" .	<ul style="list-style-type: none"> • CloudFormation • Nuvem de computação elástica (EC2) • Gerenciamento de identidade e acesso (IAM) • Key Management Service (KMS) • Serviço de token de segurança (STS) • Serviço de armazenamento simples (S3) 	Comunicação com os serviços da AWS.	Modos padrão e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço AWS para executar operações específicas do BlueXP na AWS.
O ponto de extremidade do governo exato para o serviço AWS depende da região da AWS que você está usando. Os endpoints são sufixos com <code>amazonaws.com</code> e <code>c2s.ic.gov</code> . "AWS SDK" Consulte e "Documentação da Amazon" para obter mais informações.	<ul style="list-style-type: none"> • CloudFormation • Nuvem de computação elástica (EC2) • Gerenciamento de identidade e acesso (IAM) • Key Management Service (KMS) • Serviço de token de segurança (STS) • Serviço de armazenamento simples (S3) 	Comunicação com os serviços da AWS.	Modo restrito.	O Cloud Volumes ONTAP não pode se comunicar com o serviço AWS para executar operações específicas do BlueXP na AWS.

Acesso de saída à Internet para NetApp AutoSupport

Os nós de Cloud Volumes ONTAP requerem acesso de saída à Internet para acessar endpoints externos para várias funções. O Cloud Volumes ONTAP não pode funcionar corretamente se esses endpoints forem bloqueados em ambientes com requisitos rígidos de segurança.

Os nós do Cloud Volumes ONTAP exigem acesso de saída à Internet para NetApp AutoSupport, que monitora proativamente a integridade do sistema e envia mensagens para o suporte técnico da NetApp.

As políticas de roteamento e firewall devem permitir o tráfego HTTP/HTTPS para os seguintes endpoints para

que o Cloud Volumes ONTAP possa enviar mensagens AutoSupport:

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

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

Se uma conexão de saída à Internet não estiver disponível para enviar mensagens AutoSupport, o BlueXP configura automaticamente seus sistemas Cloud Volumes ONTAP para usar o conector como um servidor proxy. O único requisito é garantir que o grupo de segurança do conector permita conexões *inbound* pela porta 3128. Você precisará abrir essa porta depois de implantar o conector.

Se você definiu regras de saída rígidas para o Cloud Volumes ONTAP, também precisará garantir que o grupo de segurança do Cloud Volumes ONTAP permita conexões *de saída* pela porta 3128.

Depois de verificar que o acesso de saída à Internet está disponível, você pode testar o AutoSupport para garantir que ele possa enviar mensagens. Para obter instruções, "[ONTAP docs: Configurar o AutoSupport](#)" consulte .

Se o BlueXP notificar que as mensagens do AutoSupport não podem ser enviadas, "[Solucionar problemas da configuração do AutoSupport](#)".

Acesso de saída à Internet para o mediador HA

A instância de mediador de HA precisa ter uma conexão de saída para o serviço AWS EC2 para que a TI possa ajudar no failover de storage. Para fornecer a conexão, você pode adicionar um endereço IP público, especificar um servidor proxy ou usar uma opção manual.

A opção manual pode ser um gateway NAT ou um endpoint de VPC de interface da sub-rede de destino para o serviço AWS EC2. Para obter detalhes sobre endpoints da VPC, consulte o "[Documentação da AWS: Endpoints da interface VPC \(AWS PrivateLink\)](#)".

Endereços IP privados

O BlueXP atribui automaticamente o número necessário de endereços IP privados ao Cloud Volumes ONTAP. Você precisa garantir que sua rede tenha endereços IP privados suficientes disponíveis.

O número de LIFs alocadas pelo BlueXP para Cloud Volumes ONTAP depende da implantação de um único sistema de nós ou de um par de HA. Um LIF é um endereço IP associado a uma porta física.

Endereços IP para um sistema de nó único

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

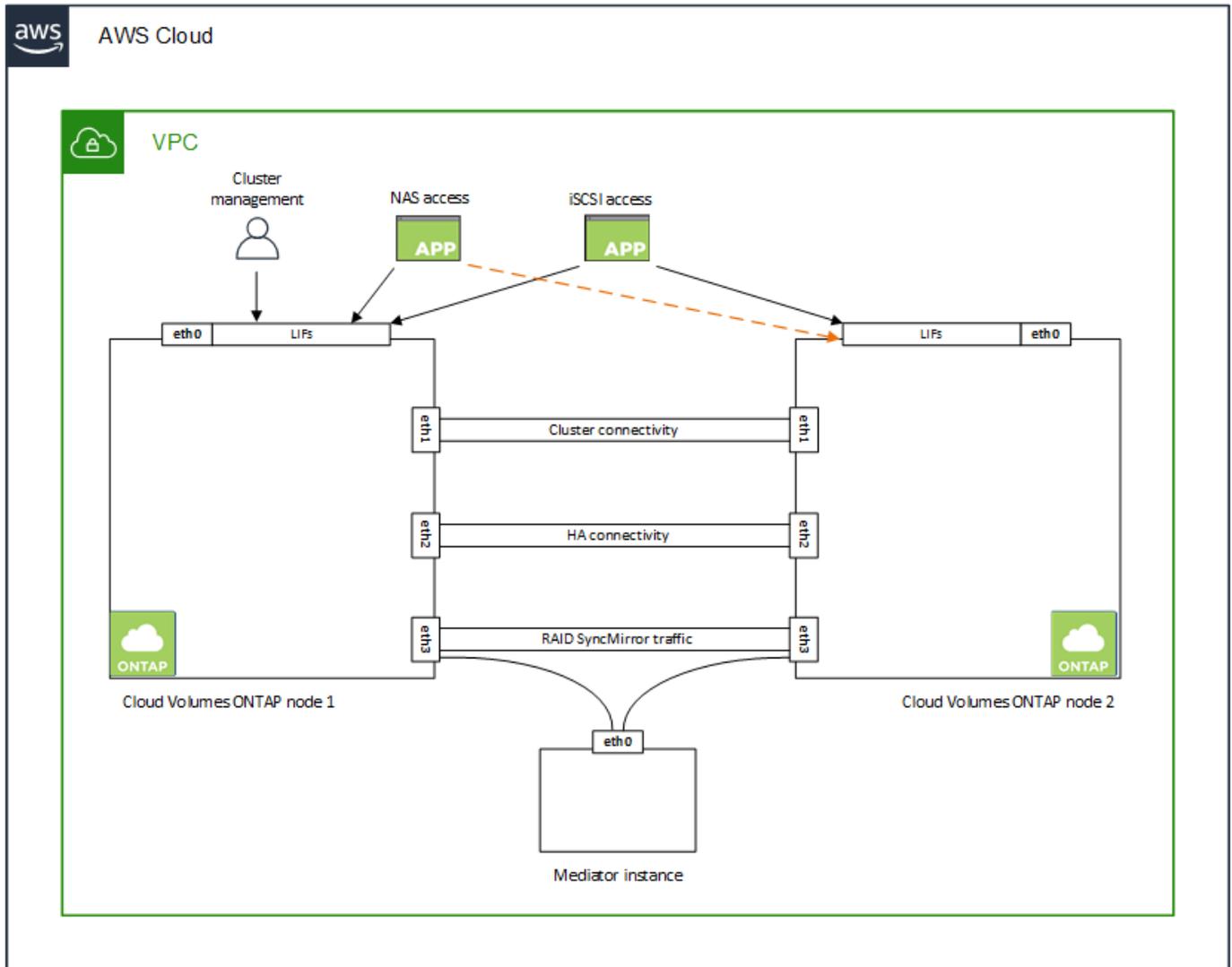
A tabela a seguir fornece detalhes sobre os LIFs associados a cada endereço IP privado.

LIF	Finalidade
Gerenciamento de clusters	Gerenciamento administrativo de todo o cluster (par de HA).
Gerenciamento de nós	Gerenciamento administrativo de um nó.
Entre clusters	Comunicação, backup e replicação entre clusters.
Dados nas	Acesso de cliente através de protocolos nas.

LIF	Finalidade
Dados iSCSI	Acesso de cliente através do protocolo iSCSI. Também usado pelo sistema para outros fluxos de trabalho de rede importantes. Este LIF é necessário e não deve ser eliminado.
Gerenciamento de VM de storage	Um LIF de gerenciamento de VM de storage é usado com ferramentas de gerenciamento como o SnapCenter.

Endereços IP para pares de HA

Os pares DE HA exigem mais endereços IP do que um sistema de nó único. Esses endereços IP estão espalhados por diferentes interfaces ethernet, como mostrado na imagem a seguir:



O número de endereços IP privados necessários para um par de HA depende do modelo de implantação escolhido. Um par de HA implantado em uma zona de disponibilidade (AZ) *single* da AWS requer 15 endereços IP privados, enquanto um par de HA implantado em *multiple* AZs requer 13 endereços IP privados.

As tabelas a seguir fornecem detalhes sobre os LIFs associados a cada endereço IP privado.

LIFs para pares de HA em uma única AZ

LIF	Interface	Nó	Finalidade
Gerenciamento de clusters	eth0	nó 1	Gerenciamento administrativo de todo o cluster (par de HA).
Gerenciamento de nós	eth0	nó 1 e nó 2	Gerenciamento administrativo de um nó.
Entre clusters	eth0	nó 1 e nó 2	Comunicação, backup e replicação entre clusters.
Dados nas	eth0	nó 1	Acesso de cliente através de protocolos nas.
Dados iSCSI	eth0	nó 1 e nó 2	Acesso de cliente através do protocolo iSCSI. Também usado pelo sistema para outros fluxos de trabalho de rede importantes. Estes LIFs são necessários e não devem ser excluídos.
Conectividade de cluster	eth1	nó 1 e nó 2	Permite que os nós se comuniquem entre si e movam dados dentro do cluster.
Conectividade HA	eth2	nó 1 e nó 2	Comunicação entre os dois nós em caso de failover.
Tráfego iSCSI RSM	eth3	nó 1 e nó 2	Tráfego iSCSI RAID SyncMirror, bem como a comunicação entre os dois nós Cloud Volumes ONTAP e o mediador.
Mediador	eth0	Mediador	Um canal de comunicação entre os nós e o mediador para ajudar nos processos de aquisição de storage e giveback.

LIFs para pares de HA em várias AZs

LIF	Interface	Nó	Finalidade
Gerenciamento de nós	eth0	nó 1 e nó 2	Gerenciamento administrativo de um nó.
Entre clusters	eth0	nó 1 e nó 2	Comunicação, backup e replicação entre clusters.
Dados iSCSI	eth0	nó 1 e nó 2	Acesso de cliente através do protocolo iSCSI. Esses LIFs também gerenciam a migração de endereços IP flutuantes entre nós. Estes LIFs são necessários e não devem ser excluídos.
Conectividade de cluster	eth1	nó 1 e nó 2	Permite que os nós se comuniquem entre si e movam dados dentro do cluster.
Conectividade HA	eth2	nó 1 e nó 2	Comunicação entre os dois nós em caso de failover.

LIF	Interface	Nó	Finalidade
Tráfego iSCSI RSM	eth3	nó 1 e nó 2	Tráfego iSCSI RAID SyncMirror, bem como a comunicação entre os dois nós Cloud Volumes ONTAP e o mediador.
Mediador	eth0	Mediador	Um canal de comunicação entre os nós e o mediador para ajudar nos processos de aquisição de storage e giveback.



Quando implantadas em várias zonas de disponibilidade, várias LIFs são associadas ao "Endereços IP flutuantes", que não contam com o limite de IP privado da AWS.

Grupos de segurança

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



Procurando informações sobre o conetor? "[Ver regras do grupo de segurança para o conetor](#)"

Conexão para categorização de dados

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

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

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

Ligações a sistemas ONTAP

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

DNS e active Directory para CIFS

Se você quiser provisionar o storage CIFS, configure o DNS e o active Directory na AWS ou estenda sua configuração local para a AWS.

O servidor DNS deve fornecer serviços de resolução de nomes para o ambiente do active Directory. Você pode configurar conjuntos de opções DHCP para usar o servidor DNS padrão EC2, que não deve ser o servidor DNS usado pelo ambiente active Directory.

Para obter instruções, consulte "[Documentação da AWS: Serviços de domínio do active Directory na nuvem AWS: Implantação de referência de início rápido](#)" a .

Compartilhamento de VPC

A partir da versão 9.11.1, os pares de HA do Cloud Volumes ONTAP são compatíveis com o compartilhamento de VPC na AWS. O compartilhamento de VPC permite que sua organização compartilhe sub-redes com outras contas da AWS. Para usar essa configuração, você deve configurar seu ambiente AWS e implantar o par de HA usando a API.

["Saiba como implantar um par de HA em uma sub-rede compartilhada"](#).

Requisitos para pares de HA em várias AZs

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

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

Zonas de disponibilidade

Este modelo de implantação de HA usa vários AZs para garantir alta disponibilidade de seus dados. Você deve usar uma AZ dedicada para cada instância do Cloud Volumes ONTAP e a instância do mediador, que fornece um canal de comunicação entre o par de HA.

Uma sub-rede deve estar disponível em cada zona de disponibilidade.

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

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

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



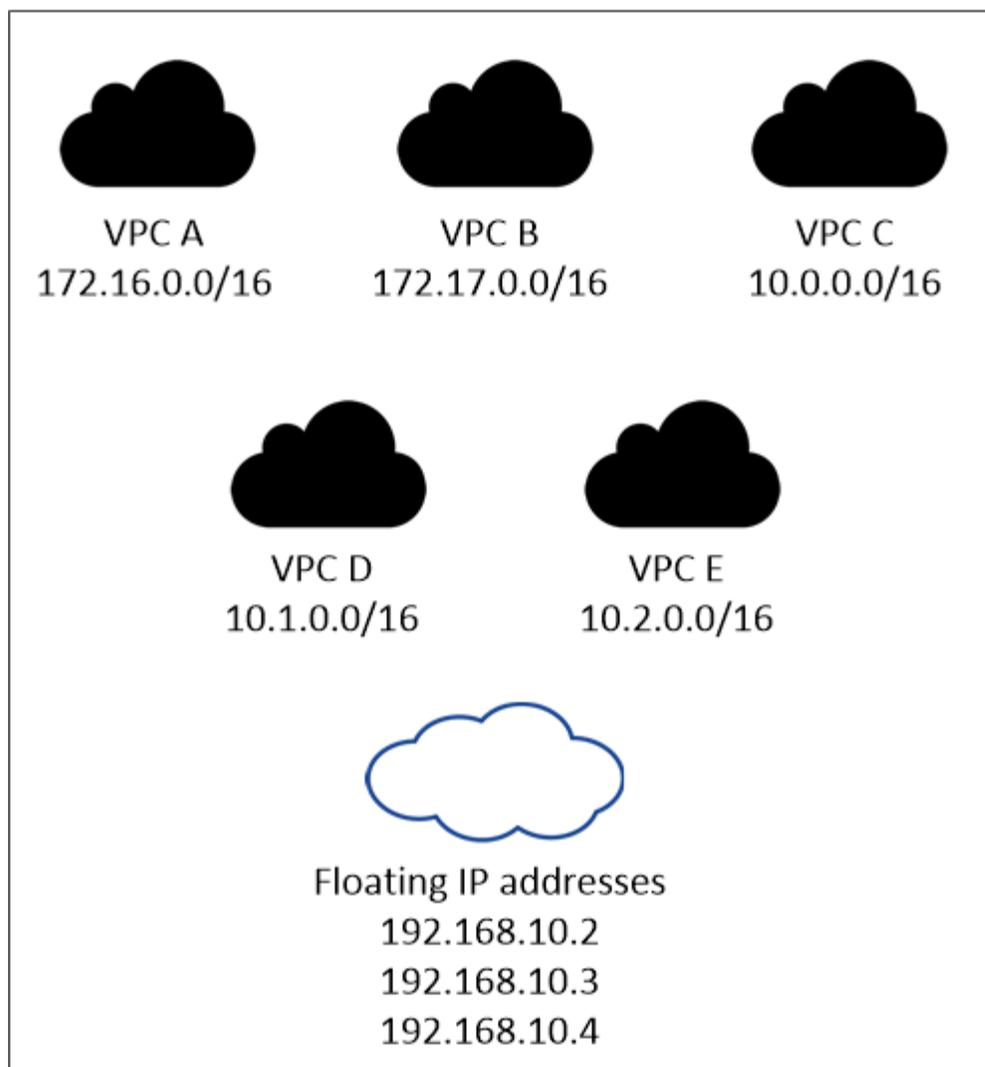
Um endereço IP flutuante é necessário para o LIF de gerenciamento da SVM se você usar o SnapDrive para Windows ou SnapCenter com o par de HA.

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

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

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

AWS region



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

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

Se necessário, ["Configure um gateway de trânsito da AWS"](#) para habilitar o acesso aos endereços IP flutuantes de um par de HA de fora da VPC onde o par de HA reside.

Tabelas de rotas

Depois de especificar os endereços IP flutuantes no BlueXP, você será solicitado a selecionar as tabelas de rota que devem incluir rotas para os endereços IP flutuantes. Isso permite o acesso do cliente ao par de HA.

Se você tiver apenas uma tabela de rota para as sub-redes na VPC (a tabela de rotas principal), o BlueXP adicionará automaticamente os endereços IP flutuantes a essa tabela de rotas. Se tiver mais de uma tabela de rota, é muito importante selecionar as tabelas de rota corretas ao iniciar o par HA. Caso contrário, alguns clientes podem não ter acesso ao Cloud Volumes ONTAP.

Por exemplo, você pode ter duas sub-redes associadas a tabelas de rota diferentes. Se você selecionar a

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

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

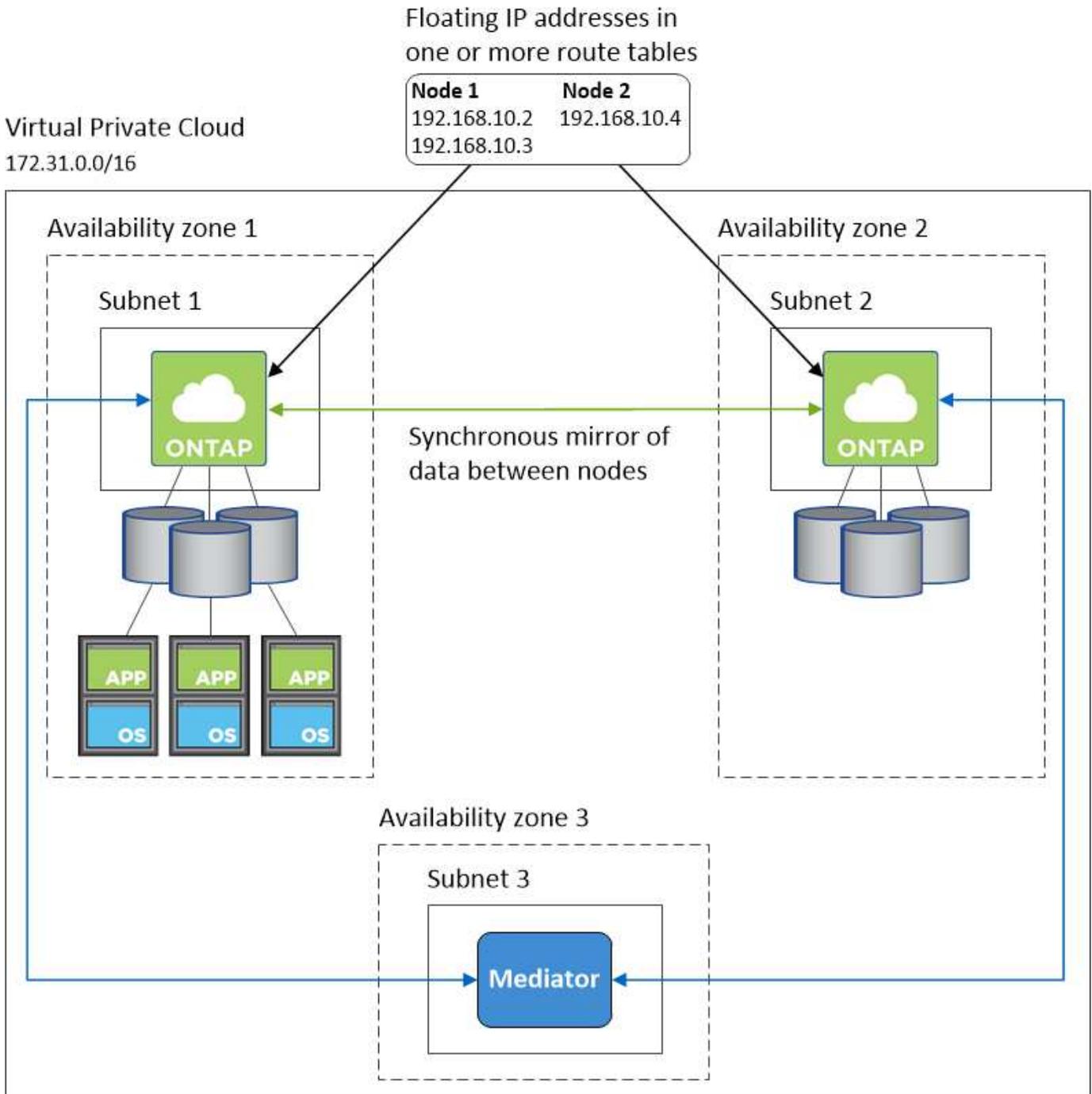
Conexão com ferramentas de gerenciamento do NetApp

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

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

Exemplo de configuração de HA

A imagem a seguir ilustra os componentes de rede específicos de um par de HA em vários AZs: Três zonas de disponibilidade, três sub-redes, endereços IP flutuantes e uma tabela de rotas.



Requisitos para o conetor

Se você ainda não criou um conetor, você deve rever os requisitos de rede para o conetor também.

- ["Veja os requisitos de rede para o conetor"](#)
- ["Regras do grupo de segurança na AWS"](#)

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

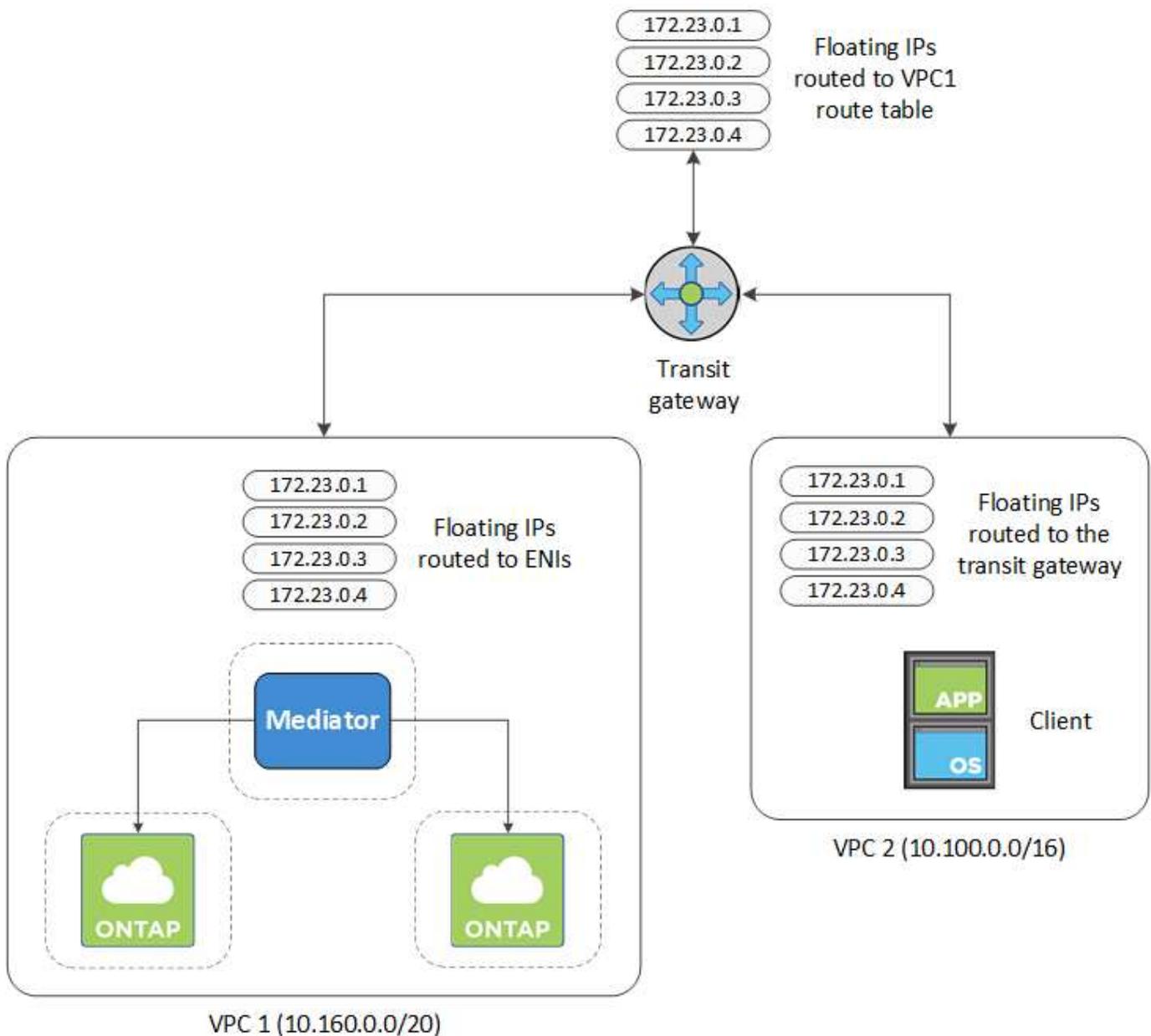
Configure um gateway de trânsito da AWS para permitir o acesso a um par de HA ["Endereços IP flutuantes"](#) de fora da VPC onde o par de HA reside.

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

Endereços IP flutuantes também são necessários para a interface de gerenciamento de cluster e o LIF de gerenciamento opcional SVM.

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

Aqui está um exemplo que mostra dois VPCs conectados por um gateway de trânsito. Um sistema de HA reside em uma VPC, enquanto um cliente reside no outro. Em seguida, você pode montar um volume nas no cliente usando o endereço IP flutuante.



As etapas a seguir ilustram como configurar uma configuração semelhante.

Passos

1. "Crie um gateway de trânsito e conete os VPCs ao gateway".
2. Associe os VPCs à tabela de rotas do gateway de trânsito.
 - a. No serviço **VPC**, clique em **Transit Gateway Route Tables**.
 - b. Selecione a tabela de rotas.
 - c. Clique em **associações** e selecione **criar associação**.
 - d. Escolha os anexos (os VPCs) a associar e clique em **criar associação**.
3. Crie rotas na tabela de rotas do gateway de trânsito especificando os endereços IP flutuantes do par HA.

Você pode encontrar os endereços IP flutuantes na página informações do ambiente de trabalho no BlueXP . Aqui está um exemplo:

NFS & CIFS access from within the VPC using Floating IP

Auto failover

Cluster Management : 172.23.0.1

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

Access

SVM Management : 172.23.0.4

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

Transit Gateway Route Table: tgw-rtb-0ea8ee291c7aedd3

Details Associations Propagations **Routes** Tags

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

Create route Replace route Delete route

Filter by attributes or search by keyword

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

Floating IP Addresses

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

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

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

Route Table: rtb-0569a1bd740ed033f

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

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

VPC1
Floating IP Addresses

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

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

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

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

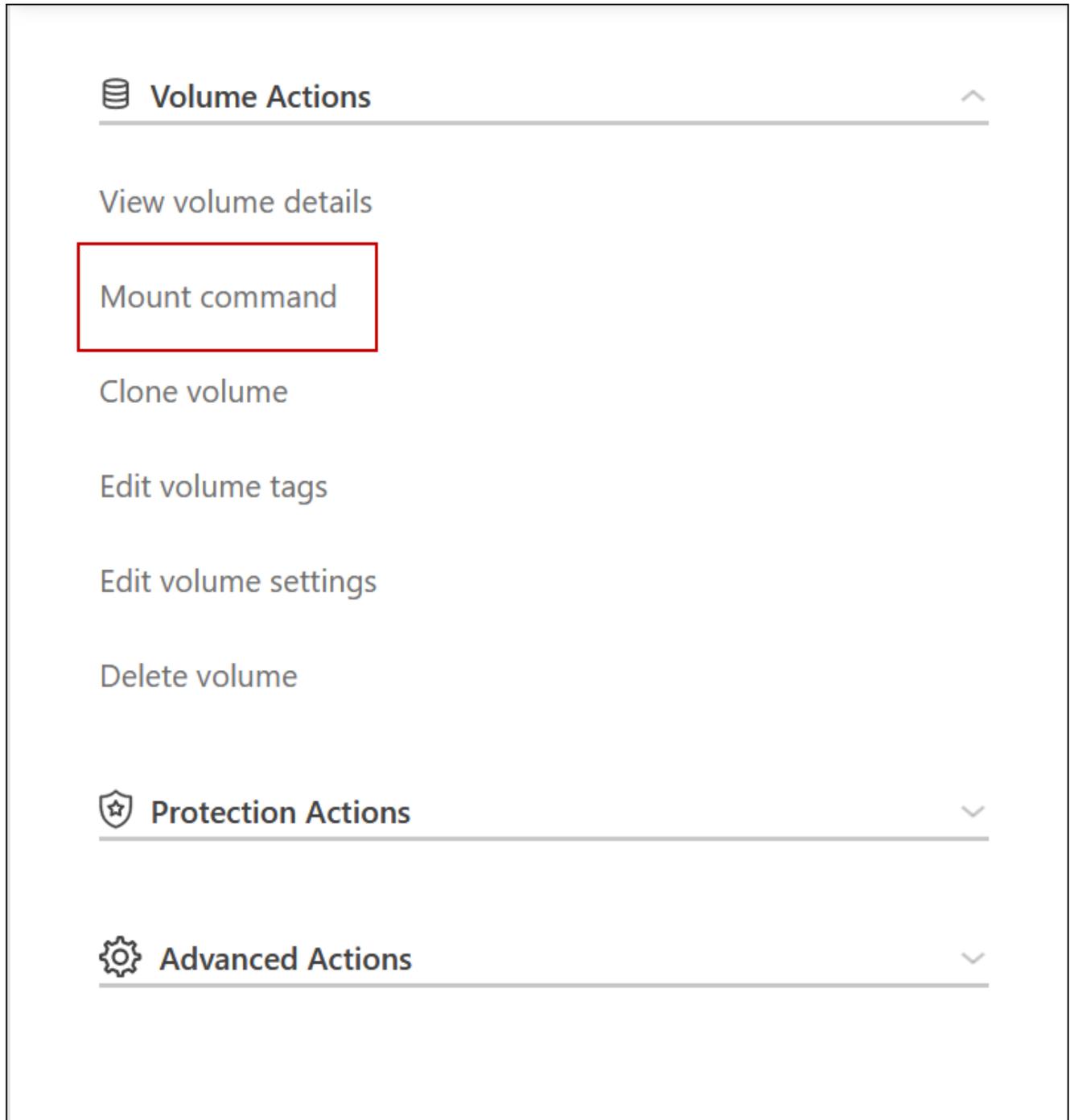
Destination	Target	Status
10.160.0.0/20	local	active
pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22)	vpce-cb51a0a2	active
0.0.0.0/0	igw-b2182dd7	active
10.60.29.0/25	pcx-589c3331	active
10.100.0.0/16	tgw-015b7c249661ac279	active
10.129.0.0/20	pcx-ff7e1396	active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

VPC2
Floating act IP Addresses

6. Atualize as configurações dos grupos de segurança para todo o tráfego da VPC.
 - a. Em Virtual Private Cloud, clique em **sub-redes**.
 - b. Clique na guia **Tabela de rotas**, selecione o ambiente desejado para um dos endereços IP flutuantes para um par de HA.
 - c. Clique em **grupos de segurança**.
 - d. Selecione **Editar regras de entrada**.

- e. Clique em **Adicionar regra**.
 - f. Em tipo, selecione **todo o tráfego** e, em seguida, selecione o endereço IP da VPC.
 - g. Clique em **Salvar regras** para aplicar as alterações.
7. Monte volumes em clientes usando o endereço IP flutuante.

Você pode encontrar o endereço IP correto no BlueXP por meio da opção **comando de montagem** no painel Gerenciar volumes no BlueXP .



8. Se você estiver montando um volume NFS, configure a política de exportação para corresponder à sub-rede da VPC cliente.

["Saiba como editar um volume"](#).

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

Implante um par de HA em uma sub-rede compartilhada

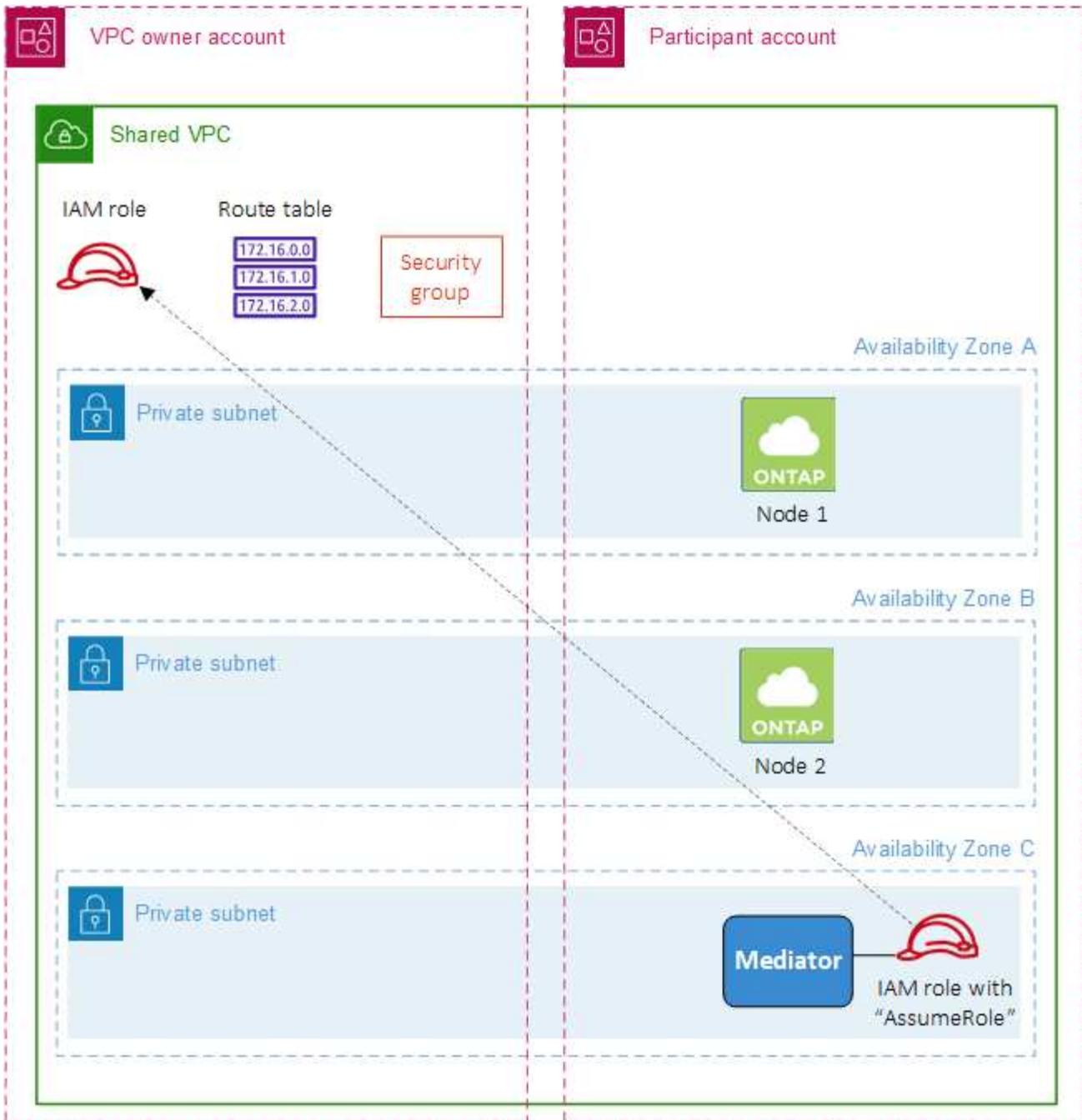
A partir da versão 9.11.1, os pares de HA do Cloud Volumes ONTAP são compatíveis com o compartilhamento de VPC na AWS. O compartilhamento de VPC permite que sua organização compartilhe sub-redes com outras contas da AWS. Para usar essa configuração, você deve configurar seu ambiente AWS e implantar o par de HA usando a API.

Com "[Compartilhamento de VPC](#)"o , uma configuração do Cloud Volumes ONTAP HA é distribuída por duas contas:

- A conta de proprietário da VPC, que possui a rede (VPC, sub-redes, tabelas de rota e grupo de segurança do Cloud Volumes ONTAP)
- A conta do participante, onde as instâncias EC2 são implantadas em sub-redes compartilhadas (isso inclui os dois nós de HA e o mediador)

No caso de uma configuração do Cloud Volumes ONTAP HA implantada em várias zonas de disponibilidade, o mediador de HA precisa de permissões específicas para gravar nas tabelas de rota na conta de proprietário da VPC. Você precisa fornecer essas permissões configurando uma função do IAM que o mediador possa assumir.

A imagem a seguir mostra os componentes envolvidos nessa implantação:



Conforme descrito nas etapas abaixo, você precisará compartilhar as sub-redes com a conta de participante e, em seguida, criar a função do IAM e o grupo de segurança na conta de proprietário da VPC.

Quando você cria o ambiente de trabalho do Cloud Volumes ONTAP, o BlueXP cria e atribui automaticamente uma função do IAM ao mediador. Essa função assume a função do IAM que você criou na conta de proprietário da VPC para fazer alterações nas tabelas de rota associadas ao par de HA.

Passos

1. Compartilhe as sub-redes na conta de proprietário da VPC com a conta de participante.

Essa etapa é necessária para implantar o par de HA em sub-redes compartilhadas.

["Documentação da AWS: Compartilhe uma sub-rede"](#)

2. Na conta de proprietário da VPC, crie um grupo de segurança para o Cloud Volumes ONTAP.

"Consulte as regras do grupo de segurança do Cloud Volumes ONTAP". Observe que você não precisa criar um grupo de segurança para o mediador de HA. BlueXP faz isso por você.

3. Na conta de proprietário da VPC, crie uma função do IAM que inclua as seguintes permissões:

```
  "Action": [
    "ec2:AssignPrivateIpAddresses",
    "ec2:CreateRoute",
    "ec2>DeleteRoute",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeVpcs",
    "ec2:ReplaceRoute",
    "ec2:UnassignPrivateIpAddresses"
```

4. Use a API do BlueXP para criar um novo ambiente de trabalho do Cloud Volumes ONTAP.

Observe que você deve especificar os seguintes campos:

- "Segurança do GroupId"

O campo "securityGroupId" deve especificar o grupo de segurança que você criou na conta de proprietário da VPC (veja a etapa 2 acima).

- "AssumeRoleArn" no objeto "haParams"

O campo "assumeRoleArn" deve incluir o ARN da função do IAM que você criou na conta de proprietário da VPC (veja a etapa 3 acima).

Por exemplo:

```
"haParams": {
  "assumeRoleArn":
  "arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
}
```

+

["Saiba mais sobre a API Cloud Volumes ONTAP"](#)

Regras do grupo de segurança para a AWS

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

Regras para Cloud Volumes ONTAP

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

Regras de entrada

Quando você cria um ambiente de trabalho e escolhe um grupo de segurança predefinido, você pode optar por permitir tráfego em um dos seguintes:

- **Somente VPC selecionada:** A origem do tráfego de entrada é o intervalo de sub-rede da VPC para o sistema Cloud Volumes ONTAP e o intervalo de sub-rede da VPC onde o conector reside. Esta é a opção recomendada.
- **Todos os VPCs:** A origem do tráfego de entrada é o intervalo IP 0,0.0.0/0.

Protocolo	Porta	Finalidade
Todo o ICMP	Tudo	Fazer ping na instância
HTTP	80	Acesso HTTP ao console da Web do Gerenciador de sistema do ONTAP usando o endereço IP do LIF de gerenciamento de cluster
HTTPS	443	Conetividade com o conector e acesso HTTPS à consola Web do Gestor de sistema ONTAP utilizando o endereço IP do LIF de gestão de clusters
SSH	22	Acesso SSH ao endereço IP do LIF de gerenciamento de cluster ou um LIF de gerenciamento de nó
TCP	111	Chamada de procedimento remoto para NFS
TCP	139	Sessão de serviço NetBIOS para CIFS
TCP	161-162	Protocolo de gerenciamento de rede simples
TCP	445	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
TCP	635	Montagem em NFS
TCP	749	Kerberos
TCP	2049	Daemon do servidor NFS
TCP	3260	Acesso iSCSI através do iSCSI data LIF
TCP	4045	Daemon de bloqueio NFS
TCP	4046	Monitor de status da rede para NFS
TCP	10000	Backup usando NDMP
TCP	11104	Gestão de sessões de comunicação entre clusters para SnapMirror
TCP	11105	Transferência de dados SnapMirror usando LIFs entre clusters
UDP	111	Chamada de procedimento remoto para NFS
UDP	161-162	Protocolo de gerenciamento de rede simples
UDP	635	Montagem em NFS
UDP	2049	Daemon do servidor NFS

Protocolo	Porta	Finalidade
UDP	4045	Daemon de bloqueio NFS
UDP	4046	Monitor de status da rede para NFS
UDP	4049	Protocolo rquotad NFS

Regras de saída

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

Regras básicas de saída

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

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

Regras de saída avançadas

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



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

Serviço	Protocolo	Porta	Fonte	Destino	Finalidade
Ative Directory					

	TCP	445	DATA LIF (NFS, CIFS)	Floresta do ativo Directory	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
Serviço	Protocolo	Porta	Dados	Destino	Finalidade
	TCP	445	DATA LIF (NFS, CIFS)	Floresta do ativo Directory	Alterar e definir senha (SET_CHANGE)
	UDP	464	DATA LIF (NFS, CIFS)	Floresta do ativo Directory	Administração de chaves Kerberos
	TCP	749	DATA LIF (NFS, CIFS)	Floresta do ativo Directory	Palavra-passe de alteração e definição Kerberos V (RPCSEC_GSS)
AutoSupport	HTTPS	443	LIF de gerenciamento de nós	suporte.NetApp.com	AutoSupport (HTTPS é o padrão)
	HTTP	80	LIF de gerenciamento de nós	suporte.NetApp.com	AutoSupport (somente se o protocolo de transporte for alterado de HTTPS para HTTP)
	TCP	3128	LIF de gerenciamento de nós	Conetor	Enviar mensagens AutoSupport através de um servidor proxy no conetor, se uma conexão de saída de Internet não estiver disponível
Cópia de segurança para S3	TCP	5010	LIF entre clusters	Ponto de extremidade de backup ou ponto de extremidade de restauração	Fazer backup e restaurar operações para o recurso Backup to S3
Cluster	Todo o tráfego	Todo o tráfego	Todos os LIFs em um nó	Todos os LIFs no outro nó	Comunicações entre clusters (apenas Cloud Volumes ONTAP HA)
	TCP	3000	LIF de gerenciamento de nós	Ha mediador	Chamadas ZAPI (somente Cloud Volumes ONTAP HA)
	ICMP	1	LIF de gerenciamento de nós	Ha mediador	Manter vivo (apenas Cloud Volumes ONTAP HA)
Backups de configuração	HTTP	80	LIF de gerenciamento de nós	Http://<connector-IP-address>/occm/offboxconfig	Envie backups de configuração para o conetor. "Saiba mais sobre arquivos de backup de configuração" .
DHCP	UDP	68	LIF de gerenciamento de nós	DHCP	Cliente DHCP para configuração pela primeira vez
DHCPS	UDP	67	LIF de gerenciamento de nós	DHCP	Servidor DHCP
DNS	UDP	53	LIF e LIF de dados de gerenciamento de nós (NFS, CIFS)	DNS	DNS

Serviço	Protocolo	Porta	Fonte	Destino	Finalidade
NDMP	TCP	1860-18699	LIF de gerenciamento de nós	Servidores de destino	Cópia NDMP
SMTP	TCP	25	LIF de gerenciamento de nós	Servidor de correio	Alertas SMTP, podem ser usados para AutoSupport
SNMP	TCP	161	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
	UDP	161	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
	TCP	162	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
	UDP	162	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
SnapMirror	TCP	11104	LIF entre clusters	LIFs ONTAP entre clusters	Gestão de sessões de comunicação entre clusters para SnapMirror
	TCP	11105	LIF entre clusters	LIFs ONTAP entre clusters	Transferência de dados SnapMirror
Syslog	UDP	514	LIF de gerenciamento de nós	Servidor syslog	Mensagens de encaminhamento do syslog

Regras para o grupo de segurança externa do mediador HA

O grupo de segurança externo predefinido para o mediador de HA do Cloud Volumes ONTAP inclui as seguintes regras de entrada e saída.

Regras de entrada

O grupo de segurança predefinido do mediador de HA inclui a seguinte regra de entrada.

Protocolo	Porta	Fonte	Finalidade
TCP	3000	CIDR do conector	Acesso à API RESTful a partir do conector

Regras de saída

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

Regras básicas de saída

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

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

Regras de saída avançadas

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

Protocolo	Porta	Destino	Finalidade
HTTP	80	Endereço IP do conector na instância do AWS EC2	Faça o download de atualizações para o mediador
HTTPS	443	ec2.amazonaws.com	Assistência com failover de storage
UDP	53	ec2.amazonaws.com	Assistência com failover de storage



Em vez de abrir as portas 443 e 53, você pode criar um endpoint de VPC de interface da sub-rede de destino para o serviço AWS EC2.

Regras para o grupo de segurança interna de configuração de HA

O grupo de segurança interno predefinido para uma configuração de HA do Cloud Volumes ONTAP inclui as seguintes regras. Esse grupo de segurança permite a comunicação entre os nós de HA e entre o mediador e os nós.

O BlueXP sempre cria esse grupo de segurança. Você não tem a opção de usar o seu próprio.

Regras de entrada

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

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

Regras de saída

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

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

Regras para o conector

["Ver regras do grupo de segurança para o conector"](#)

Configurando o AWS KMS

Se você quiser usar a criptografia da Amazon com o Cloud Volumes ONTAP, precisará configurar o Serviço de Gerenciamento de chaves da AWS (KMS).

Passos

1. Certifique-se de que existe uma chave mestra do cliente (CMK) ativa.

O CMK pode ser um CMK gerenciado pela AWS ou um CMK gerenciado pelo cliente. Ele pode estar na mesma conta da AWS que o BlueXP e o Cloud Volumes ONTAP ou em uma conta diferente da AWS.

["Documentação da AWS: Chaves mestras do cliente \(CMKs\)"](#)

2. Modifique a política de chave para cada CMK adicionando a função do IAM que fornece permissões ao BlueXP como um *usuário-chave*.

Adicionar a função do IAM como um usuário-chave dá permissões ao BlueXP para usar o CMK com Cloud Volumes ONTAP.

["Documentação da AWS: Editando chaves"](#)

3. Se o CMK estiver em uma conta AWS diferente, execute as seguintes etapas:

- a. Vá para o console do KMS a partir da conta onde o CMK reside.
- b. Selecione a tecla .
- c. No painel **General Configuration** (Configuração geral), copie o ARN da chave.

Você precisará fornecer o ARN ao BlueXP ao criar o sistema Cloud Volumes ONTAP.

- d. No painel **outras contas da AWS**, adicione a conta da AWS que fornece permissões ao BlueXP .

Na maioria dos casos, essa é a conta onde o BlueXP reside. Se o BlueXP não fosse instalado na AWS, seria a conta para a qual você forneceu as chaves de acesso da AWS ao BlueXP .



Other AWS accounts ✕

Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. [Learn more](#)

arn:aws:iam:: :root

- e. Agora mude para a conta da AWS que fornece permissões ao BlueXP e abra o console do IAM.
- f. Crie uma política do IAM que inclua as permissões listadas abaixo.
- g. Anexe a política à função do IAM ou ao usuário do IAM que fornece permissões ao BlueXP .

A política a seguir fornece as permissões que o BlueXP precisa para usar o CMK da conta externa da AWS. Certifique-se de modificar a região e o ID da conta nas seções "recurso".

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowUseOfTheKey",
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
      ]
    },
    {
      "Sid": "AllowAttachmentOfPersistentResources",
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": [
        "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
      ],
      "Condition": {
        "Bool": {
          "kms:GrantIsForAWSResource": true
        }
      }
    }
  ]
}

```

+

Para obter mais detalhes sobre este processo, consulte o ["Documentação da AWS: Permitindo que usuários de outras contas usem uma chave KMS"](#).

4. Se você estiver usando um CMK gerenciado pelo cliente, modifique a política-chave para o CMK adicionando a função do IAM do Cloud Volumes ONTAP como um *key user*.

Essa etapa é necessária se você habilitar a disposição em camadas de dados no Cloud Volumes ONTAP e quiser criptografar os dados armazenados no bucket do S3.

Você precisará executar esta etapa *depois* você implantar o Cloud Volumes ONTAP porque a função do IAM é criada quando você cria um ambiente de trabalho. (Claro, você tem a opção de usar uma função existente do Cloud Volumes ONTAP IAM, então é possível executar essa etapa antes.)

["Documentação da AWS: Editando chaves"](#)

Configurar funções do IAM para o Cloud Volumes ONTAP

As funções do IAM com as permissões necessárias devem ser anexadas a cada nó do Cloud Volumes ONTAP. O mesmo se aplica ao mediador da HA. É mais fácil permitir que o BlueXP crie as funções do IAM para você, mas você pode usar suas próprias funções.

Esta tarefa é opcional. Quando você cria um ambiente de trabalho do Cloud Volumes ONTAP, a opção padrão é permitir que o BlueXP crie as funções do IAM para você. Se as políticas de segurança da sua empresa exigirem que você crie as funções do IAM, siga as etapas abaixo.



Fornecer sua própria função do IAM é necessário na nuvem secreta da AWS. ["Saiba como implantar o Cloud Volumes ONTAP em C2S"](#).

Passos

1. Vá para o console do AWS IAM.
2. Crie políticas do IAM que incluem as seguintes permissões:
 - Política de base para nós de Cloud Volumes ONTAP

Regiões padrão

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3>DeleteObject"
    ],
    "Resource": "arn:aws:s3:::fabric-pool-*",
    "Effect": "Allow"
  }
]
```

Regiões GovCloud (EUA)

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws-us-gov:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject"
    ],
    "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
    "Effect": "Allow"
  }]
}
```

Top regiões secretas

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws-iso:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws-iso:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3>DeleteObject"
    ],
    "Resource": "arn:aws-iso:s3:::fabric-pool-*",
    "Effect": "Allow"
  }]
}
```

Regiões secretas

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws-iso-b:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3>DeleteObject"
    ],
    "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
    "Effect": "Allow"
  }]
}

```

- Política de backup para nós de Cloud Volumes ONTAP

Se você pretende usar o backup e a recuperação do BlueXP com seus sistemas Cloud Volumes ONTAP, a função do IAM para os nós deve incluir a segunda política mostrada abaixo.

Regiões padrão

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*/**",
      "Effect": "Allow"
    }
  ]
}
```

Regiões GovCloud (EUA)

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws-us-gov:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws-us-gov:s3:::netapp-backup*/**",
      "Effect": "Allow"
    }
  ]
}

```

Top regiões secretas

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws-iso:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws-iso:s3:::netapp-backup*/**",
      "Effect": "Allow"
    }
  ]
}

```

Regiões secretas

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws-iso-b:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws-iso-b:s3:::netapp-backup*/**",
      "Effect": "Allow"
    }
  ]
}

```

- Ha mediador

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:AssignPrivateIpAddresses",
      "ec2:CreateRoute",
      "ec2>DeleteRoute",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeRouteTables",
      "ec2:DescribeVpcs",
      "ec2:ReplaceRoute",
      "ec2:UnassignPrivateIpAddresses",
      "sts:AssumeRole",
      "ec2:DescribeSubnets"
    ],
    "Resource": "*"
  }
]
}

```

3. Crie uma função do IAM e anexe as políticas que você criou à função.

Resultado

Agora você tem funções do IAM que pode selecionar ao criar um novo ambiente de trabalho do Cloud Volumes ONTAP.

Mais informações

- ["Documentação da AWS: Criando políticas do IAM"](#)
- ["Documentação da AWS: Criando funções do IAM"](#)

Configure o licenciamento para o Cloud Volumes ONTAP na AWS

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

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 à esquerda, selecione **Storage > Canvas**.
2. Na página Canvas, clique em **Adicionar ambiente de trabalho** e siga as etapas no BlueXP .

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

Você não será cobrado por meio da assinatura do mercado, a menos que exceda 500 GiB de capacidade provisionada, momento em que o sistema é convertido automaticamente para o "Pacote Essentials".

Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

Pay-Per-TiB - Annual Contract
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

Pay-as-you-go
Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

- 1 AWS Marketplace**
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 Cloud Manager**
Save your subscription and associate the Marketplace subscription with your AWS credentials.

- a. Depois de voltar ao BlueXP , selecione **Freemium** quando chegar à página métodos de carregamento.

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 na AWS"](#).

Licença baseada em capacidade

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

Os pacotes Essentials e Professional estão disponíveis com os seguintes modelos de consumo:

- Uma licença (traga sua própria licença (BYOL)) comprada da NetApp
- Uma assinatura por hora, com pagamento conforme o uso (PAYGO) no AWS Marketplace
- Um contrato anual do AWS Marketplace

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

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

BYOL

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

Passos

1. ["Entre em Contato com a NetApp Sales para obter uma licença"](#)
2. ["Adicione sua conta do site de suporte da NetApp ao BlueXP "](#)

A BlueXP 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 BlueXP adiciona automaticamente as licenças à carteira digital.

A sua licença tem de estar disponível na carteira digital BlueXP antes de a poder utilizar com o Cloud Volumes ONTAP. Se necessário, você pode ["Adicione manualmente a licença à carteira digital BlueXP "](#).

3. Na página Canvas, clique em **Adicionar ambiente de trabalho** e siga as etapas no BlueXP .
 - a. Na página **Detalhes e credenciais**, clique em **Editar credenciais > Adicionar assinatura** e siga as instruções para assinar a oferta de pagamento conforme o uso no AWS Marketplace.

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

Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

Pay-Per-TiB - Annual Contract
 Pay for Cloud Volumes ONTAP with an annual, upfront payment.

Pay-as-you-go
 Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

- 1 **AWS Marketplace**
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 **Cloud Manager**
Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue
Cancel

- a. Depois de voltar ao BlueXP , selecione um pacote baseado na capacidade quando chegar à página métodos de carregamento.

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 na AWS".

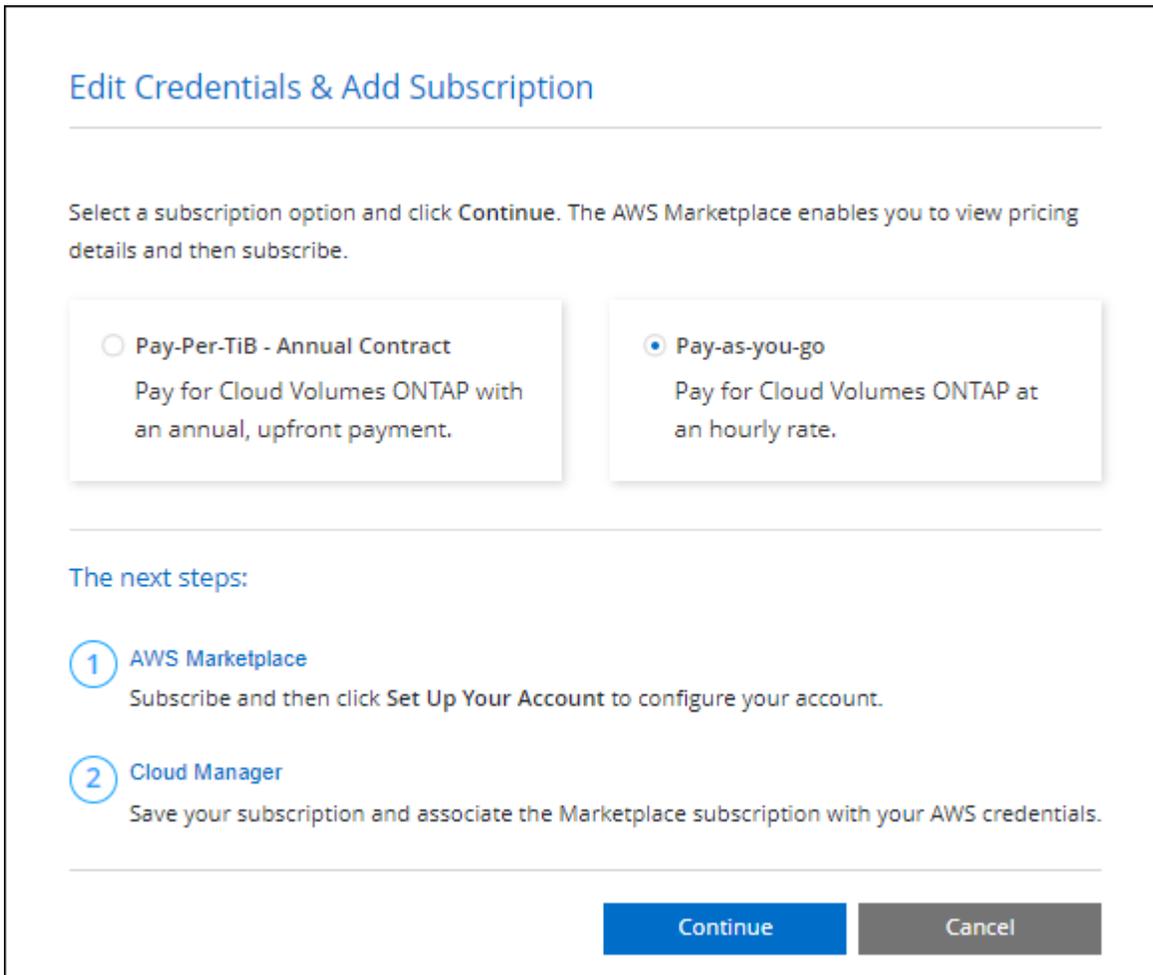
Subscrição PAYGO

Pague por hora assinando a oferta no mercado do seu provedor de nuvem.

Quando você cria um ambiente de trabalho do Cloud Volumes ONTAP, o BlueXP solicita que você assine o contrato disponível no AWS Marketplace. Essa assinatura é então associada ao ambiente de trabalho para cobrança. Você pode usar essa mesma assinatura para ambientes de trabalho adicionais.

Passos

1. No menu de navegação à esquerda, selecione **Storage > Canvas**.
2. Na página Canvas, clique em **Adicionar ambiente de trabalho** e siga as etapas no BlueXP .
 - a. Na página **Detalhes e credenciais**, clique em **Editar credenciais > Adicionar assinatura** e siga as instruções para assinar a oferta de pagamento conforme o uso no AWS Marketplace.



Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

Pay-Per-TiB - Annual Contract
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

Pay-as-you-go
Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

1 AWS Marketplace
Subscribe and then click **Set Up Your Account** to configure your account.

2 Cloud Manager
Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue **Cancel**

- b. Depois de voltar ao BlueXP , selecione um pacote baseado na capacidade quando chegar à página métodos de carregamento.

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 na AWS".



Você pode gerenciar as assinaturas do AWS Marketplace associadas às suas contas da AWS na página Configurações > credenciais. ["Saiba como gerenciar suas contas e assinaturas da AWS"](#)

Contrato anual

Pague anualmente comprando um contrato anual no mercado do seu fornecedor de nuvem.

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

Passos

1. Na página Canvas, clique em **Adicionar ambiente de trabalho** e siga as etapas no BlueXP .
 - a. Na página **Detalhes e credenciais**, clique em **Editar credenciais > Adicionar assinatura** e siga as instruções para assinar o contrato anual no AWS Marketplace.

Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

Pay-Per-TiB - Annual Contract
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

Pay-as-you-go
Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

- 1 AWS Marketplace**
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 Cloud Manager**
Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue **Cancel**

- b. Depois de voltar ao BlueXP , selecione um pacote baseado na capacidade quando chegar à página métodos de carregamento.

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 na AWS".

Inscrição no Keystone

Uma subscrição do Keystone é um serviço baseado em subscrição com pagamento conforme o uso. ["Saiba mais sobre as assinaturas do NetApp Keystone"](#).

Passos

1. Se você ainda não tem uma assinatura, ["Entre em Contato com a NetApp"](#)
2. Para autorizar sua conta de usuário do BlueXP com uma ou mais assinaturas do Keystone NetApp NetApp.
3. Depois que o NetApp autorizar sua conta ["Vincule suas assinaturas para uso com o Cloud Volumes ONTAP"](#), .
4. Na página Canvas, clique em **Adicionar ambiente de trabalho** e siga as etapas no BlueXP .
 - a. Selecione o método de cobrança da assinatura Keystone quando solicitado a escolher um método de cobrança.

The screenshot shows a 'Select Charging Method' dialog box with the following content:

- Keystone** (selected): *By capacity* (blue button), ^
- Professional**: *By capacity* (blue button), v
- Essential**: *By capacity* (blue button), v
- Freemium (Up to 500 GiB)**: *By capacity* (blue button), v
- Per Node**: *By node* (purple button), v

Expanded details for the selected **Keystone** option:

- Storage management
- Charged against your NetApp credit
- Keystone Subscription: A-AMRITA1 (dropdown)

["Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP na AWS"](#).

Iniciando o Cloud Volumes ONTAP na AWS

É possível iniciar o Cloud Volumes ONTAP em uma configuração de sistema único ou como par de HA na AWS.

Antes de começar

Você precisa do seguinte para criar um ambiente de trabalho.

- Um conector que está em funcionamento.
 - Você deve ter um ["Conector que está associado ao seu projeto ou área de trabalho"](#).
 - ["Você deve estar preparado para deixar o conector funcionando o tempo todo"](#).
- Uma compreensão da configuração que você deseja usar.

Você deve se preparar escolhendo uma configuração e obtendo informações de rede da AWS de seu administrador. Para obter detalhes, ["Planejando sua configuração do Cloud Volumes ONTAP"](#) consulte .

- Uma compreensão do que é necessário para configurar o licenciamento para o Cloud Volumes ONTAP.
["Saiba como configurar o licenciamento"](#).
- DNS e ative Directory para configurações CIFS.

Para obter detalhes, ["Requisitos de rede para o Cloud Volumes ONTAP na AWS"](#) consulte .

Lançamento de um sistema Cloud Volumes ONTAP de nó único na AWS

Para iniciar o Cloud Volumes ONTAP na AWS, é necessário criar um novo ambiente de trabalho no BlueXP

Sobre esta tarefa

Imediatamente após criar o ambiente de trabalho, o BlueXP inicia uma instância de teste na VPC especificada para verificar a conectividade. Se bem-sucedido, o BlueXP encerra imediatamente a instância e, em seguida, começa a implantar o sistema Cloud Volumes ONTAP. Se o BlueXP não puder verificar a conectividade, a criação do ambiente de trabalho falhará. A instância de teste é um T2.nano (para alocação de VPC padrão) ou m3.medium (para alocação de VPC dedicada).

Passos

1. No menu de navegação à esquerda, selecione **Storage > Canvas**.
2. na página do Canvas, clique em **Adicionar ambiente de trabalho** e siga as instruções.
3. **Escolha um local:** Selecione **Serviços da Amazon** e **nó único Cloud Volumes ONTAP**.
4. Se for solicitado, ["Crie um conector"](#).
5. **Detalhes e credenciais:** Opcionalmente, altere as credenciais e a assinatura da AWS, insira um nome de ambiente de trabalho, adicione tags, se necessário, e insira uma senha.

Alguns dos campos desta página são auto-explicativos. A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Nome do ambiente de trabalho	O BlueXP usa o nome do ambiente de trabalho para nomear tanto o sistema Cloud Volumes ONTAP quanto a instância do Amazon EC2. Ele também usa o nome como prefixo para o grupo de segurança predefinido, se você selecionar essa opção.

Campo	Descrição
Adicionar etiquetas	As tags AWS são metadados para seus recursos da AWS. O BlueXP adiciona as tags à instância do Cloud Volumes ONTAP e a cada recurso da AWS associado à instância. Você pode adicionar até quatro tags da interface do usuário ao criar um ambiente de trabalho e, em seguida, você pode adicionar mais após a criação. Observe que a API não limita a quatro tags ao criar um ambiente de trabalho. Para obter informações sobre tags, " Documentação da AWS: Marcando seus recursos do Amazon EC2 " consulte .
Nome de utilizador e palavra-passe	Estas são as credenciais da conta de administrador de cluster do Cloud Volumes ONTAP. Você pode usar essas credenciais para se conectar ao Cloud Volumes ONTAP por meio do Gerenciador de sistemas do ONTAP ou da CLI do ONTAP. Mantenha o nome de usuário padrão <i>admin</i> ou altere-o para um nome de usuário personalizado.
Editar credenciais	Escolha as credenciais da AWS associadas à conta na qual você deseja implantar esse sistema. Você também pode associar a assinatura do AWS Marketplace para usar com este sistema Cloud Volumes ONTAP. Clique em Adicionar assinatura para associar as credenciais selecionadas a uma nova assinatura do AWS Marketplace. A assinatura pode ser feita por um contrato anual ou para pagar por Cloud Volumes ONTAP a uma taxa por hora. " Saiba como adicionar credenciais adicionais da AWS ao BlueXP ".

O vídeo a seguir mostra como associar uma assinatura do Marketplace de pagamento conforme o uso às suas credenciais da AWS:

[Inscreva-se no BlueXP no AWS Marketplace](#)

Se vários usuários do IAM trabalharem na mesma conta da AWS, cada usuário precisará se inscrever. Depois que o primeiro usuário se inscreve, o AWS Marketplace informa aos usuários subsequentes que eles já estão inscritos, como mostrado na imagem abaixo. Enquanto uma assinatura está em vigor para a AWS *account*, cada usuário do IAM precisa se associar a essa assinatura. Se você vir a mensagem mostrada abaixo, clique no link **clique aqui** para acessar o site da BlueXP e concluir o processo.



Cloud Manager (for Cloud Volumes ONTAP)

You are currently subscribed to this product and will be charged for your accumulated usage at the end of your next billing cycle, based on the costs listed in Pricing information on the right.

? **Having issues signing up for your product?**
If you were unable to complete the set-up process for this software, please [click here](#) to be taken to the product's registration area.

Subscribe

You are already subscribed to this product

Pricing Details

Software Fees

6. **Serviços:** Mantenha os serviços ativados ou desative os serviços individuais que você não deseja usar com o Cloud Volumes ONTAP.

- "[Saiba mais sobre a classificação BlueXP](#)"
- "[Saiba mais sobre backup e recuperação do BlueXP](#)"



Se quiser utilizar WORM e disposição de dados em camadas, desative o backup e a recuperação do BlueXP e implante um ambiente de trabalho do Cloud Volumes ONTAP com a versão 9,8 ou superior.

7. **Localização e conectividade:** Introduza as informações de rede que gravou no ["Planilha da AWS"](#).

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

Campo	Descrição
VPC	Se você tiver um AWS Outpost, você poderá implantar um sistema Cloud Volumes ONTAP de nó único nesse Outpost selecionando a VPC Outpost. A experiência é a mesma que qualquer outra VPC que reside na AWS.
Grupo de segurança gerado	Se você permitir que o BlueXP gere o grupo de segurança para você, você precisa escolher como permitirá o tráfego: <ul style="list-style-type: none">• Se você escolher somente VPC selecionada, a origem do tráfego de entrada será o intervalo de sub-rede da VPC selecionada e o intervalo de sub-rede da VPC onde o conector reside. Esta é a opção recomendada.• Se você escolher todos os VPCs, a origem do tráfego de entrada é o intervalo IP 0,0.0.0/0.
Use o grupo de segurança existente	Se utilizar uma política de firewall existente, certifique-se de que inclui as regras necessárias. "Saiba mais sobre as regras de firewall do Cloud Volumes ONTAP" .

8. **Criptografia de dados:** Não escolha criptografia de dados ou criptografia gerenciada pela AWS.

Para criptografia gerenciada pela AWS, você pode escolher uma chave mestra do cliente (CMK) diferente da sua conta ou de outra conta da AWS.



Não é possível alterar o método de criptografia de dados da AWS depois de criar um sistema Cloud Volumes ONTAP.

["Saiba como configurar o AWS KMS para Cloud Volumes ONTAP"](#).

["Saiba mais sobre as tecnologias de criptografia suportadas"](#).

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

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

10. **Configuração do Cloud Volumes ONTAP** (somente contrato anual do AWS Marketplace): Revise a configuração padrão e clique em **continuar** ou em **alterar configuração** para selecionar sua própria configuração.

Se você mantiver a configuração padrão, precisará especificar apenas um volume e, em seguida, revisar e aprovar a configuração.

11. **Pacotes pré-configurados:** Selecione um dos pacotes para iniciar rapidamente o Cloud Volumes ONTAP ou clique em **alterar configuração** para selecionar sua própria configuração.

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

12. **Função do IAM:** É melhor manter a opção padrão para permitir que o BlueXP crie a função para você.

Se você preferir usar sua própria política, ela deve atender "[Requisitos de política para nós de Cloud Volumes ONTAP](#)".

13. **Licenciamento:** Altere a versão do Cloud Volumes ONTAP conforme necessário e selecione um tipo de instância e a alocação de instância.



Se um candidato de lançamento mais recente, disponibilidade geral ou liberação de 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 9.13.1 e 9.13.1 P4 estiver disponível. A atualização não ocorre de uma versão para outra, por exemplo, de 9,13 a 9,14.

14. **Recursos de armazenamento subjacentes:** Escolha um tipo de disco, configure o armazenamento subjacente e escolha se deseja manter a disposição de dados ativada.

Observe o seguinte:

- O tipo de disco é para o volume inicial (e agregado). Você pode escolher um tipo de disco diferente para volumes subsequentes (e agregados).
- Se você escolher um disco de GP3 TB ou IO1 tb, o BlueXP usará o recurso volumes elásticos na AWS para aumentar automaticamente a capacidade de disco de storage subjacente conforme necessário. Você pode escolher a capacidade inicial com base nas suas necessidades de storage e revisá-la após a implantação do Cloud Volumes ONTAP. "[Saiba mais sobre o suporte a volumes elásticos na AWS](#)".
- Se você escolher um disco de GP2 TB ou st1 TB, poderá selecionar um tamanho de disco para todos os discos no agregado inicial e para quaisquer agregados adicionais criados pelo BlueXP ao usar a opção de provisionamento simples. Você pode criar agregados que usam um tamanho de disco diferente usando a opção Alocação avançada.
- Você pode escolher uma política específica de disposição em categorias de volume ao criar ou editar um volume.
- Se você desativar a disposição de dados em categorias, poderá ativá-la em agregados subsequentes.

["Saiba como funciona a disposição em camadas de dados"](#).

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

a. Escolha **normal** ou **alta** velocidade de gravação, se desejado.

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

b. Ative o storage WORM (uma gravação, muitas leituras), se desejado.

O WORM não pode ser ativado se a disposição de dados em camadas foi ativada para o Cloud Volumes ONTAP versões 9,7 e inferiores. Reverter ou fazer downgrade para o Cloud Volumes ONTAP 9,8 é bloqueado depois de ativar WORM e disposição em camadas.

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

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

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

"Saiba mais sobre protocolos e versões de clientes compatíveis".

Alguns dos campos desta página são auto-explicativos. A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Tamanho	O tamanho máximo que você pode inserir depende, em grande parte, se você ativar o provisionamento de thin, o que permite criar um volume maior do que o armazenamento físico atualmente disponível para ele.
Controle de acesso (somente para NFS)	Uma política de exportação define os clientes na sub-rede que podem acessar o volume. Por padrão, o BlueXP insere um valor que fornece acesso a todas as instâncias na sub-rede.
Permissões e utilizadores/grupos (apenas para CIFS)	Esses campos permitem controlar o nível de acesso a um compartilhamento para usuários e grupos (também chamados de listas de controle de acesso ou ACLs). Você pode especificar usuários ou grupos do Windows locais ou de domínio, ou usuários ou grupos UNIX. Se você especificar um nome de usuário do domínio do Windows, você deve incluir o domínio do usuário usando o nome de domínio do formato.
Política de instantâneos	Uma política de cópia Snapshot especifica a frequência e o número de cópias snapshot do NetApp criadas automaticamente. Uma cópia Snapshot do NetApp é uma imagem pontual do sistema de arquivos que não afeta a performance e exige o mínimo de storage. Você pode escolher a política padrão ou nenhuma. Você pode escolher nenhum para dados transitórios: Por exemplo, tempdb para Microsoft SQL Server.
Opções avançadas (somente para NFS)	Selecione uma versão NFS para o volume: NFSv3 ou NFSv4.
Grupo de iniciadores e IQN (apenas para iSCSI)	Os destinos de armazenamento iSCSI são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Os grupos de iniciadores são tabelas de nomes de nós de host iSCSI e controlam quais iniciadores têm acesso a quais LUNs. Os destinos iSCSI se conectam à rede por meio de adaptadores de rede Ethernet (NICs) padrão, placas de mecanismo de descarga TCP (TOE) com iniciadores de software, adaptadores de rede convergidos (CNAs) ou adaptadores de barramento de host dedicados (HBAs) e são identificados por IQNs (iSCSI Qualified Names). Quando cria um volume iSCSI, o BlueXP cria automaticamente um LUN para si. Simplificamos a criação de apenas um LUN por volume, para que não haja gerenciamento envolvido. Depois de criar o volume, "Use o IQN para se conectar ao LUN a partir de seus hosts" .

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

Volume Details, Protection & Protocol

Details & Protection	Protocol
<p>Volume Name: <input style="width: 200px;" type="text" value="vol"/> Size (GB): <input style="width: 80px;" type="text" value="250"/></p> <p>Snapshot Policy: <input style="width: 300px;" type="text" value="default"/></p> <p><small>Default Policy</small></p>	<p style="text-align: center;"> NFS CIFS iSCSI </p> <p>Share name: <input style="width: 150px;" type="text" value="vol_share"/> Permissions: <input style="width: 150px;" type="text" value="Full Control"/></p> <p>Users / Groups: <input style="width: 300px;" type="text" value="engineering"/></p> <p><small>Valid users and groups separated by a semicolon</small></p>

17. **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 em que o servidor CIFS irá ingressar.
Active Directory Domain para aderir	O FQDN do domínio do active Directory (AD) ao qual você deseja que o servidor CIFS se associe.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores à unidade organizacional especificada (ou) dentro do domínio do AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio AD.
Unidade organizacional	A unidade organizacional dentro do domínio AD a associar ao servidor CIFS. A predefinição é computadores. Se você configurar o AWS Managed Microsoft AD como o servidor AD para o Cloud Volumes ONTAP, deverá inserir neste campo ou computadores .
Domínio DNS	O domínio DNS da máquina virtual de storage (SVM) do Cloud Volumes ONTAP. Na maioria dos casos, o domínio é o mesmo que o domínio AD.
NTP Server	Selecione Use active Directory Domain para configurar um servidor NTP usando o DNS do active Directory. Se você precisa configurar um servidor NTP usando um endereço diferente, então você deve usar a API. Consulte "Documentos de automação BlueXP" para obter mais informações. Observe que você pode configurar um servidor NTP somente ao criar um servidor CIFS. Não é configurável depois de criar o servidor CIFS.

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

Para obter mais informações, consulte ["Compreender os perfis de utilização de volume"](#) ["Visão geral de](#)

categorização de dados", e "KB: Quais recursos de eficiência de armazenamento em linha são suportados pelo CVO?"

19. **Rever & aprovar:** Revise e confirme suas seleções.

- a. Reveja os detalhes sobre a configuração.
- b. Clique em **mais informações** para analisar detalhes sobre o suporte e os recursos da AWS que o BlueXP adquirirá.
- c. Selecione as caixas de verificação **I understand....**
- d. Clique em **Go**.

Resultado

O BlueXP inicia a instância do Cloud Volumes ONTAP. Você pode acompanhar o progresso na linha do tempo.

Se você tiver algum problema ao iniciar a instância do Cloud Volumes ONTAP, revise a mensagem de falha. Você também pode selecionar o ambiente de trabalho e clicar em recriar ambiente.

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

Depois de terminar

- Se você provisionou um compartilhamento CIFS, dê aos usuários ou grupos permissões para os arquivos e pastas e verifique se esses usuários podem acessar o compartilhamento e criar um arquivo.
- Se você quiser aplicar cotas a volumes, use o Gerenciador de sistema do ONTAP ou a CLI do ONTAP.

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

Lançamento de um par de HA do Cloud Volumes ONTAP na AWS

Para iniciar um par de HA da Cloud Volumes ONTAP na AWS, é necessário criar um ambiente de trabalho de HA no BlueXP .

Limitação

Neste momento, os pares de HA não são compatíveis com o AWS Outposts.

Sobre esta tarefa

Imediatamente após criar o ambiente de trabalho, o BlueXP inicia uma instância de teste na VPC especificada para verificar a conectividade. Se bem-sucedido, o BlueXP encerra imediatamente a instância e, em seguida, começa a implantar o sistema Cloud Volumes ONTAP. Se o BlueXP não puder verificar a conectividade, a criação do ambiente de trabalho falhará. A instância de teste é um T2.nano (para alocação de VPC padrão) ou m3.medium (para alocação de VPC dedicada).

Passos

1. No menu de navegação à esquerda, selecione **Storage > Canvas**.
2. Na página Canvas, clique em **Adicionar ambiente de trabalho** e siga as instruções.
3. **Escolha um local:** Selecione **Serviços da Amazon** e **Cloud Volumes ONTAP HA**.

Algumas zonas locais da AWS estão disponíveis.

Antes de usar as zonas locais da AWS, você deve habilitar zonas locais e criar uma sub-rede na zona

local da sua conta da AWS. Siga as etapas **Opt in to a AWS local Zone** e **Extend your Amazon VPC to the local Zone** no "[Tutorial da AWS "Introdução à implantação de aplicativos de baixa latência com zonas locais da AWS"](#)".

Se você estiver executando um conector versão 3.9.36 ou inferior, será necessário adicionar a seguinte permissão à função do AWS Connector no console AWS EC2: DescribeAvailabilityZones.

4. **Detalhes e credenciais:** Opcionalmente, altere as credenciais e a assinatura da AWS, insira um nome de ambiente de trabalho, adicione tags, se necessário, e insira uma senha.

Alguns dos campos desta página são auto-explicativos. A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Nome do ambiente de trabalho	O BlueXP usa o nome do ambiente de trabalho para nomear tanto o sistema Cloud Volumes ONTAP quanto a instância do Amazon EC2. Ele também usa o nome como prefixo para o grupo de segurança predefinido, se você selecionar essa opção.
Adicionar etiquetas	As tags AWS são metadados para seus recursos da AWS. O BlueXP adiciona as tags à instância do Cloud Volumes ONTAP e a cada recurso da AWS associado à instância. Você pode adicionar até quatro tags da interface do usuário ao criar um ambiente de trabalho e, em seguida, você pode adicionar mais após a criação. Observe que a API não limita a quatro tags ao criar um ambiente de trabalho. Para obter informações sobre tags, " Documentação da AWS: Marcando seus recursos do Amazon EC2 " consulte .
Nome de utilizador e palavra-passe	Estas são as credenciais da conta de administrador de cluster do Cloud Volumes ONTAP. Você pode usar essas credenciais para se conectar ao Cloud Volumes ONTAP por meio do Gerenciador de sistemas do ONTAP ou da CLI do ONTAP. Mantenha o nome de usuário padrão <i>admin</i> ou altere-o para um nome de usuário personalizado.
Editar credenciais	Escolha as credenciais da AWS e a assinatura do mercado a serem usadas com este sistema Cloud Volumes ONTAP. Clique em Adicionar assinatura para associar as credenciais selecionadas a uma nova assinatura do AWS Marketplace. A assinatura pode ser feita por um contrato anual ou para pagar por Cloud Volumes ONTAP a uma taxa por hora. Se você comprou uma licença diretamente da NetApp (traga sua própria licença (BYOL)), então uma assinatura da AWS não será necessária. " Saiba como adicionar credenciais adicionais da AWS ao BlueXP ".

O vídeo a seguir mostra como associar uma assinatura do Marketplace de pagamento conforme o uso às suas credenciais da AWS:

[Inscreva-se no BlueXP no AWS Marketplace](#)

Se vários usuários do IAM trabalharem na mesma conta da AWS, cada usuário precisará se inscrever. Depois que o primeiro usuário se inscreve, o AWS Marketplace informa aos usuários subsequentes que eles já estão inscritos, como mostrado na imagem abaixo. Enquanto uma assinatura está em vigor para a AWS *account*, cada usuário do IAM precisa se associar a essa assinatura. Se você vir a mensagem mostrada abaixo, clique no link **clique aqui** para acessar o site da BlueXP e concluir o processo.



Cloud Manager (for Cloud Volumes ONTAP)

You are currently subscribed to this product and will be charged for your accumulated usage at the end of your next billing cycle, based on the costs listed in Pricing information on the right.

Having issues signing up for your product?
If you were unable to complete the set-up process for this software, please [click here](#) to be taken to the product's registration area.

Subscribe

You are already subscribed to this product

Pricing Details

Software Fees

5. **Serviços:** Mantenha os serviços ativados ou desative os serviços individuais que você não deseja usar com este sistema Cloud Volumes ONTAP.

- ["Saiba mais sobre a classificação BlueXP"](#)
- ["Saiba mais sobre backup e recuperação do BlueXP "](#)



Se quiser utilizar WORM e disposição de dados em camadas, desative o backup e a recuperação do BlueXP e implante um ambiente de trabalho do Cloud Volumes ONTAP com a versão 9,8 ou superior.

6. **Modelos de implantação HA:** Escolha uma configuração de HA.

Para obter uma visão geral dos modelos de implantação, ["Cloud Volumes ONTAP HA para AWS"](#) consulte .

7. **Localização e conectividade** (AZ único) ou **região e VPC** (AZs múltiplos): Insira as informações de rede gravadas na Planilha da AWS.

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

Campo	Descrição
Grupo de segurança gerado	Se você permitir que o BlueXP gere o grupo de segurança para você, você precisa escolher como permitirá o tráfego: <ul style="list-style-type: none"> • Se você escolher somente VPC selecionada, a origem do tráfego de entrada será o intervalo de sub-rede da VPC selecionada e o intervalo de sub-rede da VPC onde o conector reside. Esta é a opção recomendada. • Se você escolher todos os VPCs, a origem do tráfego de entrada é o intervalo IP 0,0.0.0/0.
Use o grupo de segurança existente	Se utilizar uma política de firewall existente, certifique-se de que inclui as regras necessárias. "Saiba mais sobre as regras de firewall do Cloud Volumes ONTAP" .

8. **Conectividade e Autenticação SSH:** Escolha métodos de conexão para o par HA e o mediador.

9. **IPs flutuantes:** Se você escolher vários AZs, especifique os endereços IP flutuantes.

Os endereços IP devem estar fora do bloco CIDR para todos os VPCs da região. Para obter mais detalhes, ["Requisitos de rede da AWS para o Cloud Volumes ONTAP HA em vários AZs"](#) consulte .

10. **Tabelas de rotas:** Se você escolher vários AZs, selecione as tabelas de rotas que devem incluir rotas para os endereços IP flutuantes.

Se tiver mais de uma tabela de rotas, é muito importante selecionar as tabelas de rotas corretas. Caso contrário, alguns clientes podem não ter acesso ao par de HA do Cloud Volumes ONTAP. Para obter mais informações sobre tabelas de rotas, consulte ["Documentação da AWS: Tabelas de rotas"](#) a .

11. **Criptografia de dados:** Não escolha criptografia de dados ou criptografia gerenciada pela AWS.

Para criptografia gerenciada pela AWS, você pode escolher uma chave mestra do cliente (CMK) diferente da sua conta ou de outra conta da AWS.



Não é possível alterar o método de criptografia de dados da AWS depois de criar um sistema Cloud Volumes ONTAP.

["Saiba como configurar o AWS KMS para Cloud Volumes ONTAP"](#).

["Saiba mais sobre as tecnologias de criptografia suportadas"](#).

12. **Métodos de carregamento e conta NSS:** Especifique qual opção de carregamento você gostaria de usar com este sistema e especifique uma conta do site de suporte da NetApp.

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

13. **Configuração do Cloud Volumes ONTAP** (somente contrato anual do AWS Marketplace): Revise a configuração padrão e clique em **continuar** ou em **alterar configuração** para selecionar sua própria configuração.

Se você mantiver a configuração padrão, precisará especificar apenas um volume e, em seguida, revisar e aprovar a configuração.

14. **Pacotes pré-configurados** (somente por hora ou BYOL): Selecione um dos pacotes para iniciar rapidamente o Cloud Volumes ONTAP ou clique em **alterar configuração** para selecionar sua própria configuração.

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

15. **Função do IAM:** É melhor manter a opção padrão para permitir que o BlueXP crie a função para você.

Se você preferir usar sua própria política, ela deve atender ["Requisitos de política para nós de Cloud Volumes ONTAP e o mediador de HA"](#).

16. **Licenciamento:** Altere a versão do Cloud Volumes ONTAP conforme necessário e selecione um tipo de instância e a alocação de instância.



Se um candidato de lançamento mais recente, disponibilidade geral ou liberação de 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 9.13.1 e 9.13.1 P4 estiver disponível. A atualização não ocorre de uma versão para outra, por exemplo, de 9,13 a 9,14.

17. **Recursos de armazenamento subjacentes:** Escolha um tipo de disco, configure o armazenamento subjacente e escolha se deseja manter a disposição de dados ativada.

Observe o seguinte:

- O tipo de disco é para o volume inicial (e agregado). Você pode escolher um tipo de disco diferente para volumes subsequentes (e agregados).
- Se você escolher um disco de GP3 TB ou IO1 tb, o BlueXP usará o recurso volumes elásticos na AWS para aumentar automaticamente a capacidade de disco de storage subjacente conforme necessário. Você pode escolher a capacidade inicial com base nas suas necessidades de storage e revisá-la após a implantação do Cloud Volumes ONTAP. ["Saiba mais sobre o suporte a volumes elásticos na AWS"](#).
- Se você escolher um disco de GP2 TB ou st1 TB, poderá selecionar um tamanho de disco para todos os discos no agregado inicial e para quaisquer agregados adicionais criados pelo BlueXP ao usar a opção de provisionamento simples. Você pode criar agregados que usam um tamanho de disco diferente usando a opção Alocação avançada.
- Você pode escolher uma política específica de disposição em categorias de volume ao criar ou editar um volume.
- Se você desativar a disposição de dados em categorias, poderá ativá-la em agregados subsequentes.

["Saiba como funciona a disposição em camadas de dados"](#).

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

- a. Escolha **normal** ou **alta** velocidade de gravação, se desejado.

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

- b. Ative o storage WORM (uma gravação, muitas leituras), se desejado.

O WORM não pode ser ativado se a disposição de dados em camadas foi ativada para o Cloud Volumes ONTAP versões 9,7 e inferiores. Reverter ou fazer downgrade para o Cloud Volumes ONTAP 9,8 é bloqueado depois de ativar WORM e disposição em camadas.

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

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

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

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

Alguns dos campos desta página são auto-explicativos. A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Tamanho	O tamanho máximo que você pode inserir depende, em grande parte, se você ativar o provisionamento de thin, o que permite criar um volume maior do que o armazenamento físico atualmente disponível para ele.
Controle de acesso (somente para NFS)	Uma política de exportação define os clientes na sub-rede que podem acessar o volume. Por padrão, o BlueXP insere um valor que fornece acesso a todas as instâncias na sub-rede.

Campo	Descrição
Permissões e utilizadores/grupos (apenas para CIFS)	Esses campos permitem controlar o nível de acesso a um compartilhamento para usuários e grupos (também chamados de listas de controle de acesso ou ACLs). Você pode especificar usuários ou grupos do Windows locais ou de domínio, ou usuários ou grupos UNIX. Se você especificar um nome de usuário do domínio do Windows, você deve incluir o domínio do usuário usando o nome de domínio do formato.
Política de instantâneos	Uma política de cópia Snapshot especifica a frequência e o número de cópias snapshot do NetApp criadas automaticamente. Uma cópia Snapshot do NetApp é uma imagem pontual do sistema de arquivos que não afeta a performance e exige o mínimo de storage. Você pode escolher a política padrão ou nenhuma. Você pode escolher nenhum para dados transitórios: Por exemplo, tempdb para Microsoft SQL Server.
Opções avançadas (somente para NFS)	Selecione uma versão NFS para o volume: NFSv3 ou NFSv4.
Grupo de iniciadores e IQN (apenas para iSCSI)	Os destinos de armazenamento iSCSI são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Os grupos de iniciadores são tabelas de nomes de nós de host iSCSI e controlam quais iniciadores têm acesso a quais LUNs. Os destinos iSCSI se conectam à rede por meio de adaptadores de rede Ethernet (NICs) padrão, placas de mecanismo de descarga TCP (TOE) com iniciadores de software, adaptadores de rede convergidos (CNAs) ou adaptadores de barramento de host dedicados (HBAs) e são identificados por IQNs (iSCSI Qualified Names). Quando cria um volume iSCSI, o BlueXP cria automaticamente um LUN para si. Simplificamos a criação de apenas um LUN por volume, para que não haja gerenciamento envolvido. Depois de criar o volume, "Use o IQN para se conectar ao LUN a partir de seus hosts" .

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

Volume Details, Protection & Protocol

Details & Protection

Volume Name: Size (GB):

Snapshot Policy:

Default Policy

Protocol

NFS
 CIFS
 iSCSI

Share name: Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

20. **Configuração CIFS:** Se você selecionou o protocolo CIFS, configure um servidor CIFS.

Campo	Descrição
Endereço IP primário e secundário do DNS	Os endereços IP dos servidores DNS que fornecem resolução de nomes para o servidor CIFS. Os servidores DNS listados devem conter os Registros de localização de serviço (SRV) necessários para localizar os servidores LDAP do Active Directory e os controladores de domínio para o domínio em que o servidor CIFS irá ingressar.
Active Directory Domain para aderir	O FQDN do domínio do Active Directory (AD) ao qual você deseja que o servidor CIFS se associe.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores à unidade organizacional especificada (ou) dentro do domínio do AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio AD.
Unidade organizacional	A unidade organizacional dentro do domínio AD a associar ao servidor CIFS. A predefinição é computadores. Se você configurar o AWS Managed Microsoft AD como o servidor AD para o Cloud Volumes ONTAP, deverá inserir neste campo ou computadores .
Domínio DNS	O domínio DNS da máquina virtual de storage (SVM) do Cloud Volumes ONTAP. Na maioria dos casos, o domínio é o mesmo que o domínio AD.
NTP Server	Selecione Use Active Directory Domain para configurar um servidor NTP usando o DNS do Active Directory. Se você precisa configurar um servidor NTP usando um endereço diferente, então você deve usar a API. Consulte " Documentos de automação BlueXP " para obter mais informações. Observe que você pode configurar um servidor NTP somente ao criar um servidor CIFS. Não é configurável depois de criar o servidor CIFS.

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

Para obter mais informações, "[Escolha um perfil de uso de volume](#)" consulte e "[Visão geral de categorização de dados](#)".

22. **Rever & aprovar:** Revise e confirme suas seleções.

- Reveja os detalhes sobre a configuração.
- Clique em **mais informações** para analisar detalhes sobre o suporte e os recursos da AWS que o BlueXP adquirirá.
- Selecione as caixas de verificação **I understand...**
- Clique em **Go**.

Resultado

A BlueXP lança o par de HA da Cloud Volumes ONTAP. Você pode acompanhar o progresso na linha do tempo.

Se tiver algum problema ao iniciar o par de HA, reveja a mensagem de falha. Você também pode selecionar o ambiente de trabalho e clicar em recriar ambiente.

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

Depois de terminar

- Se você provisionou um compartilhamento CIFS, dê aos usuários ou grupos permissões para os arquivos e pastas e verifique se esses usuários podem acessar o compartilhamento e criar um arquivo.
- Se você quiser aplicar cotas a volumes, use o Gerenciador de sistema do ONTAP ou a CLI do ONTAP.

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

Implante o Cloud Volumes ONTAP nas regiões da nuvem secreta da AWS e das principais regiões da nuvem secreta

Semelhante a uma região padrão da AWS, você pode usar o BlueXP in "[Nuvem secreta da AWS](#)" e in "[Nuvem secreta principal da AWS](#)" para implantar o Cloud Volumes ONTAP, que fornece recursos de classe empresarial para o seu storage de nuvem. A nuvem secreta da AWS e a nuvem secreta principal são regiões fechadas específicas para a Comunidade de Inteligência dos EUA; as instruções nesta página aplicam-se apenas aos usuários da região da nuvem secreta da AWS e da nuvem secreta principal.

Antes de começar

Antes de começar, consulte as versões suportadas na nuvem secreta da AWS e na nuvem secreta principal e saiba mais sobre o modo privado no BlueXP .

- Consulte as seguintes versões suportadas na nuvem secreta da AWS e na nuvem secreta principal:
 - Cloud Volumes ONTAP 9.12.1 P2
 - Versão 3.9.32 do conetor

O conetor é um software necessário para implantar e gerenciar o Cloud Volumes ONTAP na AWS. Você fará login no BlueXP a partir do software que é instalado na instância do Connector. O site SaaS da BlueXP não é compatível com a nuvem secreta da AWS e a nuvem secreta principal.

- Saiba mais sobre o modo privado

Na nuvem secreta da AWS e na nuvem secreta principal, o BlueXP opera em *modo privado*. No modo privado, não há conectividade com a camada SaaS do BlueXP . Os usuários acessam o BlueXP localmente a partir do console baseado na Web que está disponível no conetor, não na camada SaaS.

Para saber mais sobre como o modo privado funciona, "[Modo de implantação privada do BlueXP](#)" consulte

Passo 1: Configure sua rede

Configure sua rede da AWS para que o Cloud Volumes ONTAP possa funcionar corretamente.

Passos

1. Escolha a VPC e as sub-redes nas quais você deseja iniciar a instância do Connector e as instâncias do Cloud Volumes ONTAP.
2. Certifique-se de que a VPC e as sub-redes suportem a conectividade entre o conetor e o Cloud Volumes ONTAP.
3. Configure um endpoint de VPC para o serviço S3.

Um endpoint de VPC é necessário se você quiser categorizar dados inativos do Cloud Volumes ONTAP para storage de objetos de baixo custo.

Passo 2: Configurar permissões

Configure as políticas e funções do IAM que fornecem ao Connector e ao Cloud Volumes ONTAP as permissões necessárias para executar ações na nuvem secreta da AWS ou na nuvem secreta principal.

Você precisa de uma política do IAM e de uma função do IAM para cada uma das seguintes opções:

- A instância do conetor
- Instâncias do Cloud Volumes ONTAP
- Para pares de HA, a instância de mediador do Cloud Volumes ONTAP HA (se você quiser implantar pares de HA)

Passos

1. Vá para o console do AWS IAM e clique em **políticas**.
2. Crie uma política para a instância do conetor.



Você cria essas políticas para dar suporte aos buckets do S3 no seu ambiente AWS. Ao criar os buckets mais tarde, certifique-se de que os nomes dos buckets sejam prefixados com `fabric-pool-`. Esse requisito se aplica às regiões da nuvem secreta da AWS e da nuvem secreta principal.

Regiões secretas

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceStatus",
      "ec2:RunInstances",
      "ec2:ModifyInstanceAttribute",
      "ec2:DescribeRouteTables",
      "ec2:DescribeImages",
      "ec2:CreateTags",
      "ec2:CreateVolume",
      "ec2:DescribeVolumes",
      "ec2:ModifyVolumeAttribute",
      "ec2>DeleteVolume",
      "ec2:CreateSecurityGroup",
      "ec2>DeleteSecurityGroup",
      "ec2:DescribeSecurityGroups",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:CreateNetworkInterface",
      "ec2:DescribeNetworkInterfaces",
      "ec2>DeleteNetworkInterface",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeDhcpOptions",
      "ec2:CreateSnapshot",
      "ec2>DeleteSnapshot",
      "ec2:DescribeSnapshots",
      "ec2:GetConsoleOutput",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeRegions",
      "ec2>DeleteTags",
      "ec2:DescribeTags",
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:DescribeStacks",
      "cloudformation:DescribeStackEvents",
      "cloudformation:ValidateTemplate",
      "iam:PassRole",
```

```

        "iam:CreateRole",
        "iam>DeleteRole",
        "iam:PutRolePolicy",
        "iam:ListInstanceProfiles",
        "iam:CreateInstanceProfile",
        "iam>DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam>DeleteInstanceProfile",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "kms:List*",
        "kms:Describe*",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2>DeletePlacementGroup"
    ],
    "Resource": "*"
},
{
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
        "s3>DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
    ],
    "Resource": [
        "arn:aws-iso-b:s3:::fabric-pool*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",

```

```

        "ec2:DetachVolume"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/WorkingEnvironment": "*"
        }
    },
    "Resource": [
        "arn:aws-iso-b:ec2:*:*:instance/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Resource": [
        "arn:aws-iso-b:ec2:*:*:volume/*"
    ]
}
]
}

```

Top regiões secretas

```

{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeInstances",
            "ec2:DescribeInstanceStatus",
            "ec2:RunInstances",
            "ec2:ModifyInstanceAttribute",
            "ec2:DescribeRouteTables",
            "ec2:DescribeImages",
            "ec2:CreateTags",
            "ec2:CreateVolume",
            "ec2:DescribeVolumes",
            "ec2:ModifyVolumeAttribute",
            "ec2>DeleteVolume",
            "ec2:CreateSecurityGroup",
            "ec2>DeleteSecurityGroup",
            "ec2:DescribeSecurityGroups",
            "ec2:RevokeSecurityGroupEgress",

```

```
"ec2:RevokeSecurityGroupIngress",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:CreateNetworkInterface",
"ec2:DescribeNetworkInterfaces",
"ec2>DeleteNetworkInterface",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:DescribeSubnets",
"ec2:DescribeVpcs",
"ec2:DescribeDhcpOptions",
"ec2:CreateSnapshot",
"ec2>DeleteSnapshot",
"ec2:DescribeSnapshots",
"ec2:GetConsoleOutput",
"ec2:DescribeKeyPairs",
"ec2:DescribeRegions",
"ec2>DeleteTags",
"ec2:DescribeTags",
"cloudformation:CreateStack",
"cloudformation>DeleteStack",
"cloudformation:DescribeStacks",
"cloudformation:DescribeStackEvents",
"cloudformation:ValidateTemplate",
"iam:PassRole",
"iam:CreateRole",
"iam>DeleteRole",
"iam:PutRolePolicy",
"iam:ListInstanceProfiles",
"iam:CreateInstanceProfile",
"iam>DeleteRolePolicy",
"iam:AddRoleToInstanceProfile",
"iam:RemoveRoleFromInstanceProfile",
"iam>DeleteInstanceProfile",
"s3:GetObject",
"s3:ListBucket",
"s3:GetBucketTagging",
"s3:GetBucketLocation",
"s3:ListAllMyBuckets",
"kms:List*",
"kms:Describe*",
"ec2:AssociateIamInstanceProfile",
"ec2:DescribeIamInstanceProfileAssociations",
"ec2:DisassociateIamInstanceProfile",
"ec2:DescribeInstanceAttribute",
"ec2:CreatePlacementGroup",
"ec2>DeletePlacementGroup"
```

```

    ],
    "Resource": "*"
  },
  {
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
      "s3:DeleteBucket",
      "s3:GetLifecycleConfiguration",
      "s3:PutLifecycleConfiguration",
      "s3:PutBucketTagging",
      "s3:ListBucketVersions"
    ],
    "Resource": [
      "arn:aws-iso:s3:::fabric-pool*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:StartInstances",
      "ec2:StopInstances",
      "ec2:TerminateInstances",
      "ec2:AttachVolume",
      "ec2:DetachVolume"
    ],
    "Condition": {
      "StringLike": {
        "ec2:ResourceTag/WorkingEnvironment": "*"
      }
    },
    "Resource": [
      "arn:aws-iso:ec2:*:*:instance/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:AttachVolume",
      "ec2:DetachVolume"
    ],
    "Resource": [
      "arn:aws-iso:ec2:*:*:volume/*"
    ]
  }
]

```

```
}
```

3. Crie uma política para o Cloud Volumes ONTAP.

Regiões secretas

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws-iso-b:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3>DeleteObject"
    ],
    "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
    "Effect": "Allow"
  }
]
```

Top regiões secretas

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws-iso:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws-iso:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3>DeleteObject"
    ],
    "Resource": "arn:aws-iso:s3:::fabric-pool-*",
    "Effect": "Allow"
  }]
}

```

Para pares de HA, se você planeja implantar um par de HA do Cloud Volumes ONTAP, crie uma política para o mediador de HA.

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:AssignPrivateIpAddresses",
      "ec2:CreateRoute",
      "ec2>DeleteRoute",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeRouteTables",
      "ec2:DescribeVpcs",
      "ec2:ReplaceRoute",
      "ec2:UnassignPrivateIpAddresses"
    ],
    "Resource": "*"
  }
]
}

```

4. Crie funções do IAM com o tipo de função Amazon EC2 e anexe as políticas criadas nas etapas anteriores.

Crie a função:

Semelhante às políticas, você deve ter uma função do IAM para o conetor e uma para os nós do Cloud Volumes ONTAP. Para pares de HA: Assim como as políticas, você deve ter uma função do IAM para o conetor, uma para os nós Cloud Volumes ONTAP e uma para o mediador de HA (se quiser implantar pares de HA).

Selecione a função:

Você deve selecionar a função do IAM do conetor quando iniciar a instância do conetor. Você pode selecionar as funções do IAM para o Cloud Volumes ONTAP ao criar um ambiente de trabalho do Cloud Volumes ONTAP no BlueXP . Para pares de HA, você pode selecionar as funções do IAM para o Cloud Volumes ONTAP e o mediador de HA ao criar um ambiente de trabalho do Cloud Volumes ONTAP no BlueXP .

Etapa 3: Configurar o AWS KMS

Se você quiser usar a criptografia da Amazon com o Cloud Volumes ONTAP, verifique se os requisitos são atendidos para o Serviço de Gerenciamento de chaves da AWS (KMS).

Passos

1. Certifique-se de que existe uma chave mestra do cliente (CMK) ativa na sua conta ou em outra conta da AWS.

O CMK pode ser um CMK gerenciado pela AWS ou um CMK gerenciado pelo cliente.

2. Se o CMK estiver em uma conta da AWS separada da conta em que você planeja implantar o Cloud Volumes ONTAP, você precisará obter o ARN dessa chave.

Você precisará fornecer o ARN ao BlueXP ao criar o sistema Cloud Volumes ONTAP.

3. Adicione a função do IAM para a instância do Connector à lista de usuários-chave de um CMK.

Isso dá permissões BlueXP para usar o CMK com Cloud Volumes ONTAP.

Passo 4: Instale o conetor e configure o BlueXP

Antes de começar a usar o BlueXP para implantar o Cloud Volumes ONTAP na AWS, você deve instalar e configurar o BlueXP Connector. O conetor permite que o BlueXP gerencie recursos e processos em seu ambiente de nuvem pública (isso inclui o Cloud Volumes ONTAP).

Passos

1. Obtenha um certificado raiz assinado por uma autoridade de certificação (CA) no formato X.509 codificado com base em Email Avançado de Privacidade (PEM) 64. Consulte as políticas e procedimentos da sua organização para obter o certificado.



Para regiões da nuvem secreta da AWS, você deve fazer o upload do NSS Root CA 2 certificado e, para a nuvem secreta superior, o Amazon Root CA 4 certificado. Certifique-se de carregar apenas estes certificados e não toda a cadeia. O arquivo para a cadeia de certificados é grande e o upload pode falhar. Se você tiver certificados adicionais, você pode carregá-los mais tarde, como descrito na próxima etapa.

Você precisará fazer o upload do certificado durante o processo de configuração. O BlueXP usa o certificado confiável ao enviar solicitações para a AWS por HTTPS.

2. Inicie a instância do conetor:
 - a. Acesse a página do mercado da Comunidade de Inteligência da AWS para o BlueXP.
 - b. Na guia Lançamento Personalizado, escolha a opção para iniciar a instância no console EC2.
 - c. Siga as instruções para configurar a instância.

Observe o seguinte ao configurar a instância:

- Recomendamos T3.xlarge.
- Você deve escolher a função do IAM que você criou ao configurar permissões.
- Você deve manter as opções de armazenamento padrão.
- Os métodos de conexão necessários para o conetor são os seguintes: SSH, HTTP e HTTPS.

3. Configure o BlueXP a partir de um host que tenha uma conexão com a instância do conetor:
 - a. Abra um navegador da Web e digite `https://ipaddress` onde `ipaddress` é o endereço IP do host Linux onde você instalou o conetor.
 - b. Especifique um servidor proxy para conectividade com os serviços da AWS.
 - c. Carregue o certificado obtido na etapa 1.
 - d. Selecione **Configurar novo BlueXP** e siga as instruções para configurar o sistema.
 - **Detalhes do sistema:** Insira um nome para o conetor e o nome da sua empresa.
 - **Criar usuário Admin:** Crie o usuário admin para o sistema.

Esta conta de utilizador é executada localmente no sistema. Não há conexão com o serviço auth0

disponível através do BlueXP .

- **Revisão:** Revise os detalhes, aceite o contrato de licença e selecione **Configurar**.

- e. Para concluir a instalação do certificado assinado pela CA, reinicie a instância do conector a partir do console EC2.
4. Depois que o conector for reiniciado, faça login usando a conta de usuário do administrador criada no assistente de configuração.

Passo 5: (Opcional) instale um certificado de modo privado

Esta etapa é opcional para as regiões da AWS Secret Cloud e Top Secret Cloud e é necessária somente se você tiver certificados adicionais além dos certificados raiz instalados na etapa anterior.

Passos

1. Listar os certificados instalados existentes.
 - a. Para coletar o ID do docker do contentor occm (nome identificado "ds-occm-1"), execute o seguinte comando:

```
docker ps
```

- b. Para entrar no contentor occm, execute o seguinte comando:

```
docker exec -it <docker-id> /bin/sh
```

- c. Para coletar a senha da variável de ambiente "TRUST_STORE_password", execute o seguinte comando:

```
env
```

- d. Para listar todos os certificados instalados no truststore, execute o seguinte comando e use a senha coletada na etapa anterior:

```
keytool -list -v -keystore occm.truststore
```

2. Adicione um certificado.

- a. Para coletar o ID do docker do contentor occm (nome identificado "ds-occm-1"), execute o seguinte comando:

```
docker ps
```

- b. Para entrar no contentor occm, execute o seguinte comando:

```
docker exec -it <docker-id> /bin/sh
```

Salve o novo arquivo de certificado dentro.

- c. Para coletar a senha da variável de ambiente "TRUST_STORE_password", execute o seguinte comando:

```
env
```

- d. Para adicionar o certificado ao armazenamento confiável, execute o seguinte comando e use a senha da etapa anterior:

```
keytool -import -alias <alias-name> -file <certificate-file-name>  
-keystore occm.truststore
```

- e. Para verificar se o certificado foi instalado, execute o seguinte comando:

```
keytool -list -v -keystore occm.truststore -alias <alias-name>
```

- f. Para sair do contentor de occm, execute o seguinte comando:

```
exit
```

- g. Para redefinir o contentor de occm, execute o seguinte comando:

```
docker restart <docker-id>
```

Passo 6: Adicione uma licença à carteira digital BlueXP

Se você comprou uma licença da NetApp, precisará adicioná-la à carteira digital da BlueXP para que possa selecionar a licença ao criar um novo sistema Cloud Volumes ONTAP. A carteira digital identifica essas licenças como não atribuídas.

Passos

1. No menu de navegação BlueXP, selecione **Governança > carteira digital**.
2. Na guia **Cloud Volumes ONTAP**, selecione **licenças baseadas em nós** na lista suspensa.
3. Clique em **Unassigned**.
4. Clique em **Adicionar licenças não atribuídas**.
5. Introduza o número de série da licença ou carregue o ficheiro da licença.
6. Se ainda não tiver o ficheiro de licença, terá de carregar manualmente o ficheiro de licença a partir do NetApp.com.

- a. Acesse ao "[Gerador de arquivos de licença NetApp](#)" e inicie sessão utilizando as suas credenciais do site de suporte da NetApp.
- b. Introduza a sua palavra-passe, escolha o seu produto, introduza o número de série, confirme que leu e aceitou a política de privacidade e, em seguida, clique em **Enviar**.
- c. Escolha se você deseja receber o arquivo JSON serialnumber.NLF por e-mail ou download direto.

7. Clique em **Adicionar licença**.

Resultado

O BlueXP adiciona a licença à carteira digital. A licença será identificada como não atribuída até que você a associe a um novo sistema Cloud Volumes ONTAP. Depois que isso acontece, a licença passa para a guia BYOL na carteira digital.

Passo 7: Inicie o Cloud Volumes ONTAP a partir do BlueXP

Você pode iniciar instâncias do Cloud Volumes ONTAP na nuvem secreta da AWS e na nuvem secreta criando novos ambientes de trabalho no BlueXP .

Antes de começar

Para pares de HA, é necessário um par de chaves para habilitar a autenticação SSH baseada em chave para o mediador de HA.

Passos

1. Na página ambientes de trabalho, clique em **Adicionar ambiente de trabalho**.
2. Em **criar**, selecione Cloud Volumes ONTAP.

Para HA: Em **Create**, selecione Cloud Volumes ONTAP ou Cloud Volumes ONTAP HA.

3. Conclua as etapas no assistente para iniciar o sistema Cloud Volumes ONTAP.



Ao fazer seleções através do assistente, não selecione **Data Sense & Compliance** e **Backup to Cloud** em **Serviços**. Em **Pacotes pré-configurados**, selecione **alterar configuração** somente e certifique-se de que não selecionou nenhuma outra opção. Pacotes pré-configurados não são suportados nas regiões da AWS Secret Cloud e Top Secret Cloud e, se selecionado, sua implantação falhará.

Notas para implantar o Cloud Volumes ONTAP HA em várias zonas de disponibilidade

Observe o seguinte ao concluir o assistente para pares de HA.

- Você deve configurar um gateway de trânsito quando implantar o Cloud Volumes ONTAP HA em várias zonas de disponibilidade (AZs). Para obter instruções, "[Configure um gateway de trânsito da AWS](#)" consulte .
- Implemente a configuração como a seguir, porque apenas dois AZs estavam disponíveis na nuvem secreta principal da AWS no momento da publicação:
 - Nó 1: Zona de disponibilidade A
 - Nó 2: Zona de disponibilidade B
 - Mediador: Zona de disponibilidade A ou B

Notas para implantar o Cloud Volumes ONTAP em nós único e de HA

Observe o seguinte ao concluir o assistente:

- Você deve deixar a opção padrão para usar um grupo de segurança gerado.

O grupo de segurança predefinido inclui as regras que o Cloud Volumes ONTAP precisa para operar com êxito. Se você tiver um requisito para usar o seu próprio, você pode consultar a seção do grupo de segurança abaixo.

- Você deve escolher a função do IAM que criou ao preparar seu ambiente AWS.
- O tipo de disco subjacente da AWS é para o volume inicial do Cloud Volumes ONTAP.

Você pode escolher um tipo de disco diferente para volumes subsequentes.

- O desempenho dos discos da AWS está vinculado ao tamanho do disco.

Você deve escolher o tamanho de disco que ofereça a performance contínua de que precisa. Consulte a documentação da AWS para obter mais detalhes sobre o desempenho do EBS.

- O tamanho do disco é o tamanho padrão para todos os discos no sistema.



Se você precisar de um tamanho diferente mais tarde, você pode usar a opção Alocação avançada para criar um agregado que use discos de um tamanho específico.

Resultado

O BlueXP inicia a instância do Cloud Volumes ONTAP. Você pode acompanhar o progresso na linha do tempo.

Etapa 8: Instalar certificados de segurança para categorização de dados

Você precisa instalar manualmente certificados de segurança para habilitar a disposição em camadas de dados nas regiões da AWS Secret Cloud e Top Secret Cloud.

Antes de começar

1. Crie buckets do S3.



Certifique-se de que os nomes do bucket estão prefixados com `fabric-pool-`, por `fabric-pool-testbucket` exemplo, .

2. Mantenha os certificados raiz que você instalou `step 4` a calhar.

Passos

1. Copie o texto dos certificados raiz instalados no `step 4`.
2. Conecte-se com segurança ao sistema Cloud Volumes ONTAP usando a CLI.
3. Instale os certificados raiz. Talvez seja necessário pressionar a `ENTER` tecla várias vezes:

```
security certificate install -type server-ca -cert-name <certificate-name>
```

4. Quando solicitado, insira todo o texto copiado, incluindo e de `----- BEGIN CERTIFICATE -----` para `----- END CERTIFICATE -----`.

5. Mantenha uma cópia do certificado digital assinado pela CA para referência futura.
6. Guarde o nome da CA e o número de série do certificado.
7. Configure o armazenamento de objetos para as regiões da AWS Secret Cloud e da Top Secret Cloud: `set -privilege advanced -confirmations off`
8. Execute este comando para configurar o armazenamento de objetos.



Todos os nomes de recursos do Amazon (Arns) devem ser sufixos com `-iso-b`, `arn:aws-iso-b` como `.` Por exemplo, se um recurso exigir um ARN com uma região, para a nuvem secreta superior, use a convenção de nomenclatura como `us-iso-b` para a `-server` bandeira. Para a nuvem secreta da AWS, use ``us-iso-b-1`o`.

```
storage aggregate object-store config create -object-store-name
<S3Bucket> -provider-type AWS_S3 -auth-type EC2-IAM -server <s3.us-iso-
b-1.server_name> -container-name <fabric-pool-testbucket> -is-ssl
-enabled true -port 443
```

9. Verifique se o armazenamento de objetos foi criado com sucesso: `storage aggregate object-store show -instance`
10. Anexe o armazenamento de objetos ao agregado. Isso deve ser repetido para cada novo agregado: `storage aggregate object-store attach -aggregate <aggr1> -object-store-name <S3Bucket>`

Comece a usar o Microsoft Azure

Início rápido para Cloud Volumes ONTAP no Azure

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

1

Crie um conetor

Se você ainda não tem um "Conetor", você precisa criar um. ["Saiba como criar um conetor no Azure"](#)

Observe que, se você quiser implantar o Cloud Volumes ONTAP em uma sub-rede onde não há acesso à Internet disponível, precisará instalar manualmente o conetor e acessar a interface de usuário do BlueXP que está sendo executada nesse conetor. ["Saiba como instalar manualmente o conetor em um local sem acesso à Internet"](#)

2

Planeje sua configuração

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

3

Configure a rede

1. Certifique-se de que o VNet e as sub-redes suportarão a conectividade entre o conector e o Cloud Volumes ONTAP.
2. Ative o acesso de saída à Internet a partir da VPC de destino para 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 usando o BlueXP

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

Links relacionados

- ["Criando um conector a partir do BlueXP "](#)
- ["Criando um conector a partir do Azure Marketplace"](#)
- ["Instalar o software Connector em um host Linux"](#)
- ["O que o BlueXP faz com 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 requisitos de workload ou criar sua própria configuração. Se você escolher sua própria configuração, você deve entender as opções disponíveis para você.

Escolha uma licença 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 para o Cloud Volumes ONTAP"](#)
- ["Saiba como configurar o licenciamento"](#)

Escolha uma região suportada

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 suporta vários tipos de VM, dependendo do tipo de licença escolhido.

["Configurações compatíveis com o Cloud Volumes ONTAP no Azure"](#)

Entenda os limites de armazenamento

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

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

Dimensione seu sistema no Azure

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

Tipo de máquina virtual

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

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

Tipo de disco Azure com sistemas de nó único

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

Os sistemas de nó único podem usar esses tipos de discos gerenciados do Azure:

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

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

Tipo de disco Azure com pares de HA

Os SISTEMAS HA usam discos gerenciados compartilhados SSD premium que oferecem alto desempenho para workloads com uso intenso de e/S a um custo mais alto. As implantações DE HA criadas antes da versão 9.12.1 usam blobs de página Premium.

Tamanho do disco do Azure

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



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

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

O desempenho do armazenamento Premium do Azure está vinculado ao tamanho do disco. Discos maiores fornecem IOPS e taxa de transferência mais altas. Por exemplo, a escolha de discos TIB de 1 TB pode fornecer melhor desempenho do que discos GiB de 500 TB, 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 que você precisa.

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

- ["Microsoft Azure: Preços de discos gerenciados"](#)
- ["Microsoft Azure: Preços de Blobs de páginas"](#)

Exibir discos do sistema padrão

Além do storage para dados de usuário, a BlueXP também compra storage de nuvem para dados de sistema do Cloud Volumes ONTAP (dados de inicialização, dados de raiz, dados básicos e NVRAM). Para fins de Planejamento, pode ajudar você a analisar esses detalhes antes de implantar o Cloud Volumes ONTAP.

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



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

Colete 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 as informações do administrador.

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

Escolha uma velocidade de gravação

O BlueXP 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 e os riscos e recomendações ao usar alta velocidade de gravação. ["Saiba mais sobre a velocidade de escrita"](#).

Escolha um perfil de uso de volume

O ONTAP inclui vários recursos de eficiência de storage que podem reduzir a quantidade total de storage de que você precisa. Ao criar um volume no BlueXP, você pode escolher um perfil que ative esses recursos ou

um perfil que os desabilite. Você deve aprender mais sobre esses recursos para ajudá-lo a decidir qual perfil usar.

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

Thin Provisioning

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

Deduplicação

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

Compactação

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

Requisitos de rede para o Cloud Volumes ONTAP no Azure

Configure sua rede Azure para que os sistemas Cloud Volumes ONTAP possam funcionar corretamente.

Requisitos para o Cloud Volumes ONTAP

Os seguintes requisitos de rede devem ser atendidos no Azure.

Acesso de saída à Internet

Os nós de Cloud Volumes ONTAP requerem acesso de saída à Internet para acessar endpoints externos para várias funções. O Cloud Volumes ONTAP não pode funcionar corretamente se esses endpoints forem bloqueados em ambientes com requisitos rígidos de segurança.

Pontos de extremidade Cloud Volumes ONTAP

O Cloud Volumes ONTAP requer acesso de saída à Internet para contactar vários endpoints para operações diárias.

Os seguintes endpoints são específicos do Cloud Volumes ONTAP. O conector também entra em Contato com vários endpoints para operações diárias, bem como com o console baseado na Web do BlueXP . ["Veja os pontos finais contactados a partir do conector"](#)Consulte e ["Prepare a rede para usar o console BlueXP "](#).

Endpoints	Aplicável para	Finalidade	Modos de implantação do BlueXP	Impacto se não estiver disponível
https://NetApp-cloud-account.auth0.com	Autenticação	Usado para autenticação BlueXP .	Modos padrão e restritos.	A autenticação do usuário falha e os seguintes serviços permanecem indisponíveis: <ul style="list-style-type: none"> • Serviços da Cloud Volumes ONTAP • Serviços da ONTAP • Protocolos e serviços proxy
https://keyvault-production-aks.vault.azure.net	Cofre de chaves	Usado para recuperar a chave secreta do cliente do Azure Key Vault para se comunicar com buckets do S3 para manipulação de metadados. O serviço Cloud Volumes ONTAP usa esse componente internamente.	Modos padrão, restrito e privado.	Os serviços Cloud Volumes ONTAP não estão disponíveis.
https://cloudmanager.cloud.NetApp.com/locação	Alocação	Usado para recuperar os recursos do Cloud Volumes ONTAP da BlueXP Locancy para autorizar recursos e usuários.	Modos padrão e restritos.	Os recursos do Cloud Volumes ONTAP e os usuários não estão autorizados.
https://support.NetApp.com/aods/asupmessage https://support.NetApp.com/asupprod/post/1,0/postAsup	AutoSupport	Usado para enviar dados de telemetria do AutoSupport para o suporte do NetApp.	Modos padrão e restritos.	As informações do AutoSupport permanecem não entregues.

Endpoints	Aplicável para	Finalidade	Modos de implantação do BlueXP	Impacto se não estiver disponível
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Regiões públicas	Comunicação com os serviços do Azure.	Modos padrão, restrito e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço Azure para executar operações específicas do BlueXP no Azure.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Região da China	Comunicação com os serviços do Azure.	Modos padrão, restrito e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço Azure para executar operações específicas do BlueXP no Azure.
https://management.microsoftazure.de https://login.microsoftonline.de https://blob.core.cloudapi.de https://core.cloudapi.de	Região da Alemanha	Comunicação com os serviços do Azure.	Modos padrão, restrito e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço Azure para executar operações específicas do BlueXP no Azure.
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	Regiões governamentais dos EUA	Comunicação com os serviços do Azure.	Modos padrão, restrito e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço Azure para executar operações específicas do BlueXP no Azure.
https://management.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud	Governo das regiões DoD	Comunicação com os serviços do Azure.	Modos padrão, restrito e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço Azure para executar operações específicas do BlueXP no Azure.

Acesso de saída à Internet para NetApp AutoSupport

Os nós do Cloud Volumes ONTAP exigem acesso de saída à Internet para NetApp AutoSupport, que monitora proativamente a integridade do sistema e envia mensagens para o suporte técnico da NetApp.

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

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

Se uma conexão de saída à Internet não estiver disponível para enviar mensagens AutoSupport, o BlueXP configura automaticamente seus sistemas Cloud Volumes ONTAP para usar o conector como um servidor proxy. O único requisito é garantir que o grupo de segurança do conector permita conexões *inbound* pela porta 3128. Você precisará abrir essa porta depois de implantar o conector.

Se você definiu regras de saída rígidas para o Cloud Volumes ONTAP, também precisará garantir que o grupo de segurança do Cloud Volumes ONTAP permita conexões *de saída* pela porta 3128.

Depois de verificar que o acesso de saída à Internet está disponível, você pode testar o AutoSupport para garantir que ele possa enviar mensagens. Para obter instruções, "[ONTAP docs: Configurar o AutoSupport](#)" consulte .

Se o BlueXP notificar que as mensagens do AutoSupport não podem ser enviadas, "[Solucionar problemas da configuração do AutoSupport](#)".

Endereços IP

O BlueXP aloca automaticamente o número necessário de endereços IP privados para o Cloud Volumes ONTAP no Azure. Você precisa garantir que sua rede tenha endereços IP privados suficientes disponíveis.

O número de LIFs alocadas pelo BlueXP para Cloud Volumes ONTAP depende da implantação de um único sistema de nós ou de um par de HA. Um LIF é um endereço IP associado a uma porta física. É necessário um LIF de gerenciamento de SVM para ferramentas de gerenciamento como o SnapCenter.



Um iSCSI LIF fornece acesso ao cliente através do protocolo iSCSI e é utilizado pelo sistema para outros fluxos de trabalho de rede importantes. Estes LIFs são necessários e não devem ser excluídos.

Endereços IP para um sistema de nó único

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

- IP de gerenciamento de cluster
- IP de gerenciamento de nós
- IP entre clusters para SnapMirror
- IP NFS/CIFS
- IP iSCSI



O IP iSCSI fornece acesso ao 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 eliminado.

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

Endereços IP para pares de HA

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

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

NIC0

- IP de gerenciamento de nós
- IP entre clusters
- IP iSCSI



O IP iSCSI fornece acesso ao 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 eliminado.

NIC1

- IP de rede do cluster

NIC2

- IP de interconexão de cluster (HA IC)

NIC3

- Pageblob NIC IP (acesso ao disco)



O NIC3 só é aplicável a implantações de HA que usam storage de blob de páginas.

Os endereços IP acima não migram em eventos de failover.

Além disso, os IPs frontend (FIPS) 4 são configurados para migrar em eventos de failover. Esses IPs frontend vivem no balanceador de carga.

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

Conexões seguras com os serviços do Azure

Por padrão, o BlueXP habilita um link privado do Azure para conexões entre contas de armazenamento de blob de páginas do Cloud Volumes ONTAP e do Azure.

Na maioria dos casos, não há nada que você precise fazer: O BlueXP gerencia o link privado do Azure para você. Mas se você usar o Azure Private DNS, precisará editar um arquivo de configuração. Você também deve estar ciente de um requisito para o local do conetor no Azure.

Você também pode desativar a conexão de link privado, se necessário pelas necessidades da sua empresa. Se você desabilitar o link, o BlueXP configura o Cloud Volumes ONTAP para usar um endpoint de serviço.

"Saiba mais sobre como usar links privados do Azure ou endpoints de serviço com o Cloud Volumes ONTAP".

Ligações a 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 o Azure VNet e a outra rede, por exemplo, sua rede corporativa.

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

Porta para a interconexão HA

Um par de HA da Cloud Volumes ONTAP inclui uma interconexão de HA, que permite que cada nó verifique continuamente se seu parceiro está funcionando e espelhar 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 as LIFs de interconexão HA está aberta e não há regras de grupo de segurança para essa porta. Mas se você criar um firewall entre as LIFs de interconexão HA, precisará garantir que o tráfego TCP esteja aberto para a porta 10006 para que o par de HA possa funcionar corretamente.

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

Você deve usar um grupo de recursos *dedicados* para cada par de HA do Cloud Volumes ONTAP que você implantar no Azure. Apenas um par de HA é compatível em um grupo de recursos.

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

Regras do grupo de segurança

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

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



Procurando informações sobre o conetor? "[Ver regras do grupo de segurança para o conetor](#)"

Regras de entrada para sistemas de nó único

Quando você cria um ambiente de trabalho e escolhe um grupo de segurança predefinido, você pode optar por permitir tráfego em um dos seguintes:

- **Somente VNet selecionado:** A origem do tráfego de entrada é o intervalo de sub-rede do VNet para o sistema Cloud Volumes ONTAP e o intervalo de sub-rede do VNet onde o conetor reside. Esta é a opção recomendada.
- **Todos os VNets:** A origem do tráfego de entrada é o intervalo IP 0,0.0.0/0.
- **Disabled:** Esta opção restringe o acesso da rede pública à sua conta de armazenamento e desativa a disposição em camadas de dados para sistemas Cloud Volumes ONTAP. Esta é uma opção recomendada se os seus endereços IP privados não devem ser expostos mesmo dentro do mesmo VNet devido a regulamentos e políticas de segurança.

Prioridade e nome	Porta e protocolo	Origem e destino	Descrição
1000 inbound_ssh	22 TCP	Qualquer a qualquer	Acesso SSH ao endereço IP do LIF de gerenciamento de cluster ou um LIF de gerenciamento de nó
1001 inbound_http	80 TCP	Qualquer a qualquer	Acesso HTTP ao console da Web do Gerenciador de sistema do ONTAP usando o endereço IP do LIF de gerenciamento de cluster
1002 inbound_111_tcp	111 TCP	Qualquer a qualquer	Chamada de procedimento remoto para NFS
1003 inbound_111_udp	111 UDP	Qualquer a qualquer	Chamada de procedimento remoto para NFS
1004 inbound_139	139 TCP	Qualquer a qualquer	Sessão de serviço NetBIOS para CIFS
1005 inbound_161-162_tcp	161-162 TCP	Qualquer a qualquer	Protocolo de gerenciamento de rede simples
1006 inbound_161-162_udp	161-162 UDP	Qualquer a qualquer	Protocolo de gerenciamento de rede simples
1007 inbound_443	443 TCP	Qualquer a qualquer	Conetividade com o conector e acesso HTTPS à consola Web do Gestor de sistema ONTAP utilizando o endereço IP do LIF de gestão de clusters
1008 inbound_445	445 TCP	Qualquer a qualquer	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
1009 inbound_635_tcp	635 TCP	Qualquer a qualquer	Montagem em NFS
1010 inbound_635_udp	635 UDP	Qualquer a qualquer	Montagem em NFS
1011 inbound_749	749 TCP	Qualquer a qualquer	Kerberos
1012 inbound_2049_tcp	2049 TCP	Qualquer a qualquer	Daemon do servidor NFS
1013 inbound_2049_udp	2049 UDP	Qualquer a qualquer	Daemon do servidor NFS
1014 inbound_3260	3260 TCP	Qualquer a qualquer	Acesso iSCSI através do iSCSI data LIF

Prioridade e nome	Porta e protocolo	Origem e destino	Descrição
1015 inbound_4045-4046_tcp	4045-4046 TCP	Qualquer a qualquer	Daemon de bloqueio NFS e monitor de status da rede
1016 inbound_4045-4046_udp	4045-4046 UDP	Qualquer a qualquer	Daemon de bloqueio NFS e monitor de status da rede
1017 inbound_10000	10000 TCP	Qualquer a qualquer	Backup usando NDMP
1018 inbound_11104-11105	11104-11105 TCP	Qualquer a qualquer	Transferência de dados SnapMirror
3000 inbound_deny_all_tcp	Qualquer porta TCP	Qualquer a qualquer	Bloquear todo o outro tráfego de entrada TCP
3001 inbound_deny_all_udp	Qualquer porta UDP	Qualquer a qualquer	Bloqueie todo o outro tráfego de entrada UDP
65000 AllowVnetInBound	Qualquer porta de qualquer protocolo	VirtualNetwork para VirtualNetwork	Tráfego de entrada de dentro da VNet
65001 AllowAzureLoadBalancerInBound	Qualquer porta de qualquer protocolo	AzureLoadBalancer para qualquer	Tráfego de dados do Azure Standard Load Balancer
65500 DenyAllInBound	Qualquer porta de qualquer protocolo	Qualquer a qualquer	Bloquear todo o outro tráfego de entrada

Regras de entrada para sistemas HA

Quando você cria um ambiente de trabalho e escolhe um grupo de segurança predefinido, você pode optar por permitir tráfego em um dos seguintes:

- **Somente VNet selecionado:** A origem do tráfego de entrada é o intervalo de sub-rede do VNet para o sistema Cloud Volumes ONTAP e o intervalo de sub-rede do VNet onde o conector reside. Esta é a opção recomendada.
- **Todos os VNets:** A origem do tráfego de entrada é o intervalo IP 0,0.0.0/0.



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

- **Disabled:** Esta opção restringe o acesso da rede pública à sua conta de armazenamento e desativa a disposição em camadas de dados para sistemas Cloud Volumes ONTAP. Esta é uma opção recomendada se os seus endereços IP privados não devem ser expostos mesmo dentro do mesmo VNet devido a regulamentos e políticas de segurança.

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

Regras de saída

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

Regras básicas de saída

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

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

Regras de saída avançadas

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



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

Serviço	Porta	Prot ocol o	Fonte	Destino	Finalidade
---------	-------	-------------------	-------	---------	------------

Ative
Directory

	389	TCP	DATA LIF (NFS, CIFS)	Floresta do ativo Directory	LDAP
Serviço	Porta	UDP	Fonte	Destino	Finalidade
	445	TCP	DATA LIF (NFS, CIFS)	Floresta do ativo Directory	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
	464	TCP	DATA LIF (NFS, CIFS)	Floresta do ativo Directory	Kerberos V alterar e definir senha (SET_CHANGE)
	464	UDP	DATA LIF (NFS, CIFS)	Floresta do ativo Directory	Administração de chaves Kerberos
	749	TCP	DATA LIF (NFS, CIFS)	Floresta do ativo Directory	Palavra-passe de alteração e definição Kerberos V (RPCSEC_GSS)
AutoSupport	HTTPS	443	LIF de gerenciamento de nós	suporte.NetApp.com	AutoSupport (HTTPS é o padrão)
	HTTP	80	LIF de gerenciamento de nós	suporte.NetApp.com	AutoSupport (somente se o protocolo de transporte for alterado de HTTPS para HTTP)
	TCP	3128	LIF de gerenciamento de nós	Conetor	Enviar mensagens AutoSupport através de um servidor proxy no conetor, se uma conexão de saída de Internet não estiver disponível
Backups de configuração	HTTP	80	LIF de gerenciamento de nós	Http://<connector-IP-address>/occm/offboxconfig	Envie backups de configuração para o conetor. "Saiba mais sobre arquivos de backup de configuração" .
DHCP	68	UDP	LIF de gerenciamento de nós	DHCP	Cliente DHCP para configuração pela primeira vez
DHCPS	67	UDP	LIF de gerenciamento de nós	DHCP	Servidor DHCP
DNS	53	UDP	LIF e LIF de dados de gerenciamento de nós (NFS, CIFS)	DNS	DNS
NDMP	18600–18699	TCP	LIF de gerenciamento de nós	Servidores de destino	Cópia NDMP
SMTP	25	TCP	LIF de gerenciamento de nós	Servidor de correio	Alertas SMTP, podem ser usados para AutoSupport

Serviço	Porta	Protocolo	Fonte	Destino	Finalidade
SNMP	161	TCP	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
	161	UDP	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
	162	TCP	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
	162	UDP	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
SnapMirror	11104	TCP	LIF entre clusters	LIFs ONTAP entre clusters	Gestão de sessões de comunicação entre clusters para SnapMirror
	11105	TCP	LIF entre clusters	LIFs ONTAP entre clusters	Transferência de dados SnapMirror
Syslog	514	UDP	LIF de gerenciamento de nós	Servidor syslog	Mensagens de encaminhamento do syslog

Requisitos para o conetor

Se você ainda não criou um conetor, você deve rever os requisitos de rede para o conetor também.

- ["Veja os requisitos de rede para o conetor"](#)
- ["Regras do grupo de segurança no Azure"](#)

Configure 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 a criptografia do Serviço de armazenamento do Azure com uma chave gerenciada pela Microsoft. Mas você pode usar sua própria chave de criptografia seguindo as etapas desta página.

Visão geral da criptografia de dados

Os dados do Cloud Volumes ONTAP são criptografados automaticamente no Azure usando ["Criptografia do Serviço de storage 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, então você precisa concluir as seguintes etapas:

1. A partir do Azure, crie um cofre de chaves e, em seguida, gere uma chave nesse cofre.

2. No BlueXP , use a API para criar um ambiente de trabalho do Cloud Volumes ONTAP que use a chave.

Rotação das teclas

Se você criar uma nova versão de sua chave, o Cloud Volumes ONTAP usará automaticamente a versão de chave mais recente.

Como os dados são criptografados

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

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

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

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

Crie uma identidade gerenciada atribuída pelo usuário

Você tem a opção de criar um recurso chamado uma identidade gerenciada atribuída pelo usuário. Com isso, você pode criptografar suas contas de storage ao criar um ambiente de trabalho do Cloud Volumes ONTAP. Recomendamos criar esse recurso antes de criar um cofre de chaves e gerar uma chave.

O recurso tem o seguinte ID: `userassignedidentity`.

Passos

1. No Azure, vá para Serviços do Azure e selecione **identidades gerenciadas**.
2. Clique em **criar**.
3. Forneça os seguintes detalhes:
 - **Assinatura**: Escolha uma assinatura. Recomendamos escolher a mesma assinatura que a assinatura do conector.
 - **Grupo de recursos**: Use um grupo de recursos existente ou crie um novo.
 - **Região**: Opcionalmente, selecione a mesma região que o conector.
 - **Nome**: Insira 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 subscrição e região do Azure na qual pretende criar o sistema Cloud Volumes ONTAP.

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

Passos

1. "[Crie um cofre-chave na sua subscrição 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 ativadas:
 - **Soft-delete** (esta opção está ativada por padrão, mas *não* deve ser desativada)
 - * Purge proteção*
 - **Criptografia de disco do Azure para criptografia de volume** (para sistemas de nó único, pares de HA em várias zonas e implantações de AZ únicas de HA)



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

- A seguinte opção deve ser ativada 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, vá para o passo 3.
 - a. Selecione as seguintes permissões:
 - obter
 - lista
 - descriptografar

- criptografar
- tecla de desatamento
- tecla de atamento
- verifique
- assinar

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

c. Revise e crie a política de acesso.

3. "Gere uma chave no cofre de chaves".

Observe os seguintes requisitos para a chave:

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

Crie um ambiente de trabalho 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 do BlueXP .

Permissões necessárias

Se você quiser usar uma chave gerenciada pelo cliente com um sistema Cloud Volumes ONTAP de nó único, verifique se o conector BlueXP tem 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-chave na sua assinatura do Azure usando a seguinte chamada de API do BlueXP .

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

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

Anote o **name** 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 Vault usando a seguinte chamada de API do BlueXP .

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

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

Anote o **keyname**. Você precisará especificar esse valor (juntamente com o nome do Vault) na próxima etapa.

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

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

a. Para um par de HA:

POST /azure/ha/working-environments

O corpo da solicitação deve incluir os seguintes campos:

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



Inclua o "userAssignedIdentity": " userAssignedIdentityId" campo se você criou esse 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"  
}
```



Inclua o "userAssignedIdentity": " userAssignedIdentityId" campo se você criou esse 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.

Configure o licenciamento para o Cloud Volumes ONTAP no Azure

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

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 à esquerda, selecione **Storage > Canvas**.
2. Na página Canvas, clique em **Adicionar ambiente de trabalho** e siga as etapas no BlueXP .
 - 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 por meio da assinatura do mercado, a menos que exceda 500 GiB de capacidade provisionada, momento em que o sistema é convertido automaticamente 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. Depois de voltar ao BlueXP , selecione **Freemium** quando chegar à página métodos de carregamento.

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 com os seguintes modelos de consumo:

- Uma licença (traga sua própria licença (BYOL)) comprada da NetApp
- Uma assinatura por hora, com pagamento conforme o uso (PAYGO) no Azure Marketplace
- Um contrato anual

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

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

BYOL

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

Passos

1. ["Entre em Contato com a NetApp Sales para obter uma licença"](#)
2. ["Adicione sua conta do site de suporte da NetApp ao BlueXP "](#)

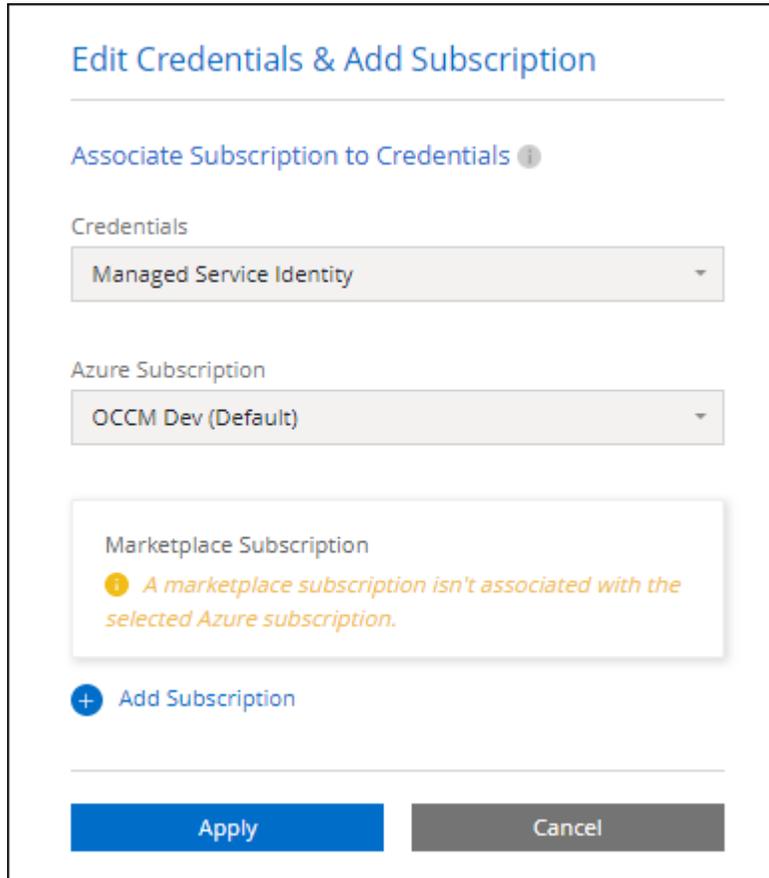
A BlueXP consulta automaticamente o serviço de licenciamento da NetApp para obter detalhes sobre as licenças associadas à sua conta do site de suporte da NetApp. Se não houver erros, o BlueXP adiciona automaticamente as licenças à carteira digital.

A sua licença tem de estar disponível na carteira digital BlueXP antes de a poder utilizar com o Cloud Volumes ONTAP. Se necessário, você pode ["Adicione manualmente a licença à carteira digital BlueXP "](#).

3. Na página Canvas, clique em **Adicionar ambiente de trabalho** e siga as etapas no BlueXP .

- 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 sempre será cobrada primeiro, mas você será cobrado da taxa por hora no mercado se exceder sua capacidade licenciada ou se o prazo da licença expirar.



Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials
Managed Service Identity

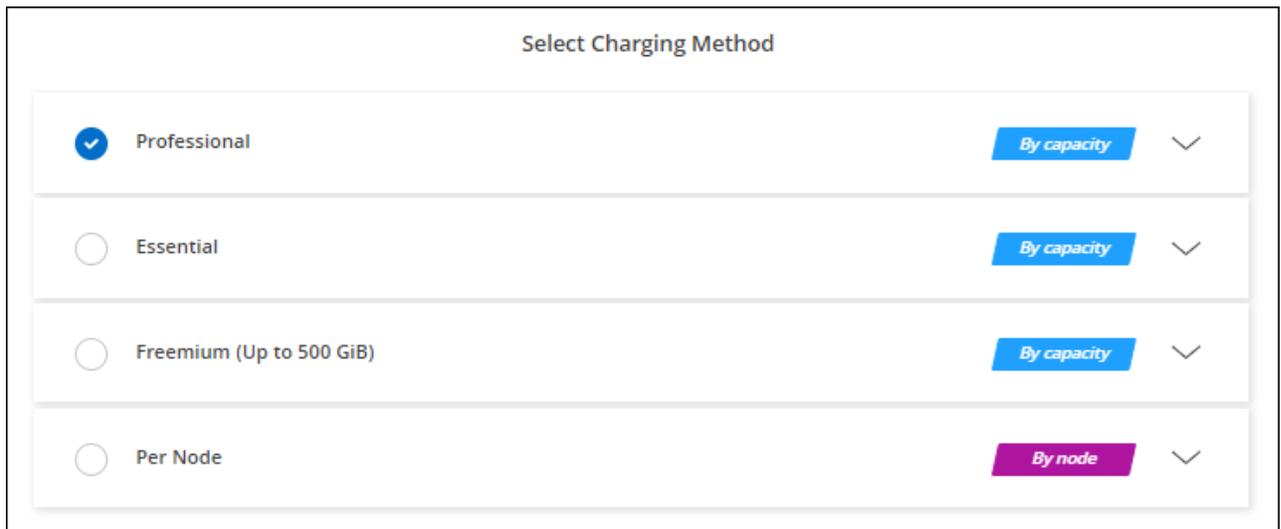
Azure Subscription
OCCM Dev (Default)

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

+ Add Subscription

Apply Cancel

- a. Depois de voltar ao BlueXP , selecione um pacote baseado na capacidade quando chegar à página métodos de carregamento.



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".

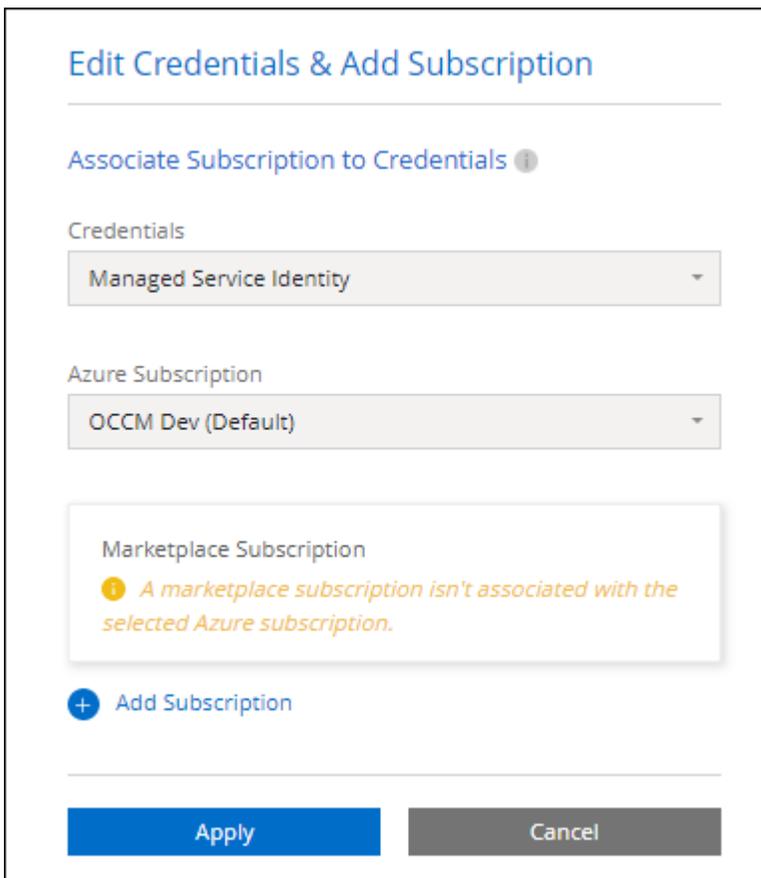
Subscrição PAYGO

Pague por hora assinando a oferta no mercado do seu provedor de nuvem.

Quando você cria um ambiente de trabalho do Cloud Volumes ONTAP, o BlueXP solicita que você assine o contrato disponível no mercado do Azure. Essa assinatura é então associada ao ambiente de trabalho para cobrança. Você pode usar essa mesma assinatura para ambientes de trabalho adicionais.

Passos

1. No menu de navegação à esquerda, selecione **Storage > Canvas**.
2. Na página Canvas, clique em **Adicionar ambiente de trabalho** e siga as etapas no BlueXP .
 - 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. Depois de voltar ao BlueXP , selecione um pacote baseado na capacidade quando chegar à página métodos de carregamento.

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".



Pode gerir as subscrições do Azure Marketplace associadas às suas contas Azure a partir da página Definições > credenciais. ["Saiba como gerenciar suas contas e assinaturas do Azure"](#)

Contrato anual

Pague pelo Cloud Volumes ONTAP anualmente comprando um contrato anual.

Passos

1. Contacte o seu representante de vendas da NetApp para adquirir um contrato anual.

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

Depois que o NetApp compartilhar a oferta privada com você, você pode selecionar o plano anual ao se inscrever no mercado Azure durante a criação do ambiente de trabalho.

2. Na página Canvas, clique em **Adicionar ambiente de trabalho** e siga as etapas no BlueXP .
 - 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 **Subscribe**.
 - c. Depois de voltar ao BlueXP , selecione um pacote baseado na capacidade quando chegar à página métodos de carregamento.

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".

Inscrição no Keystone

Uma subscrição do Keystone é um serviço baseado em subscrição com pagamento conforme o uso. ["Saiba mais sobre as assinaturas do NetApp Keystone"](#).

Passos

1. Se você ainda não tem uma assinatura, ["Entre em Contato com a NetApp"](#)
2. Para autorizar sua conta de usuário do BlueXP com uma ou mais assinaturas do Keystone NetApp NetApp.
3. Depois que o NetApp autorizar sua conta ["Vincule suas assinaturas para uso com o Cloud Volumes ONTAP"](#), .
4. Na página Canvas, clique em **Adicionar ambiente de trabalho** e siga as etapas no BlueXP .
 - 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".

Ative o modo de alta disponibilidade no Azure

O modo de alta disponibilidade (HA) do Microsoft Azure deve estar ativado para reduzir o tempo de failover não planejado e para habilitar o suporte NFSv4 para Cloud Volumes ONTAP. Nesse modo, seus nós de HA do Cloud Volumes ONTAP podem alcançar um objetivo de tempo de recuperação (rto) baixo (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 executados no Microsoft Azure e adicionamos suporte para NFSv4. Para disponibilizar esses aprimoramentos ao Cloud Volumes ONTAP, você precisa ativar o recurso de alta disponibilidade na sua assinatura do Azure.

O BlueXP solicitará esses detalhes em uma mensagem Ação necessária quando o recurso precisar ser habilitado em uma assinatura do Azure.

Observe o seguinte:

- Não há problemas com a alta disponibilidade do seu par de HA do Cloud Volumes ONTAP. Esse recurso do Azure funciona em conjunto com o ONTAP para reduzir o tempo de interrupção de aplicativos observado pelo cliente para protocolos NFS que resultam de eventos de failover não planejados.
- A ativação desse recurso não causa interrupções aos pares de HA do Cloud Volumes ONTAP.

- Ativar este recurso na sua assinatura do Azure não causa problemas a 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 ativado, o BlueXP verifica o sistema a cada 12 horas para atualizar as regras internas do Azure Load Balancer.

Um usuário do Azure que tenha Privileges de "proprietário" pode ativar o recurso a partir da CLI do Azure.

Passos

1. ["Acesse o Azure Cloud Shell a partir do Portal do Azure"](#)
2. Registre a funcionalidade do 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/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

Ative VMOrchestratorZonalMultiFD para zonas de disponibilidade únicas

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

A menos que você ative esse recurso, a implantação zonal não ocorre e a implantação LRS não zonal anterior se torna efetiva.

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

Execute estas etapas como um usuário com o Privileges "proprietário":

Passos

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

```
az Account Set -s <Azure_subscription_name_or_ID> az Feature register --name VMOrchestratorZonalMultiFD --namespace Microsoft.Compute
```

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

```
Clique no botão Microsoft.Compute "OK". Clique no botão "OK": "/Subscription/<ID>/Providers/Microsoft.features/Providers/Microsoft.Compute/features/VMOrchestratorZonalMultiFD", "name": "Microsoft.Compute/VMOrchestratorZonalMultiFD", "Properties": "State": "Registered", "type": "Microsoft.features/Providers/Features"
```

Iniciar o Cloud Volumes ONTAP no Azure

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

O que você vai precisar

Você precisa do seguinte para criar um ambiente de trabalho.

- Um conector que está em funcionamento.
 - Você deve ter um "[Conector que está associado ao seu projeto ou área de trabalho](#)".
 - "[Você deve estar preparado para deixar o conector funcionando o tempo todo](#)".
- Uma compreensão da configuração que você deseja usar.

Você deve ter escolhido uma configuração e obtido informações de rede do Azure do administrador. Para obter informações, "[Planejando sua configuração do Cloud Volumes ONTAP](#)" consulte .

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

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

Sobre esta tarefa

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

do assistente.

Potencial para perda de dados

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



A implantação do Cloud Volumes ONTAP em um grupo de recursos compartilhados existente não é recomendada devido ao risco de perda de dados. Embora o BlueXP possa remover recursos do Cloud Volumes ONTAP de um grupo de recursos compartilhados em caso de falha ou exclusão da implantação, um usuário do Azure pode excluir acidentalmente recursos do Cloud Volumes ONTAP de um grupo de recursos compartilhados.

Iniciar um sistema Cloud Volumes ONTAP de nó único no Azure

Para iniciar um sistema Cloud Volumes ONTAP de nó único no Azure, é necessário criar um ambiente de trabalho de nó único no BlueXP .

Passos

1. No menu de navegação à esquerda, selecione **Storage > Canvas**.
2. na página do Canvas, clique em **Adicionar ambiente de trabalho** e siga as instruções.
3. **Escolha um local:** Selecione **Microsoft Azure** e **nó único Cloud Volumes ONTAP**.
4. Se for solicitado, "[Crie um conector](#)".
5. **Detalhes e credenciais:** Opcionalmente, altere as credenciais e a assinatura do Azure, especifique um nome de cluster, adicione tags se necessário e especifique credenciais.

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

Campo	Descrição
Nome do ambiente de trabalho	O BlueXP usa o nome do ambiente de trabalho para nomear o sistema Cloud Volumes ONTAP e a máquina virtual do Azure. Ele também usa o nome como prefixo para o grupo de segurança predefinido, se você selecionar essa opção.
Tags Grupo recursos	As tags são metadados para seus recursos do Azure. Quando você insere tags neste campo, o BlueXP as adiciona ao grupo de recursos associado ao sistema Cloud Volumes ONTAP. Você pode adicionar até quatro tags da interface do usuário ao criar um ambiente de trabalho e, em seguida, você pode adicionar mais após a criação. Observe que a API não limita a quatro tags ao criar um ambiente de trabalho. Para obter informações sobre tags, consulte o " Documentação do Microsoft Azure: Usando tags para organizar seus recursos do Azure ".
Nome de utilizador e palavra-passe	Estas são as credenciais da conta de administrador de cluster do Cloud Volumes ONTAP. Você pode usar essas credenciais para se conectar ao Cloud Volumes ONTAP por meio do Gerenciador de sistemas do ONTAP ou da CLI do ONTAP. 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 pay-as-you-go. " Saiba como adicionar credenciais ".

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

[Inscreva-se no BlueXP a partir do Azure Marketplace](#)

6. **Serviços:** Ative ou desative os serviços individuais que você deseja ou não deseja usar com o Cloud Volumes ONTAP.

- ["Saiba mais sobre a classificação BlueXP"](#)
- ["Saiba mais sobre backup e recuperação do BlueXP "](#)



Se quiser utilizar WORM e disposição de dados em camadas, desative o backup e a recuperação do BlueXP e implante um ambiente de trabalho do Cloud Volumes ONTAP com a versão 9,8 ou superior.

7. **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 conector e o local de destino.

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

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

Campo	Descrição
Grupo 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 compartilhado existente, não é recomendado devido ao risco de perda de dados. Consulte o aviso acima para obter mais detalhes.</p> <p> Se a conta do Azure que você está usando tiver o "permissões necessárias", o BlueXP removerá recursos do Cloud Volumes ONTAP de um grupo de recursos, em caso de falha ou exclusão da implantação.</p>
Grupo de segurança gerado	<p>Se você permitir que o BlueXP gere o grupo de segurança para você, você precisa escolher como permitirá o tráfego:</p> <ul style="list-style-type: none">• Se você escolher somente VNet selecionado, a origem do tráfego de entrada é o intervalo de sub-rede do VNet selecionado e o intervalo de sub-rede do VNet onde o conector reside. Esta é a opção recomendada.• Se você escolher todos os VNets, a origem do tráfego de entrada é o intervalo IP 0,0.0.0/0.
Utilizar existente	<p>Se você escolher um grupo de segurança existente, ele deverá atender aos requisitos do Cloud Volumes ONTAP. "Exibir o grupo de segurança padrão".</p>

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

- ["Saiba mais sobre as opções de licenciamento para o Cloud Volumes ONTAP"](#).
- ["Saiba 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, você só precisa especificar um volume e, em seguida, revisar e aprovar a configuração.

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



Se um candidato de lançamento mais recente, disponibilidade geral ou liberação de 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 9.13.1 e 9.13.1 P4 estiver disponível. A atualização não ocorre de uma versão para outra, por exemplo, de 9,13 a 9,14.

12. **Assine no Azure Marketplace:** Você verá esta página se o BlueXP não puder habilitar implantações programáticas do Cloud Volumes ONTAP. Siga as etapas listadas na tela. Consulte "[Implantação programática de produtos do Marketplace](#)" para obter mais informações.
13. **Recursos de armazenamento subjacentes:** Escolha configurações para o agregado inicial: Um tipo de disco, um tamanho para cada disco e se a disposição de dados em camadas para armazenamento Blob deve ser ativada.

Observe o seguinte:

- Se o acesso público à sua conta de armazenamento estiver desativado no VNet, não será possível ativar a disposição de dados em camadas no sistema Cloud Volumes ONTAP. Para obter informações, "[Regras do grupo de segurança](#)" consulte .
- O tipo de disco é para o volume inicial. Você pode escolher um tipo de disco diferente para volumes subsequentes.
- O tamanho do disco é para todos os discos no agregado inicial e para quaisquer agregados adicionais criados pelo BlueXP quando você usa a opção de provisionamento simples. Você pode criar agregados que usam um tamanho de disco diferente usando a opção Alocação avançada.

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

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

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

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

- a. Escolha **normal** ou **alta** velocidade de gravação, se desejado.

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

- b. Ative o storage WORM (uma gravação, muitas leituras), se desejado.

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

O WORM não pode ser ativado se a disposição de dados em camadas foi ativada para o Cloud Volumes ONTAP versões 9,7 e inferiores. Reverter ou fazer downgrade para o Cloud Volumes ONTAP 9,8 é bloqueado depois de ativar WORM e disposição em camadas.

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

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

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

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

Alguns dos campos desta página são auto-explicativos. A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Tamanho	O tamanho máximo que você pode inserir depende, em grande parte, se você ativar o provisionamento de thin, o que permite criar um volume maior do que o armazenamento físico atualmente disponível para ele.
Controle de acesso (somente para NFS)	Uma política de exportação define os clientes na sub-rede que podem acessar o volume. Por padrão, o BlueXP insere um valor que fornece acesso a todas as instâncias na sub-rede.
Permissões e utilizadores/grupos (apenas para CIFS)	Esses campos permitem controlar o nível de acesso a um compartilhamento para usuários e grupos (também chamados de listas de controle de acesso ou ACLs). Você pode especificar usuários ou grupos do Windows locais ou de domínio, ou usuários ou grupos UNIX. Se você especificar um nome de usuário do domínio do Windows, você deve incluir o domínio do usuário usando o nome de domínio do formato.
Política de instantâneos	Uma política de cópia Snapshot especifica a frequência e o número de cópias snapshot do NetApp criadas automaticamente. Uma cópia Snapshot do NetApp é uma imagem pontual do sistema de arquivos que não afeta a performance e exige o mínimo de storage. Você pode escolher a política padrão ou nenhuma. Você pode escolher nenhum para dados transitórios: Por exemplo, tempdb para Microsoft SQL Server.
Opções avançadas (somente para NFS)	Selecione uma versão NFS para o volume: NFSv3 ou NFSv4.
Grupo de iniciadores e IQN (apenas para iSCSI)	Os destinos de armazenamento iSCSI são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Os grupos de iniciadores são tabelas de nomes de nós de host iSCSI e controlam quais iniciadores têm acesso a quais LUNs. Os destinos iSCSI se conectam à rede por meio de adaptadores de rede Ethernet (NICs) padrão, placas de mecanismo de descarga TCP (TOE) com iniciadores de software, adaptadores de rede convergidos (CNAs) ou adaptadores de barramento de host dedicados (HBAs) e são identificados por IQNs (iSCSI Qualified Names). Quando cria um volume iSCSI, o BlueXP cria automaticamente um LUN para si. Simplificamos a criação de apenas um LUN por volume, para que não haja gerenciamento envolvido. Depois de criar o volume, "Use o IQN para se conectar ao LUN a partir de seus hosts" .

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

Volume Details, Protection & Protocol

Details & Protection	Protocol
<p>Volume Name: <input style="width: 200px;" type="text" value="vol"/> Size (GB): <input style="width: 80px;" type="text" value="250"/></p> <p>Snapshot Policy: <input style="width: 300px;" type="text" value="default"/></p> <p><small>Default Policy</small></p>	<p style="text-align: center;"> NFS iSCSI </p> <p>Share name: <input style="width: 150px;" type="text" value="vol_share"/> Permissions: <input style="width: 150px;" type="text" value="Full Control"/></p> <p>Users / Groups: <input style="width: 300px;" type="text" value="engineering"/></p> <p><small>Valid users and groups separated by a semicolon</small></p>

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 ativo Directory e os controladores de domínio para o domínio em que o servidor CIFS irá ingressar.
Ativo Directory Domain para aderir	O FQDN do domínio do ativo Directory (AD) ao qual você deseja que o servidor CIFS se associe.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores à unidade organizacional especificada (ou) dentro do domínio do AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio AD.
Unidade organizacional	A unidade organizacional dentro do domínio AD a associar ao servidor CIFS. A predefinição é computadores. Para configurar os Serviços de domínio do Azure AD como o servidor AD para o Cloud Volumes ONTAP, você deve inserir computadores AADDC ou usuários AADDC neste campo. "Documentação do Azure: Crie uma unidade organizacional (ou) em um domínio gerenciado dos Serviços de domínio do Azure AD"
Domínio DNS	O domínio DNS da máquina virtual de storage (SVM) do Cloud Volumes ONTAP. Na maioria dos casos, o domínio é o mesmo que o domínio AD.
NTP Server	Selecione Use ativo Directory Domain para configurar um servidor NTP usando o DNS do ativo Directory. Se você precisa configurar um servidor NTP usando um endereço diferente, então você deve usar a API. Consulte "Documentos de automação BlueXP" para obter mais informações. Observe que você pode configurar um servidor NTP somente ao criar um servidor CIFS. Não é configurável depois de criar o servidor CIFS.

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

Para obter mais informações, "[Compreender os perfis de utilização de volume](#)" consulte e "[Visão geral de categorização de dados](#)".

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

Resultado

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

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

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

Depois de terminar

- Se você provisionou um compartilhamento CIFS, dê aos usuários ou grupos permissões para os arquivos e pastas e verifique se esses usuários podem acessar o compartilhamento e criar um arquivo.
- Se você quiser aplicar cotas a volumes, use o Gerenciador de sistema do ONTAP ou a CLI do ONTAP.

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

Lançamento de um par de HA do Cloud Volumes ONTAP no Azure

Para iniciar um par de HA do Cloud Volumes ONTAP no Azure, é necessário criar um ambiente de trabalho de HA no BlueXP .

Passos

1. No menu de navegação à esquerda, selecione **Storage > Canvas**.
2. na página do Canvas, clique em **Adicionar ambiente de trabalho** e siga as instruções.
3. Se for solicitado, "[Crie um conector](#)".
4. **Detalhes e credenciais:** Opcionalmente, altere as credenciais e a assinatura do Azure, especifique um nome de cluster, adicione tags se necessário e especifique credenciais.

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

Campo	Descrição
Nome do ambiente de trabalho	O BlueXP usa o nome do ambiente de trabalho para nomear o sistema Cloud Volumes ONTAP e a máquina virtual do Azure. Ele também usa o nome como prefixo para o grupo de segurança predefinido, se você selecionar essa opção.

Campo	Descrição
Tags Grupo recursos	As tags são metadados para seus recursos do Azure. Quando você insere tags neste campo, o BlueXP as adiciona ao grupo de recursos associado ao sistema Cloud Volumes ONTAP. Você pode adicionar até quatro tags da interface do usuário ao criar um ambiente de trabalho e, em seguida, você pode adicionar mais após a criação. Observe que a API não limita a quatro tags ao criar um ambiente de trabalho. Para obter informações sobre tags, consulte o "Documentação do Microsoft Azure: Usando tags para organizar seus recursos do Azure" .
Nome de utilizador e palavra-passe	Estas são as credenciais da conta de administrador de cluster do Cloud Volumes ONTAP. Você pode usar essas credenciais para se conectar ao Cloud Volumes ONTAP por meio do Gerenciador de sistemas do ONTAP ou da CLI do ONTAP. 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 pay-as-you-go. "Saiba como adicionar credenciais" .

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

[Inscreva-se no BlueXP a partir do Azure Marketplace](#)

5. **Serviços:** Ative ou desative os serviços individuais com base se você deseja usá-los com o Cloud Volumes ONTAP.

- ["Saiba mais sobre a classificação BlueXP"](#)
- ["Saiba mais sobre backup e recuperação do BlueXP "](#)



Se quiser utilizar WORM e disposição de dados em camadas, desative o backup e a recuperação do BlueXP e implante um ambiente de trabalho do Cloud Volumes ONTAP com a versão 9,8 ou superior.

6. **Modelos de implantação HA:**

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

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

A partir do Cloud Volumes ONTAP 9.15.1, é possível 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 suporte essa implantação. Se a zona ou a região não suportar a implantação por zona, o modo de implantação não por zona anterior para LRS será seguido. Para entender as configurações suportadas para discos gerenciados compartilhados, ["Configuração de zona de disponibilidade única DE HA com discos gerenciados compartilhados"](#) consulte .

- 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 **Eu tenho conectividade de rede verificada....**

7. **Conetividade:** Escolha um grupo de recursos novo ou existente e escolha se deseja usar o grupo de

segurança predefinido ou o seu próprio.

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

Campo	Descrição
Grupo 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 compartilhado existente, não é recomendado devido ao risco de perda de dados. Consulte o aviso acima para obter mais detalhes.</p> <p>Você deve usar um grupo de recursos dedicado para cada par de HA do Cloud Volumes ONTAP implantado no Azure. Apenas um par de HA é compatível em um grupo de recursos. O BlueXP enfrenta problemas de conexão se você tentar implantar um segundo par de HA do Cloud Volumes ONTAP em um grupo de recursos do Azure.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"><p>Se a conta do Azure que você está usando tiver o "permissões necessárias", o BlueXP removerá recursos do Cloud Volumes ONTAP de um grupo de recursos, em caso de falha ou exclusão da implantação.</p></div>
Grupo de segurança gerado	<p>Se você permitir que o BlueXP gere o grupo de segurança para você, você precisa escolher como permitirá o tráfego:</p> <ul style="list-style-type: none">• Se você escolher somente VNet selecionado, a origem do tráfego de entrada é o intervalo de sub-rede do VNet selecionado e o intervalo de sub-rede do VNet onde o conector reside. Esta é a opção recomendada.• Se você escolher todos os VNets, a origem do tráfego de entrada é o intervalo IP 0,0.0.0/0.
Utilizar existente	<p>Se você escolher um grupo de segurança existente, ele deverá atender aos requisitos do Cloud Volumes ONTAP. "Exibir o grupo de segurança padrão".</p>

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

- "[Saiba mais sobre as opções de licenciamento para o Cloud Volumes ONTAP](#)".
- "[Saiba 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, você só precisa especificar um volume e, em seguida, revisar e aprovar a configuração.

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



Se um candidato de lançamento mais recente, disponibilidade geral ou liberação de 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 9.13.1 e 9.13.1 P4 estiver disponível. A atualização não ocorre de uma versão para outra, por exemplo, de 9,13 a 9,14.

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

Observe o seguinte:

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

Para obter ajuda sobre como escolher um tamanho de disco, ["Dimensione seu sistema no Azure"](#) consulte .

- Se o acesso público à sua conta de armazenamento estiver desativado no VNet, não será possível ativar a disposição de dados em camadas no sistema Cloud Volumes ONTAP. Para obter informações, ["Regras do grupo de segurança"](#) consulte .
- Você pode escolher uma política específica de disposição em categorias de volume ao criar ou editar um volume.
- Se você desativar a disposição de dados em categorias, poderá ativá-la em agregados subsequentes.

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

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

- a. Escolha **normal** ou **alta** velocidade de gravação, se desejado.

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

- b. Ative o storage WORM (uma gravação, muitas leituras), se desejado.

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

O WORM não pode ser ativado se a disposição de dados em camadas foi ativada para o Cloud Volumes ONTAP versões 9,7 e inferiores. Reverter ou fazer downgrade para o Cloud Volumes ONTAP 9,8 é bloqueado depois de ativar WORM e disposição em camadas.

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

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

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

A conexão HTTPS é de um par de HA do Cloud Volumes ONTAP 9,7 para contas de armazenamento de blob de páginas do Azure. Observe que ativar essa opção pode afetar o desempenho de gravação. Não é

possível alterar a configuração depois de criar o ambiente de trabalho.

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

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

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

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

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

Alguns dos campos desta página são auto-explicativos. A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Tamanho	O tamanho máximo que você pode inserir depende, em grande parte, se você ativar o provisionamento de thin, o que permite criar um volume maior do que o armazenamento físico atualmente disponível para ele.
Controle de acesso (somente para NFS)	Uma política de exportação define os clientes na sub-rede que podem acessar o volume. Por padrão, o BlueXP insere um valor que fornece acesso a todas as instâncias na sub-rede.
Permissões e utilizadores/grupos (apenas para CIFS)	Esses campos permitem controlar o nível de acesso a um compartilhamento para usuários e grupos (também chamados de listas de controle de acesso ou ACLs). Você pode especificar usuários ou grupos do Windows locais ou de domínio, ou usuários ou grupos UNIX. Se você especificar um nome de usuário do domínio do Windows, você deve incluir o domínio do usuário usando o nome de domínio do formato.
Política de instantâneos	Uma política de cópia Snapshot especifica a frequência e o número de cópias snapshot do NetApp criadas automaticamente. Uma cópia Snapshot do NetApp é uma imagem pontual do sistema de arquivos que não afeta a performance e exige o mínimo de storage. Você pode escolher a política padrão ou nenhuma. Você pode escolher nenhum para dados transitórios: Por exemplo, tempdb para Microsoft SQL Server.
Opções avançadas (somente para NFS)	Selecione uma versão NFS para o volume: NFSv3 ou NFSv4.
Grupo de iniciadores e IQN (apenas para iSCSI)	Os destinos de armazenamento iSCSI são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Os grupos de iniciadores são tabelas de nomes de nós de host iSCSI e controlam quais iniciadores têm acesso a quais LUNs. Os destinos iSCSI se conectam à rede por meio de adaptadores de rede Ethernet (NICs) padrão, placas de mecanismo de descarga TCP (TOE) com iniciadores de software, adaptadores de rede convergidos (CNAs) ou adaptadores de barramento de host dedicados (HBAs) e são identificados por IQNs (iSCSI Qualified Names). Quando cria um volume iSCSI, o BlueXP cria automaticamente um LUN para si. Simplificamos a criação de apenas um LUN por volume, para que não haja gerenciamento envolvido. Depois de criar o volume, "Use o IQN para se conectar ao LUN a partir de seus hosts" .

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

Volume Details, Protection & Protocol

Details & Protection	Protocol
<p>Volume Name: <input style="width: 200px;" type="text" value="vol"/> Size (GB): <input style="width: 80px;" type="text" value="250"/></p> <p>Snapshot Policy: <input style="width: 300px;" type="text" value="default"/></p> <p><small>Default Policy</small></p>	<p style="text-align: center;"> <input type="radio"/> NFS <input checked="" type="radio"/> CIFS <input type="radio"/> iSCSI </p> <hr/> <p>Share name: <input style="width: 150px;" type="text" value="vol_share"/> Permissions: <input style="width: 150px;" type="text" value="Full Control"/></p> <p>Users / Groups: <input style="width: 300px;" type="text" value="engineering"/></p> <p><small>Valid users and groups separated by a semicolon</small></p>

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 ativo Directory e os controladores de domínio para o domínio em que o servidor CIFS irá ingressar.
Ative Directory Domain para aderir	O FQDN do domínio do ativo Directory (AD) ao qual você deseja que o servidor CIFS se associe.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores à unidade organizacional especificada (ou) dentro do domínio do AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio AD.
Unidade organizacional	A unidade organizacional dentro do domínio AD a associar ao servidor CIFS. A predefinição é computadores. Para configurar os Serviços de domínio do Azure AD como o servidor AD para o Cloud Volumes ONTAP, você deve inserir computadores AADDC ou usuários AADDC neste campo. "Documentação do Azure: Crie uma unidade organizacional (ou) em um domínio gerenciado dos Serviços de domínio do Azure AD"
Domínio DNS	O domínio DNS da máquina virtual de storage (SVM) do Cloud Volumes ONTAP. Na maioria dos casos, o domínio é o mesmo que o domínio AD.
NTP Server	Selecione Use ativo Directory Domain para configurar um servidor NTP usando o DNS do ativo Directory. Se você precisa configurar um servidor NTP usando um endereço diferente, então você deve usar a API. Consulte "Documentos de automação BlueXP" para obter mais informações. Observe que você pode configurar um servidor NTP somente ao criar um servidor CIFS. Não é configurável depois de criar o servidor CIFS.

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

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

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

Resultado

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

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

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

Depois de terminar

- Se você provisionou um compartilhamento CIFS, dê aos usuários ou grupos permissões para os arquivos e pastas e verifique se esses usuários podem acessar o compartilhamento e criar um arquivo.
- Se você quiser aplicar cotas a volumes, use o Gerenciador de sistema do ONTAP ou a CLI do ONTAP.

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

Verificação de imagem da Plataforma Azure

Visão geral da verificação de imagens do Azure

A verificação de imagens do Azure está em conformidade com os requisitos de segurança aprimorados do NetApp. Embora a verificação de um arquivo de imagem seja um processo simples, a verificação de assinatura de imagem do Azure requer handlings especiais para o conhecido arquivo de imagem do Azure VHD devido a uma alternância feita pelo mercado do Azure.



A verificação de imagens do Azure é suportada no software Cloud Volumes ONTAP versão 9.15.0 ou superior.

Alteração do Azure de arquivos VHD publicados

O principal 1MB (1048576 bytes) e o final de 512 bytes do arquivo VHD é modificado pelo Azure. A assinatura de imagem NetApp ignora os 1MB principais e termina 512 bytes e assina a parte restante da imagem VHD.



Como exemplo, o diagrama acima mostra um arquivo VHD com tamanho 10GB. Mas a parte assinada por NetApp é marcada em verde com tamanho de 10GB - 1MB - 512B.

Faça o download do arquivo de Digest da imagem do Azure

O ficheiro de imagem do Azure pode ser transferido a partir do "[Site de suporte da NetApp](#)". O download está no formato tar.gz e contém arquivos para verificação de assinatura de imagem.

Passos

1. Aceda ao "[Página do produto Cloud Volumes ONTAP no site de suporte da NetApp](#)" e transfira a versão de software necessária na secção Transferências.
2. Na página de download do Cloud Volumes ONTAP, clique no botão **download** do arquivo de imagem do Azure para baixar o arquivo TAR.GZ.

Cloud Volumes ONTAP 9.15.0P1

Date Posted : 17-May-2024

<p>Cloud Volumes ONTAP</p> <p>Non-Restricted Countries</p> <p>If you are upgrading to ONTAP 9.15.0P1, and you are in "Non-restricted Countries", please download the image with NetApp Volume Encryption.</p> <div style="background-color: #0070C0; color: white; padding: 5px; text-align: center; margin-bottom: 5px;"> DOWNLOAD 9150P1_V_IMAGE.TGZ [2.58 GB] </div> <p style="font-size: small; text-align: center;">View and download checksums</p> <div style="background-color: #0070C0; color: white; padding: 5px; text-align: center; margin-bottom: 5px;"> DOWNLOAD 9150P1_V_IMAGE.TGZ.PEM [451 B] </div> <p style="font-size: small; text-align: center;">View and download checksums</p> <div style="background-color: #0070C0; color: white; padding: 5px; text-align: center; margin-bottom: 5px;"> DOWNLOAD 9150P1_V_IMAGE.TGZ.SIG [256 B] </div> <p style="font-size: small; text-align: center;">View and download checksums</p>	<p>Cloud Volumes ONTAP</p> <p>Restricted Countries</p> <p>If you are unsure whether your company complied with all applicable legal requirements on encryption technology, download the image without NetApp Volume Encryption.</p> <div style="background-color: #0070C0; color: white; padding: 5px; text-align: center; margin-bottom: 5px;"> DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ [2.58 GB] </div> <p style="font-size: small; text-align: center;">View and download checksums</p> <div style="background-color: #0070C0; color: white; padding: 5px; text-align: center; margin-bottom: 5px;"> DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ.PEM [451 B] </div> <p style="font-size: small; text-align: center;">View and download checksums</p> <div style="background-color: #0070C0; color: white; padding: 5px; text-align: center; margin-bottom: 5px;"> DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ.SIG [256 B] </div> <p style="font-size: small; text-align: center;">View and download checksums</p>	<p>Cloud Volumes ONTAP</p> <div style="background-color: #0070C0; color: white; padding: 5px; text-align: center; margin-bottom: 5px;"> DOWNLOAD GCP-9-15-0P1_PKG.TAR.GZ [7.49 KB] </div> <p style="font-size: small; text-align: center;">View and download checksums</p> <div style="background-color: #0070C0; color: white; padding: 5px; text-align: center; margin-bottom: 5px;"> DOWNLOAD AZURE-9-15-0P1_PKG.TAR.GZ [7.64 KB] </div> <p style="font-size: small; text-align: center;">View and download checksums</p>
--	--	--

3. Para Linux e MacOS, você deve executar o seguinte para obter o md5sum e sha256sum para o arquivo Azure Image Digest baixado.
 - a. Para md5sum, introduza o md5sum comando.
 - b. Para sha256sum, introduza o sha256sum comando.
4. Verifique se md5sum os valores e sha256sum correspondem ao download do Arquivo de Digest da imagem do Azure.

5. No Linux e Mac os, execute o `tar -xzf` comando para extrair o arquivo `tar.gz`.

O arquivo TAR.GZ extraído contém o arquivo `digest(.sig)`, o arquivo de certificado de chave pública(`.pem`) e o arquivo de certificado de cadeia(`.pem`).

Lista resultado do arquivo `untar 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
```

Exportação de imagens do Azure Marketplace

Uma vez que a imagem VHD é publicada na nuvem Azure, a imagem não é mais gerenciada pelo NetApp. Em vez disso, a imagem publicada é colocada no marketplace do Azure. A alteração do Azure para o 1MB principal e o 512B final do VHD ocorre quando a imagem é encenada e publicada no marketplace do Azure. Para verificar a assinatura do arquivo VHD, a imagem VHD modificada pelo Azure precisa ser exportada primeiro do marketplace do Azure.

O que você vai precisar

Tem de instalar os programas necessários no seu sistema.

- A CLI do Azure está instalada ou o Azure Cloud Shell por meio do portal do Azure está prontamente disponível.



Para obter mais informações sobre como instalar a CLI do Azure, "[Documentação do Azure: Como instalar a CLI do Azure](#)" consulte .

Passos

1. Mapeie a versão do ONTAP para a versão de imagem do marketplace do Azure usando o conteúdo do arquivo `version_readme`.

Para cada mapeamento de versão listado no arquivo `version_readme`, a versão do ONTAP é representada por "buildname", e a versão da imagem do marketplace do Azure é representada por "version".

Por exemplo, no seguinte arquivo `version_readme`, a versão do ONTAP "9.15.0P1" é mapeada para a versão "9150.01000024.05090105" da imagem do marketplace do Azure. Esta versão de imagem do marketplace do Azure é usada mais tarde para definir a URNA da imagem.

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

2. Identifique o nome da região onde você pretende criar VMs.

Esse nome de região é usado como o valor para a variável "locName" ao definir a URNA da imagem do mercado.

- a. Para receber uma lista de regiões disponíveis, digite o `az account list-locations -o table` comando.

Na tabela abaixo, o nome da região é chamado de campo "Nome".

```
$ 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. Reveja os nomes de SKU para as versões Cloud Volumes ONTAP correspondentes e os tipos de implantação de VM na tabela abaixo.

O nome do SKU é usado como o valor para a variável "skuName" ao definir a URNA da imagem do mercado.

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

Versão Cloud Volumes ONTAP	Tipo de implantação da VM	Nome SKU
9.15.1	Todas as implantações por meio do BlueXP	ONTAP_cloud
9.15.0	Nó único	ONTAP_cloud_byol
9.15.0	Alta disponibilidade	ONTAP_cloud_byol_ha

4. Assim que a versão do ONTAP e a imagem do marketplace do Azure forem mapeadas, exporte o arquivo VHD do marketplace do Azure por meio do Azure Cloud Shell ou da CLI do Azure.

Exporte o arquivo VHD por meio do Azure Cloud Shell no portal do Azure

1. A partir do Azure Cloud Shell, exporte a imagem do mercado para um vhd (image2, por exemplo, 9150.01000024.05090105.vhd) e faça o download para sua máquina local (por exemplo, uma máquina Linux ou um PC Windows).

Veja os passos

#Azure Cloud Shell on Azure portal to get VHD image from Azure Marketplace
a) Set the URN and other parameters of the marketplace image. URN is with format "<publisher>:<offer>:<sku>:<version>". Optionally, a user can list NetApp marketplace images to confirm the proper image version.

```
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
...
```

b) Create a new managed disk from the Marketplace image with the matching image version

```
PS /home/user1> $diskName = "9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = "fnfl"
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
```

c) Export a VHD from the managed disk to Azure Storage
Create a container with proper access level. As an example, a container named 'vm-images' with 'Container' access level is used here.

```
Get storage account access key, on Azure portal, 'Storage
Accounts/'examplesaname/'Access Key/'key1/'key/'show'/<copy>.
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
```

d) Download the generated image to your server, e.g., a Linux machine.

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

The URL is organized in a formatted way. For automation tasks, the following example could be used to derive the URL string. Otherwise, Azure CLI 'az' command could be issued to get the URL, which is not covered in this guide. URL Example:

```
https://examplesaname.blob.core.windows.net/vm-
images/9150.01000024.05090105.vhd
```

e) Clean up the managed disk

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

Exporte o arquivo VHD através da CLI do Azure a partir da máquina Linux local

1. Exporte a imagem do marketplace para um vhd através da CLI do Azure a partir de uma máquina Linux local.

Veja os passos

```
#Azure CLI on local Linux machine to get VHD image from Azure Marketplace
a) Login Azure CLI and list marketplace images
% az login --use-device-code
To sign in, use a web browser to open the page
https://microsoft.com/devicelogin and enter the code XXXXXXXXXX to
authenticate.

% 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"
},
...

b) Create a new managed disk from the Marketplace image with the
matching image version
% 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.blob.core.windows.net/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxx-xxxx-xxxx-xxxx-
xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
}

% export diskAccessSAS="https://md-
xxxxxx.blob.core.windows.net/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
#To automate the process, the SAS needs to be extracted from the
standard output. This is not included in this guide.
```

c) export vhd from managed disk

Create a container with proper access level. As an example, a container named 'vm-images' with 'Container' access level is used here.

Get storage account access key, on Azure portal, 'Storage Accounts'/'examplesaname'/'Access Key'/'key1'/'key'/'show'/'<copy>'. There should be az command that can achieve the same, but this is not included in this guide.

```
% 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
}

#to check the status of the blob copying
% 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.blob.core.windows.net/xxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "status": "success",
    "statusDescription": null
  }
}
```

```
},  
....
```

d) Download the generated image to your server, e.g., a Linux machine.

Use "wget <URL of file examplesname/Containers/vm-images/9150.01000024.05090105.vhd>".

The URL is organized in a formatted way. For automation tasks, the following example could be used to derive the URL string. Otherwise, Azure CLI 'az' command could be issued to get the URL, which is not covered in this guide. URL Example:

```
https://examplesname.blob.core.windows.net/vm-images/9150.01000024.05090105.vhd
```

e) Clean up the managed disk

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

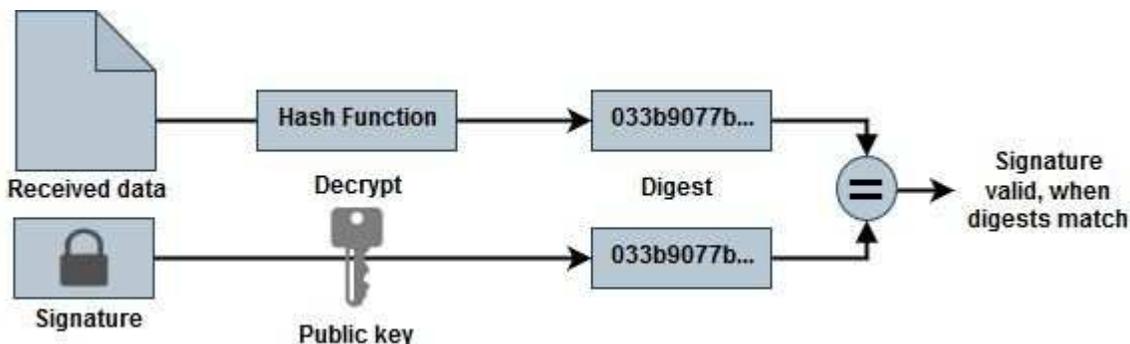
Verificação de assinatura de arquivo

Verificação de assinatura de arquivo

O processo de verificação de imagem do Azure gerará um resumo do arquivo VHD com o 1MB principal e o 512B final distribuído usando a função hash. Para corresponder ao procedimento de assinatura, SHA256 é usado para hash. Você precisa remover o 1MB principal e o 512B final do arquivo VHD e, em seguida, verificar a parte restante do arquivo VHD.

Resumo do fluxo de trabalho de verificação de assinatura de arquivo

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



- Baixe o arquivo Azure Image Digest do "[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).

"[Faça o download do arquivo de Digest da imagem do Azure](#)" Consulte para obter mais informações.

- Verifique a cadeia de confiança.
- Extraia a chave pública (.pub) do certificado de chave pública (.pem).
- A chave pública extraída é usada para descriptografar o arquivo de resumo. O resultado é então comparado com um novo resumo não criptografado do arquivo temporário criado a partir do arquivo de imagem com 1MB e terminando 512 bytes removidos.

Esta etapa é alcançada através do seguinte comando openssl.

- A instrução CLI geral aparece da seguinte forma:

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

- A ferramenta CLI OpenSSL dá uma mensagem "verificado OK" se ambos os arquivos corresponderem e "Falha de verificação" se eles não corresponderem.

Verificação de assinatura de arquivo no Linux

Você pode verificar uma assinatura de arquivo VHD exportada para Linux seguindo as etapas abaixo.

Passos

1. Baixe o arquivo Azure Image Digest do ["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 a ["Faça o download do arquivo de Digest da imagem do Azure"](#) para obter mais 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 os 1MB principais (1048576 bytes) e terminando 512 bytes do arquivo VHD.

Se 'tail' for usado, a opção '-c -K' produz bytes começando com os bytes KTH do arquivo especificado. Assim, 1048577 é passado 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 listrado (sign.tmp) com o arquivo de assinatura e chave pública.

Se o arquivo de entrada passar a verificação, o comando exibirá "Verificação OK". Caso contrário, a mensagem "Falha de verificação" será exibida.

```
% 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
```

Verificação de assinatura de arquivo no Mac os

Você pode verificar uma assinatura de arquivo VHD exportada para Mac os seguindo as etapas abaixo.

Passos

1. Baixe o arquivo Azure Image Digest do ["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 a ["Faça o download do arquivo de Digest da imagem do Azure"](#) para obter mais 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 o 1MB (1048576 bytes) e terminando 512 bytes do arquivo VHD.

Se 'tail' for usado, a opção '-c -K' produz bytes começando com os bytes KTH do arquivo especificado. Assim, 1048577 é passado para 'tail -c'. Leva cerca de 13m para que o comando tail seja concluído no Mac os.

```
% 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 listrado (sign.tmp) com o

arquivo de assinatura e chave pública.

Se o arquivo de entrada passar a verificação, o comando exibirá "Verificação OK". Caso contrário, a mensagem "Falha de verificação" será exibida.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0Pl_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
```

Onde encontrar informações adicionais sobre a verificação de imagens do Azure

Confira os links abaixo para obter informações adicionais sobre a Verificação de imagem do Azure. Os links abaixo levam você a sites não-NetApp.

Referências

- ["Page Fault Blog: Como assinar e verificar usando OpenSSL"](#)
- ["Use a imagem do Azure Marketplace para criar uma imagem de VM para a GPU do Azure Stack Edge Pro | Microsoft Learn"](#)
- ["Exporte/copie um disco gerenciado para uma conta de armazenamento usando a CLI do Azure | Microsoft Learn"](#)
- ["Guia de início rápido do Azure Cloud Shell - Bash | Microsoft Learn"](#)
- ["Como instalar a CLI do Azure | Microsoft Learn"](#)
- ["Cópia de blob de armazenamento az | Microsoft Learn"](#)
- ["Iniciar sessão com a CLI do Azure – Iniciar sessão e Autenticação | Microsoft Learn"](#)

Comece a usar o Google Cloud

Início rápido do Cloud Volumes ONTAP no Google Cloud

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

1

Crie um conetor

Se você ainda não tem um "Conetor", você precisa criar um. ["Saiba como criar um conetor no Google Cloud"](#)

Observe que, se você quiser implantar o Cloud Volumes ONTAP em uma sub-rede onde não há acesso à Internet disponível, precisará instalar manualmente o conetor e acessar a interface de usuário do BlueXP que está sendo executada nesse conetor. ["Saiba como instalar manualmente o conetor em um local sem acesso à Internet"](#)

2

Planeje sua configuração

O BlueXP oferece pacotes pré-configurados que atendem aos requisitos de carga de trabalho ou você pode criar sua própria configuração. Se você escolher sua própria configuração, você deve entender as opções disponíveis para você.

["Saiba mais sobre como Planejar sua configuração"](#).

3

Configure a rede

1. Certifique-se de que a VPC e as sub-redes suportem a conectividade entre o conetor e o Cloud Volumes ONTAP.
2. Se você pretende habilitar a disposição em camadas de dados ["Configure a sub-rede do Cloud Volumes ONTAP para o acesso privado do Google"](#), .
3. Se você estiver implantando um par de HA, verifique se você tem quatro VPCs, cada um com sua própria sub-rede.
4. Se você estiver usando uma VPC compartilhada, forneça a função *Compute Network User* à conta de serviço do Connector.
5. Ative o acesso de saída à Internet a partir da VPC de destino para 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

Configure uma conta de serviço

O Cloud Volumes ONTAP requer uma conta de serviço do Google Cloud para dois fins. A primeira é quando você pode ["categorização de dados"](#)categorizar dados inativos em storage de objetos de baixo custo no Google Cloud. A segunda é quando você permite que o ["Backup e recuperação do BlueXP"](#) faça backup de volumes para armazenamento de objetos de baixo custo.

Você pode configurar uma conta de serviço e usá-la para ambos os fins. A conta de serviço deve ter a função **Storage Admin**.

["Leia as instruções passo a passo"](#).

5

Habilite as APIs do Google Cloud

"[Ative as seguintes APIs do Google Cloud em seu projeto](#)". Essas APIs são necessárias para implantar o conector e o Cloud Volumes ONTAP.

- API do Cloud Deployment Manager V2
- API Cloud Logging
- API do Cloud Resource Manager
- API do mecanismo de computação
- API de gerenciamento de identidade e acesso (IAM)

6

Inicie o Cloud Volumes ONTAP usando o BlueXP

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

Links relacionados

- "[Criando um conector a partir do BlueXP](#) "
- "[Instalar o software Connector em um host Linux](#)"
- "[O que o BlueXP faz com as permissões do Google Cloud](#)"

Planeje sua configuração do Cloud Volumes ONTAP no Google Cloud

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

Escolha uma licença 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 para o Cloud Volumes ONTAP](#)"
- "[Saiba como configurar o licenciamento](#)"

Escolha uma região suportada

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

Escolha um tipo de máquina suportado

O Cloud Volumes ONTAP suporta vários tipos de máquina, dependendo do tipo de licença que você escolher.

"[Configurações compatíveis com o Cloud Volumes ONTAP no GCP](#)"

Entenda os limites de armazenamento

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

planeja sua configuração.

["Limites de storage para Cloud Volumes ONTAP no GCP"](#)

Dimensione seu sistema no GCP

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

Tipo de máquina

Veja os tipos de máquina suportados no ["Notas de versão do Cloud Volumes ONTAP"](#) e, em seguida, reveja os detalhes do Google sobre cada tipo de máquina suportado. Combine seus requisitos de carga de trabalho com o número de vCPUs e memória para o tipo de máquina. Observe que cada núcleo da CPU aumenta o desempenho da rede.

Consulte o seguinte para obter mais detalhes:

- ["Documentação do Google Cloud: N1 tipos de máquina padrão"](#)
- ["Documentação do Google Cloud: Desempenho"](#)

Tipo de disco do GCP

Ao criar volumes para Cloud Volumes ONTAP, você precisa escolher o storage de nuvem subjacente que o Cloud Volumes ONTAP usa para um disco. O tipo de disco pode ser qualquer um dos seguintes:

- *Zonal SSD Persistent Disks*: Os discos persistentes SSD são melhores para cargas de trabalho que exigem altas taxas de IOPS aleatórias.
- *Discos persistentes balanceados zonais*: Esses SSDs equilibram desempenho e custo fornecendo IOPS mais baixos por GB.
- *Zonal Standard Persistent Disks* : os discos persistentes padrão são econômicos e podem lidar com operações de leitura/gravação sequenciais.

Para obter mais detalhes, ["Documentação do Google Cloud: Discos persistentes zonais \(padrão e SSD\)"](#) consulte .

Tamanho do disco do GCP

Você precisa escolher um tamanho de disco inicial ao implantar um sistema Cloud Volumes ONTAP. Depois disso, você pode permitir que o BlueXP gerencie a capacidade de um sistema para você, mas se quiser construir agregados, esteja ciente do seguinte:

- Todos os discos em um agregado devem ter o mesmo tamanho.
- Determine o espaço de que você precisa, levando em consideração o desempenho.
- O desempenho dos discos persistentes é dimensionado automaticamente com o tamanho do disco e o número de vCPUs disponíveis para o sistema.

Consulte o seguinte para obter mais detalhes:

- ["Documentação do Google Cloud: Discos persistentes zonais \(padrão e SSD\)"](#)
- ["Documentação do Google Cloud: Otimizando o desempenho do disco persistente e do SSD local"](#)

Exibir discos do sistema padrão

Além do storage para dados de usuário, a BlueXP também compra storage de nuvem para dados de sistema do Cloud Volumes ONTAP (dados de inicialização, dados de raiz, dados básicos e NVRAM). Para fins de Planejamento, pode ajudar você a analisar esses detalhes antes de implantar o Cloud Volumes ONTAP.

- ["Exibir os discos padrão para os dados do sistema Cloud Volumes ONTAP no Google Cloud"](#).
- ["Google Cloud docs: Cotas de recursos"](#)

O Google Cloud Compute Engine impõe cotas sobre o uso de recursos, portanto, você deve garantir que não atingiu seu limite antes de implantar o Cloud Volumes ONTAP.



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

Colete informações de rede

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

Informações de rede para um sistema de nó único

Informações do GCP	O seu valor
Região	
Zona	
Rede VPC	
Sub-rede	
Política de firewall (se estiver usando a sua própria)	

Informações de rede para um par de HA em várias zonas

Informações do GCP	O seu valor
Região	
Zona para o nó 1	
Zona para o nó 2	
Zona para o mediador	
VPC-0 e sub-rede	
VPC-1 e sub-rede	
VPC-2 e sub-rede	
VPC-3 e sub-rede	
Política de firewall (se estiver usando a sua própria)	

Informações de rede para um par de HA em uma única zona

Informações do GCP	O seu valor
Região	
Zona	
VPC-0 e sub-rede	
VPC-1 e sub-rede	
VPC-2 e sub-rede	
VPC-3 e sub-rede	
Política de firewall (se estiver usando a sua própria)	

Escolha uma velocidade de gravação

O BlueXP permite escolher uma configuração de velocidade de gravação para o Cloud Volumes ONTAP, exceto para pares de alta disponibilidade (HA) no Google Cloud. Antes de escolher uma velocidade de gravação, você deve entender as diferenças entre as configurações normal e alta e os riscos e recomendações ao usar alta velocidade de gravação. ["Saiba mais sobre a velocidade de escrita"](#).

Escolha um perfil de uso de volume

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

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

Thin Provisioning

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

Deduplicação

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

Compactação

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

Requisitos de rede para o Cloud Volumes ONTAP no Google Cloud

Configure sua rede do Google Cloud para que os sistemas Cloud Volumes ONTAP possam funcionar corretamente.

Se você quiser implantar um par de HA, deve ["Saiba como os pares de HA funcionam no Google Cloud"](#).

Requisitos para o Cloud Volumes ONTAP

Os requisitos a seguir devem ser atendidos no Google Cloud.

Requisitos específicos para sistemas de nó único

Se você quiser implantar um sistema de nó único, certifique-se de que sua rede atenda aos seguintes requisitos.

Uma VPC

Uma Virtual Private Cloud (VPC) é necessária para um sistema de nó único.

Endereços IP privados

O BlueXP aloca 3 ou 4 endereços IP privados para um sistema de nó único no Google Cloud.

Você pode ignorar a criação do LIF de gerenciamento de VM de storage (SVM) se implantar o Cloud Volumes ONTAP usando a API e especificar o seguinte sinalizador:

```
skipSvmManagementLif: true
```



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

Requisitos específicos para pares de HA

Se você quiser implantar um par de HA, verifique se sua rede atende aos requisitos a seguir.

Uma ou várias zonas

Você pode garantir a alta disponibilidade de seus dados implantando uma configuração de HA em várias ou em uma única zona. O BlueXP solicitará que você escolha várias zonas ou uma única zona ao criar o par de HA.

- Várias zonas (recomendado)

A implantação de uma configuração de HA em três zonas garante a disponibilidade contínua dos dados em caso de falha em uma zona. Observe que o desempenho de gravação é um pouco menor em comparação com o uso de uma única zona, mas é mínimo.

- Zona única

Quando implantada em uma única zona, uma configuração do Cloud Volumes ONTAP HA usa uma política de posicionamento de distribuição. Essa política garante que uma configuração de HA seja protegida de um ponto único de falha na zona, sem ter que usar zonas separadas para conseguir o isolamento de falhas.

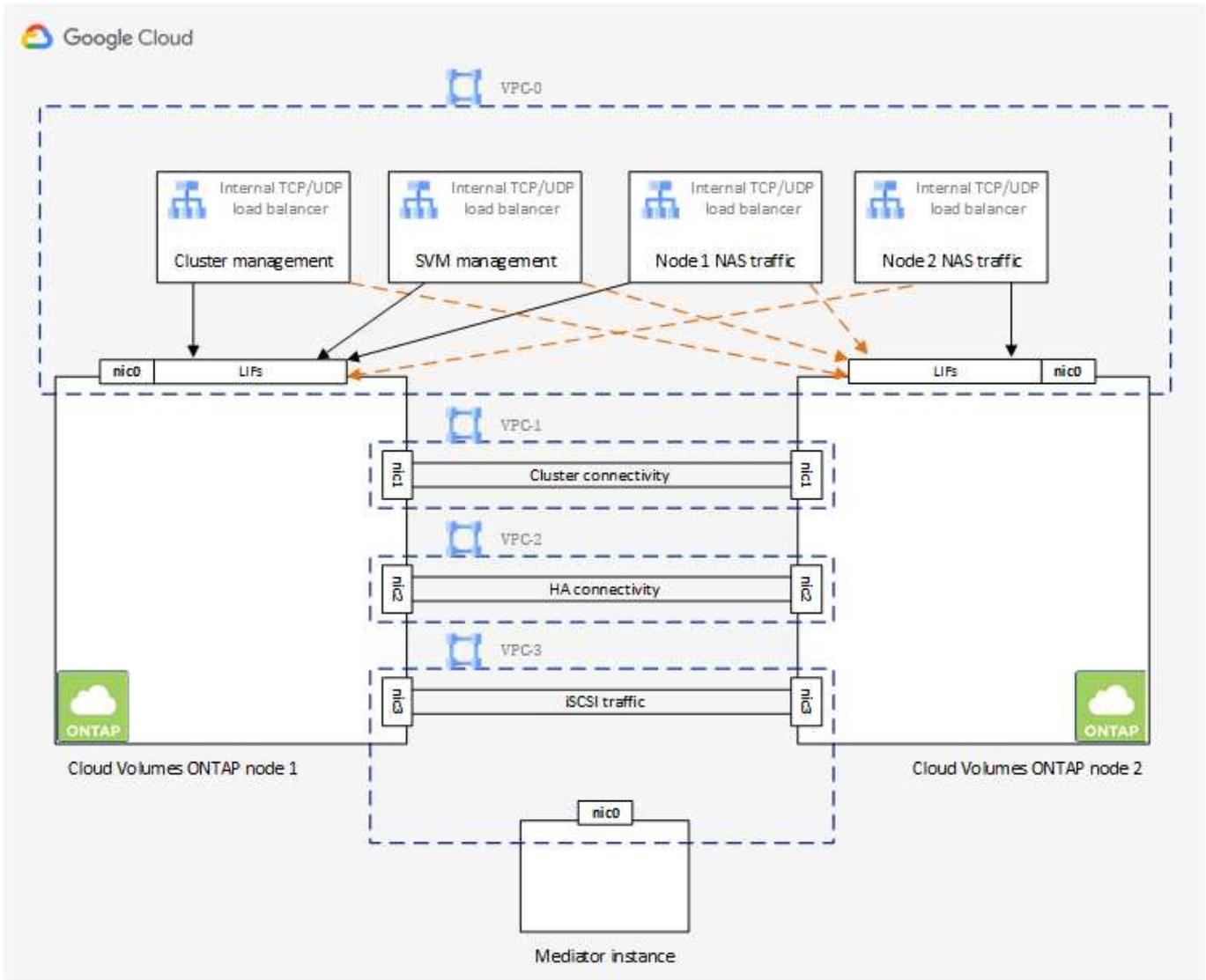
Esse modelo de implantação reduz seus custos porque não há cobranças de saída de dados entre zonas.

Quatro nuvens privadas virtuais

São necessárias quatro nuvens privadas virtuais (VPCs) para uma configuração de HA. Quatro VPCs são necessários porque o Google Cloud exige que cada interface de rede resida em uma rede VPC separada.

O BlueXP solicitará que você escolha quatro VPCs quando você criar o par HA:

- VPC-0 para conexões de entrada para os dados e nós
- VPC-1, VPC-2 e VPC-3 para comunicação interna entre os nós e o mediador do HA



Sub-redes

Uma sub-rede privada é necessária para cada VPC.

Se você colocar o conector na VPC-0, será necessário habilitar o acesso privado do Google na sub-rede para acessar as APIs e habilitar a disposição de dados em categorias.

As sub-redes nesses VPCs devem ter intervalos CIDR distintos. Eles não podem ter intervalos CIDR sobrepostos.

Endereços IP privados

O BlueXP aloca automaticamente o número necessário de endereços IP privados para o Cloud Volumes ONTAP no Google Cloud. Você precisa se certificar de que sua rede tem endereços privados suficientes disponíveis.

O número de LIFs alocadas pelo BlueXP para Cloud Volumes ONTAP depende da implantação de um único sistema de nós ou de um par de HA. Um LIF é um endereço IP associado a uma porta física. É necessário um LIF de gerenciamento de SVM para ferramentas de gerenciamento como o SnapCenter.

- *** Nó único*** BlueXP aloca 4 endereços IP para um sistema de nó único:

- LIF de gerenciamento de nós
- LIF de gerenciamento de clusters
- LIF de dados iSCSI



Um iSCSI LIF fornece acesso ao cliente através do protocolo iSCSI e é utilizado pelo sistema para outros fluxos de trabalho de rede importantes. Estes LIFs são necessários e não devem ser excluídos.

- LIF NAS

Você pode ignorar a criação do LIF de gerenciamento de VM de storage (SVM) se implantar o Cloud Volumes ONTAP usando a API e especificar o seguinte sinalizador:

```
skipSvmManagementLif: true
```

- **Par HA** BlueXP aloca 12-13 endereços IP para um par HA:

- LIFs de gerenciamento de nós de 2 (e0a)
- 1 LIF de gerenciamento de clusters (e0a)
- iSCSI LIFs de 2 GB (e0a GB)



Um iSCSI LIF fornece acesso ao cliente através do protocolo iSCSI e é utilizado pelo sistema para outros fluxos de trabalho de rede importantes. Estes LIFs são necessários e não devem ser excluídos.

- 1 ou 2 LIFs nas (e0a)
- 2 LIFs de cluster (e0b)
- 2 endereços IP de interconexão HA (e0c)
- 2 endereços IP iSCSI RSM (e0d)

Você pode ignorar a criação do LIF de gerenciamento de VM de storage (SVM) se implantar o Cloud Volumes ONTAP usando a API e especificar o seguinte sinalizador:

```
skipSvmManagementLif: true
```

Balancedores de carga internos

O BlueXP cria automaticamente quatro balanceadores de carga internos (TCP/UDP) do Google Cloud que gerenciam o tráfego de entrada para o par de HA do Cloud Volumes ONTAP. Nenhuma configuração é necessária a partir do seu final Listamos isso como um requisito simplesmente para informá-lo sobre o tráfego de rede e para mitigar quaisquer preocupações de segurança.

Um balanceador de carga é para gerenciamento de clusters, um é para gerenciamento de VM de storage (SVM), um é para tráfego nas para o nó 1 e o último é para tráfego nas para o nó 2.

A configuração para cada balanceador de carga é a seguinte:

- Um endereço IP privado compartilhado
- Uma verificação global de saúde

Por padrão, as portas usadas pela verificação de integridade são 63001, 63002 e 63003.

- Um serviço regional de back-end TCP
- Um serviço regional de backend UDP
- Uma regra de encaminhamento TCP
- Uma regra de encaminhamento UDP
- O acesso global está desativado

Mesmo que o acesso global esteja desativado por padrão, a ativação pós-implantação de TI é suportada. Desabilitamos isso porque o tráfego entre regiões terá latências significativamente maiores. Queríamos garantir que você não tivesse uma experiência negativa devido a montagens acidentais de região cruzada. Ativar esta opção é específico para as necessidades da sua empresa.

VPCs compartilhados

O Cloud Volumes ONTAP e o conector são suportados em uma VPC compartilhada do Google Cloud e também em VPCs autônomos.

Para um sistema de nó único, a VPC pode ser uma VPC compartilhada ou uma VPC autônoma.

Para um par de HA, são necessários quatro VPCs. Cada um desses VPCs pode ser compartilhado ou autônomo. Por exemplo, a VPC-0 pode ser uma VPC compartilhada, enquanto a VPC-1, a VPC-2 e a VPC-3 podem ser VPCs autônomos.

Uma VPC compartilhada permite que você configure e gerencie centralmente redes virtuais em vários projetos. Você pode configurar redes VPC compartilhadas no *projeto host* e implantar as instâncias de máquina virtual Connector e Cloud Volumes ONTAP em um *projeto de serviço*. "[Documentação do Google Cloud: Visão geral da VPC compartilhada](#)".

["Revise as permissões de VPC compartilhada necessárias cobertas na implantação do Connector"](#)

Espelhamento de pacotes em VPCs

["Espelhamento de pacotes"](#) Deve ser desabilitado na sub-rede do Google Cloud na qual você implanta o Cloud Volumes ONTAP.

Acesso de saída à Internet

Os nós de Cloud Volumes ONTAP requerem acesso de saída à Internet para acessar endpoints externos para várias funções. O Cloud Volumes ONTAP não pode funcionar corretamente se esses endpoints forem bloqueados em ambientes com requisitos rígidos de segurança.

Pontos de extremidade Cloud Volumes ONTAP

O Cloud Volumes ONTAP requer acesso de saída à Internet para contactar vários endpoints para operações diárias.

Os seguintes endpoints são específicos do Cloud Volumes ONTAP. O conector também entra em Contato com

vários endpoints para operações diárias, bem como com o console baseado na Web do BlueXP . "Veja os pontos finais contactados a partir do conetor"Consulte e "Prepare a rede para usar o console BlueXP " .

Endpoints	Aplicável para	Finalidade	Modo de implantação do BlueXP	Impacto se o endpoint não estiver disponível
https://NetApp-cloud-account.auth0.com	Autenticação	Usado para autenticação BlueXP .	Modos padrão e restritos.	A autenticação do usuário falha e os seguintes serviços permanecem indisponíveis: <ul style="list-style-type: none"> • Serviços da Cloud Volumes ONTAP • Serviços da ONTAP • Protocolos e serviços proxy
https://keyvault-production-aks.vault.azure.net	Cofre de chaves	Usado para recuperar a chave secreta do cliente do Azure Key Vault para se comunicar com o bucket do S3 para manipulação de metadados. O serviço Cloud Volumes ONTAP usa esse componente internamente.	Modos padrão, restrito e privado.	Os serviços Cloud Volumes ONTAP não estão disponíveis.
https://cloudmanager.cloud.NetApp.com/locação	Alocação	Usado para recuperar os recursos do Cloud Volumes ONTAP da BlueXP Locancy para autorizar recursos e usuários.	Modos padrão e restritos.	Os recursos do Cloud Volumes ONTAP e os usuários não estão autorizados.
https://support.NetApp.com/aods/asupmessage https://support.NetApp.com/asupprod/post/1,0/postAsup	AutoSupport	Usado para enviar dados de telemetria do AutoSupport para o suporte do NetApp.	Modos padrão e restritos.	As informações do AutoSupport permanecem não entregues.

Endpoints	Aplicável para	Finalidade	Modo de implantação do BlueXP	Impacto se o endpoint não estiver disponível
https://www.googleapis.com/compute/v1/projects/ https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects https://compute.googleapis.com/compute/v1	Google Cloud (uso comercial).	Comunicação com os serviços do Google Cloud.	Modos padrão, restrito e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço Google Cloud para executar operações específicas do BlueXP no Google Cloud.

Acesso de saída à Internet para NetApp AutoSupport

O Cloud Volumes ONTAP requer acesso de saída à Internet para NetApp AutoSupport, que monitora proativamente a integridade do sistema e envia mensagens para o suporte técnico da NetApp.

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

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

Se uma conexão de saída à Internet não estiver disponível para enviar mensagens AutoSupport, o BlueXP configura automaticamente seus sistemas Cloud Volumes ONTAP para usar o conector como um servidor proxy. O único requisito é garantir que o firewall do conector permita conexões *inbound* pela porta 3128. Você precisará abrir essa porta depois de implantar o conector.

Se você definiu regras de saída rígidas para o Cloud Volumes ONTAP, também precisará garantir que o firewall do Cloud Volumes ONTAP permita conexões *de saída* pela porta 3128.

Depois de verificar que o acesso de saída à Internet está disponível, você pode testar o AutoSupport para garantir que ele possa enviar mensagens. Para obter instruções, "[ONTAP docs: Configurar o AutoSupport](#)" consulte .



Se você estiver usando um par de HA, o mediador de HA não precisará de acesso de saída à Internet.

Se o BlueXP notificar que as mensagens do AutoSupport não podem ser enviadas, "[Solucionar problemas da configuração do AutoSupport](#)".

Conexões com sistemas ONTAP em outras redes

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

Para obter instruções, "[Documentação do Google Cloud: Visão geral do Cloud VPN](#)" consulte .

Regras de firewall

O BlueXP cria regras de firewall do Google Cloud que incluem as regras de entrada e saída que o Cloud Volumes ONTAP precisa para operar com sucesso. Você pode querer consultar as portas para fins de teste ou se preferir usar suas próprias regras de firewall.

As regras de firewall para o Cloud Volumes ONTAP exigem regras de entrada e saída. Se você estiver implantando uma configuração de HA, essas são as regras de firewall do Cloud Volumes ONTAP na VPC-0.

Observe que dois conjuntos de regras de firewall são necessários para uma configuração de HA:

- Um conjunto de regras para componentes do HA no VPC-0. Essas regras permitem o acesso aos dados ao Cloud Volumes ONTAP.
- Outro conjunto de regras para componentes do HA no VPC-1, VPC-2 e VPC-3. Essas regras estão abertas para comunicação de entrada e saída entre os componentes do HA. [Saiba mais](#).



Procurando informações sobre o conetor? "[Ver regras de firewall para o conetor](#)"

Regras de entrada

Ao criar um ambiente de trabalho, você pode escolher o filtro de origem para a política de firewall predefinida durante a implantação:

- **Somente VPC selecionada:** O filtro de origem para o tráfego de entrada é o intervalo de sub-rede da VPC para o sistema Cloud Volumes ONTAP e o intervalo de sub-rede da VPC onde o conetor reside. Esta é a opção recomendada.
- **Todos os VPCs:** O filtro de origem para o tráfego de entrada é o intervalo IP 0,0.0.0/0.

Se você usar sua própria política de firewall, certifique-se de adicionar todas as redes que precisam se comunicar com o Cloud Volumes ONTAP, mas também certifique-se de adicionar ambos os intervalos de endereços para permitir que o Google Load Balancer interno funcione corretamente. Esses endereços são 130.211.0.0/22 e 35.191.0.0/16. Para obter mais informações, "[Documentação do Google Cloud: Regras do Firewall do Load Balancer](#)" consulte .

Protocolo	Porta	Finalidade
Todo o ICMP	Tudo	Fazer ping na instância

Protocolo	Porta	Finalidade
HTTP	80	Acesso HTTP ao console da Web do Gerenciador de sistema do ONTAP usando o endereço IP do LIF de gerenciamento de cluster
HTTPS	443	Conetividade com o conetor e acesso HTTPS à consola Web do Gestor de sistema ONTAP utilizando o endereço IP do LIF de gestão de clusters
SSH	22	Acesso SSH ao endereço IP do LIF de gerenciamento de cluster ou um LIF de gerenciamento de nó
TCP	111	Chamada de procedimento remoto para NFS
TCP	139	Sessão de serviço NetBIOS para CIFS
TCP	161-162	Protocolo de gerenciamento de rede simples
TCP	445	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
TCP	635	Montagem em NFS
TCP	749	Kerberos
TCP	2049	Daemon do servidor NFS
TCP	3260	Acesso iSCSI através do iSCSI data LIF
TCP	4045	Daemon de bloqueio NFS
TCP	4046	Monitor de status da rede para NFS
TCP	10000	Backup usando NDMP
TCP	11104	Gestão de sessões de comunicação entre clusters para SnapMirror
TCP	11105	Transferência de dados SnapMirror usando LIFs entre clusters
TCP	63001-63050	Portas da sonda de balanceamento de carga para determinar qual nó está em bom estado (necessário apenas para pares de HA)
UDP	111	Chamada de procedimento remoto para NFS
UDP	161-162	Protocolo de gerenciamento de rede simples
UDP	635	Montagem em NFS
UDP	2049	Daemon do servidor NFS
UDP	4045	Daemon de bloqueio NFS
UDP	4046	Monitor de status da rede para NFS
UDP	4049	Protocolo rquotad NFS

Regras de saída

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

Regras básicas de saída

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

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

Regras de saída avançadas

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



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

Serviço	Protocolo	Porta	Fonte	Destino	Finalidade
Active Directory					

Serviço	Protocolo	Porta	Destino	Destino	Finalidade
	TCP	445	DATA LIF (NFS, CIFS)	Floresta do ativo Directory	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
	TCP	445	DATA LIF (NFS, CIFS)	Floresta do ativo Directory	Permitir alterar e definir senha (SET_CHANGE)
	UDP	464	DATA LIF (NFS, CIFS)	Floresta do ativo Directory	Administração de chaves Kerberos
	TCP	749	DATA LIF (NFS, CIFS)	Floresta do ativo Directory	Palavra-passe de alteração e definição Kerberos V (RPCSEC_GSS)
AutoSupport	HTTPS	443	LIF de gerenciamento de nós	suporte.NetApp.com	AutoSupport (HTTPS é o padrão)
	HTTP	80	LIF de gerenciamento de nós	suporte.NetApp.com	AutoSupport (somente se o protocolo de transporte for alterado de HTTPS para HTTP)
	TCP	3128	LIF de gerenciamento de nós	Conetor	Enviar mensagens AutoSupport através de um servidor proxy no conetor, se uma conexão de saída de Internet não estiver disponível
Cluster	Todo o tráfego	Todo o tráfego	Todos os LIFs em um nó	Todos os LIFs no outro nó	Comunicações entre clusters (apenas Cloud Volumes ONTAP HA)
Backups de configuração	HTTP	80	LIF de gerenciamento de nós	Http://<connector-IP-address>/occm/offbo xconfig	Envie backups de configuração para o conetor. "Saiba mais sobre arquivos de backup de configuração" .
DHCP	UDP	68	LIF de gerenciamento de nós	DHCP	Cliente DHCP para configuração pela primeira vez
DHCPS	UDP	67	LIF de gerenciamento de nós	DHCP	Servidor DHCP
DNS	UDP	53	LIF e LIF de dados de gerenciamento de nós (NFS, CIFS)	DNS	DNS
NDMP	TCP	1860-18699	LIF de gerenciamento de nós	Servidores de destino	Cópia NDMP
SMTP	TCP	25	LIF de gerenciamento de nós	Servidor de correio	Alertas SMTP, podem ser usados para AutoSupport

Serviço	Protocolo	Porta	Fonte	Destino	Finalidade
SNMP	TCP	161	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
	UDP	161	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
	TCP	162	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
	UDP	162	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
SnapMirror	TCP	11104	LIF entre clusters	LIFs ONTAP entre clusters	Gestão de sessões de comunicação entre clusters para SnapMirror
	TCP	11105	LIF entre clusters	LIFs ONTAP entre clusters	Transferência de dados SnapMirror
Syslog	UDP	514	LIF de gerenciamento de nós	Servidor syslog	Mensagens de encaminhamento do syslog

Regras para VPC-1, VPC-2 e VPC-3

No Google Cloud, uma configuração de HA é implantada em quatro VPCs. As regras de firewall necessárias para a configuração de HA na VPC-0 são [Listado acima para Cloud Volumes ONTAP](#).

Enquanto isso, as regras de firewall predefinidas que o BlueXP cria para instâncias no VPC-1, VPC-2 e VPC-3 permitem a comunicação de entrada em protocolos e portas *All*. Essas regras permitem a comunicação entre nós de HA.

A comunicação dos nós de HA para o mediador de HA ocorre na porta 3260 (iSCSI).



Para habilitar a alta velocidade de gravação para novas implantações de par de HA do Google Cloud, é necessária uma unidade máxima de transmissão (MTU) de pelo menos 8.896 bytes para VPC-1, VPC-2 e VPC-3. Se você optar por atualizar VPC-1, VPC-2 e VPC-3 existentes para uma MTU de 8.896 bytes, será necessário encerrar todos os sistemas HA existentes usando esses VPCs durante o processo de configuração.

Requisitos para o conetor

Se você ainda não criou um conetor, você deve rever os requisitos de rede para o conetor também.

- ["Veja os requisitos de rede para o conetor"](#)
- ["Regras de firewall no Google Cloud"](#)

Planejamento de controles de serviço VPC no Google Cloud

Ao optar por bloquear seu ambiente do Google Cloud com controles de serviço de VPC, você deve entender como o BlueXP e o Cloud Volumes ONTAP interagem com as APIs do Google Cloud, bem como como configurar seu perímetro de serviço para implantar o BlueXP e o Cloud Volumes ONTAP.

Os controles de serviço da VPC permitem que você controle o acesso a serviços gerenciados do Google fora de um perímetro confiável, bloqueie o acesso a dados de locais não confiáveis e reduza riscos de transferência de dados não autorizados. ["Saiba mais sobre os controles do serviço VPC do Google Cloud"](#).

Como os serviços do NetApp se comunicam com os controles de serviço da VPC

O BlueXP se comunica diretamente com as APIs do Google Cloud. Isso é acionado a partir de um endereço IP externo fora do Google Cloud (por exemplo, de `api.services.cloud.NetApp.com`) ou dentro do Google Cloud a partir de um endereço interno atribuído ao BlueXP Connector.

Dependendo do estilo de implantação do conector, algumas exceções podem ter que ser feitas para o perímetro de serviço.

Imagens

Tanto o Cloud Volumes ONTAP quanto o BlueXP usam imagens de um projeto dentro do GCP gerenciado pelo NetApp. Isso pode afetar a implantação do BlueXP Connector e do Cloud Volumes ONTAP, se sua organização tiver uma política que bloqueie o uso de imagens que não estão hospedadas na organização.

Você pode implantar um conector manualmente usando o método de instalação manual, mas o Cloud Volumes ONTAP também precisará extrair imagens do projeto NetApp. Você deve fornecer uma lista permitida para implantar um conector e Cloud Volumes ONTAP.

Implantação de um conector

O usuário que implanta um conector precisa ser capaz de fazer referência a uma imagem hospedada no ProjectID *NetApp-cloudmanager* e ao número do projeto *14190056516*.

Implantando o Cloud Volumes ONTAP

- A conta de serviço do BlueXP precisa fazer referência a uma imagem hospedada no ProjectID *NetApp-cloudmanager* e ao número do projeto de serviço *14190056516*.
- A conta de serviço do Agente de Serviço de APIs do Google padrão precisa fazer referência a uma imagem hospedada no ProjectID *NetApp-cloudmanager* e ao número do projeto de serviço *14190056516*.

Exemplos das regras necessárias para extrair essas imagens com os controles de Serviço da VPC são definidos abaixo.

O Serviço VPC controla as políticas de perímetro

As políticas permitem exceções aos conjuntos de regras de controles de serviço da VPC. Para obter mais informações sobre as políticas, visite o ["Documentação da Política de controles do Serviço VPC do GCP"](#).

Para definir as políticas que o BlueXP exige, navegue até o perímetro de controles de serviço da VPC na sua organização e adicione as seguintes políticas. Os campos devem corresponder às opções fornecidas na página de política de controles de serviço da VPC. Observe também que as regras **todas** são necessárias e os parâmetros **OU** devem ser usados no conjunto de regras.

Regras de entrada

```
From:
  Identities:
    [User Email Address]
  Source > All sources allowed
To:
  Projects =
    [Service Project]
  Services =
    Service name: iam.googleapis.com
      Service methods: All actions
    Service name: compute.googleapis.com
      Service methods: All actions
```

OU

```
From:
  Identities:
    [User Email Address]
  Source > All sources allowed
To:
  Projects =
    [Host Project]
  Services =
    Service name: compute.googleapis.com
      Service methods: All actions
```

OU

```
From:
  Identities:
    [Service Project Number]@cloudservices.gserviceaccount.com
  Source > All sources allowed
To:
  Projects =
    [Service Project]
    [Host Project]
  Services =
    Service name: compute.googleapis.com
      Service methods: All actions
```

Regras de saída

```
From:
  Identities:
    [Service Project Number]@cloudservices.gserviceaccount.com
To:
  Projects =
    14190056516
  Service =
    Service name: compute.googleapis.com
    Service methods: All actions
```



O número do projeto descrito acima é o projeto *NetApp-cloudmanager* usado pelo NetApp para armazenar imagens para o conector e para o Cloud Volumes ONTAP.

Criar uma conta de serviço para disposição de dados em categorias e backups

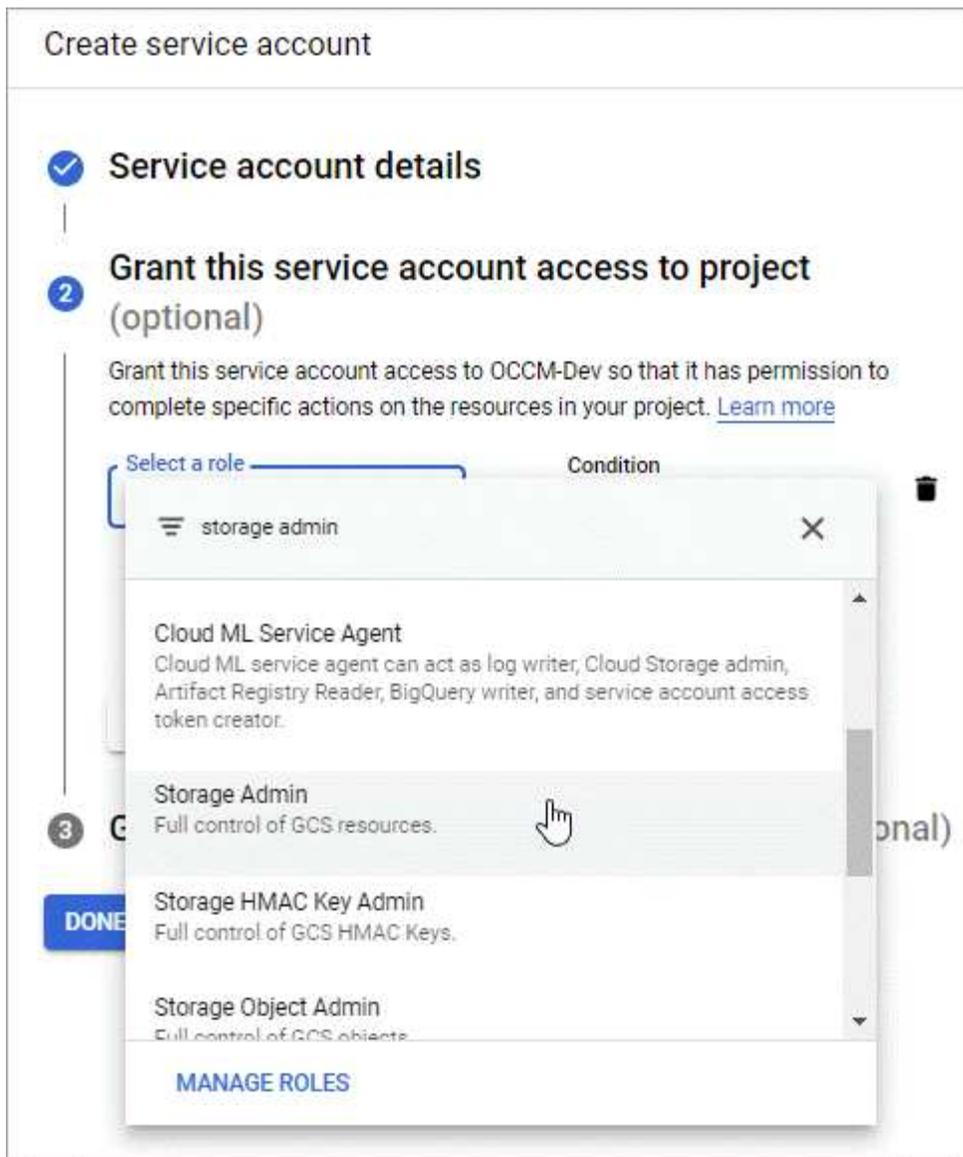
O Cloud Volumes ONTAP requer uma conta de serviço do Google Cloud para dois fins. A primeira é quando você pode "[categorização de dados](#)" categorizar dados inativos em storage de objetos de baixo custo no Google Cloud. A segunda é quando você permite que o "[Backup e recuperação do BlueXP](#)" faça backup de volumes para armazenamento de objetos de baixo custo.

O Cloud Volumes ONTAP usa a conta de serviço para acessar e gerenciar um bucket de dados em camadas e outro bucket de backups.

Você pode configurar uma conta de serviço e usá-la para ambos os fins. A conta de serviço deve ter a função **Storage Admin**.

Passos

1. No console do Google Cloud, "[Vá para a página Contas de Serviço](#)".
2. Selecione seu projeto.
3. Clique em **criar conta de serviço** e forneça as informações necessárias.
 - a. **Detalhes da conta de serviço**: Insira um nome e uma descrição.
 - b. **Conceder acesso a esta conta de serviço ao projeto**: Selecione a função **Administrador de armazenamento**.



- c. **Conceder aos usuários acesso a esta conta de serviço:** Adicione a conta de serviço Connector como *Usuário da conta de serviço* a esta nova conta de serviço.

Essa etapa é necessária apenas para categorização de dados. Não é necessário para backup e recuperação do BlueXP .

Create service account

- ✓ Service account details
- ✓ Grant this service account access to project (optional)
- 3 Grant users access to this service account (optional)
Grant access to users or groups that need to perform actions as this service account. [Learn more](#)

Service account users role

netapp-cloud-manager@iam.gserviceaccount.com

Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role

Grant users the permission to administer this service account

DONE CANCEL

O que se segue?

Você precisará selecionar a conta de serviço mais tarde quando criar um ambiente de trabalho do Cloud Volumes ONTAP.

Details and Credentials

default-project Google Cloud Project	gcp-sub2 Marketplace Subscription	Edit Project
---	--------------------------------------	------------------------------

Details

Working Environment Name (Cluster Name)

Service Account

Service Account Name

[+ Add Labels](#) Optional Field | Up to four labels

Credentials

User Name

Password

Confirm Password

Usando chaves de criptografia gerenciadas pelo cliente com o Cloud Volumes ONTAP

Embora o Google Cloud Storage sempre criptografe seus dados antes de serem gravados no disco, você pode usar a API BlueXP para criar um sistema Cloud Volumes ONTAP que use *chaves de criptografia gerenciadas pelo cliente*. Essas são as chaves que você gera e gerencia no GCP usando o Cloud Key Management Service.

Passos

1. Certifique-se de que a conta de serviço do BlueXP Connector tenha as permissões corretas no nível do projeto, no projeto em que a chave é armazenada.

As permissões são fornecidas no "[Permissões de conta de serviço do conector por padrão](#)", mas podem não ser aplicadas se você usar um projeto alternativo para o Cloud Key Management Service.

As permissões são as seguintes:

```
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
```

2. Certifique-se de que a conta de serviço do "[Google Compute Engine Service Agent](#)" tem permissões de criptografia/Decrypter do Cloud KMS na chave.

O nome da conta de serviço usa o seguinte formato: "Service-[Service_project_number] compute-system.iam.gserviceaccount.com".

["Documentação do Google Cloud: Usando o IAM com o Cloud KMS - concedendo funções em um recurso"](#)

3. Obtenha o "id" da chave invocando o comando GET para a `/gcp/vsa/metadata/gcp-encryption-keys` chamada da API ou escolhendo "Copy Resource Name" na chave no console do GCP.
4. Se estiver usando chaves de criptografia gerenciadas pelo cliente e disposição em camadas de dados no storage de objetos, o BlueXP tentará utilizar as mesmas chaves usadas para criptografar os discos persistentes. Mas primeiro você precisará habilitar os buckets do Google Cloud Storage para usar as chaves:
 - a. Localize o agente de serviço do Google Cloud Storage seguindo o ["Documentação do Google Cloud: Obtendo o agente de serviço do Cloud Storage"](#).
 - b. Navegue até a chave de criptografia e atribua ao agente de serviço do Google Cloud Storage com permissões de criptografia/Decrypter do Cloud KMS.

Para obter mais informações, consulte ["Documentação do Google Cloud: Usando chaves de criptografia gerenciadas pelo cliente"](#)

5. Use o parâmetro "GcpEncryption" com sua solicitação de API ao criar um ambiente de trabalho.

Exemplo

```
"gcpEncryptionParameters": {  
  "key": "projects/project-1/locations/us-east4/keyRings/keyring-  
1/cryptoKeys/generatedkey1"  
}
```

Consulte a ["Documentos de automação BlueXP"](#) para obter mais detalhes sobre como utilizar o parâmetro "GcpEncryption".

Configure o licenciamento para o Cloud Volumes ONTAP no Google Cloud

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

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 à esquerda, selecione **Storage > Canvas**.
2. Na página Canvas, clique em **Adicionar ambiente de trabalho** e siga as etapas no BlueXP .
 - 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 Google Cloud Marketplace.

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

b. Depois de voltar ao BlueXP , selecione **Freemium** quando chegar à página métodos de carregamento.

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 Google Cloud"](#).

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, Optimized ou Professional.

Os pacotes Essentials, Optimized e Professional estão disponíveis com os seguintes modelos de consumo:

- Uma licença (traga sua própria licença (BYOL)) comprada da NetApp
- Uma assinatura por hora, com pagamento conforme o uso (PAYGO) no Google Cloud Marketplace
- Um contrato anual

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

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

BYOL

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

Passos

1. ["Entre em Contato com a NetApp Sales para obter uma licença"](#)
2. ["Adicione sua conta do site de suporte da NetApp ao BlueXP "](#)

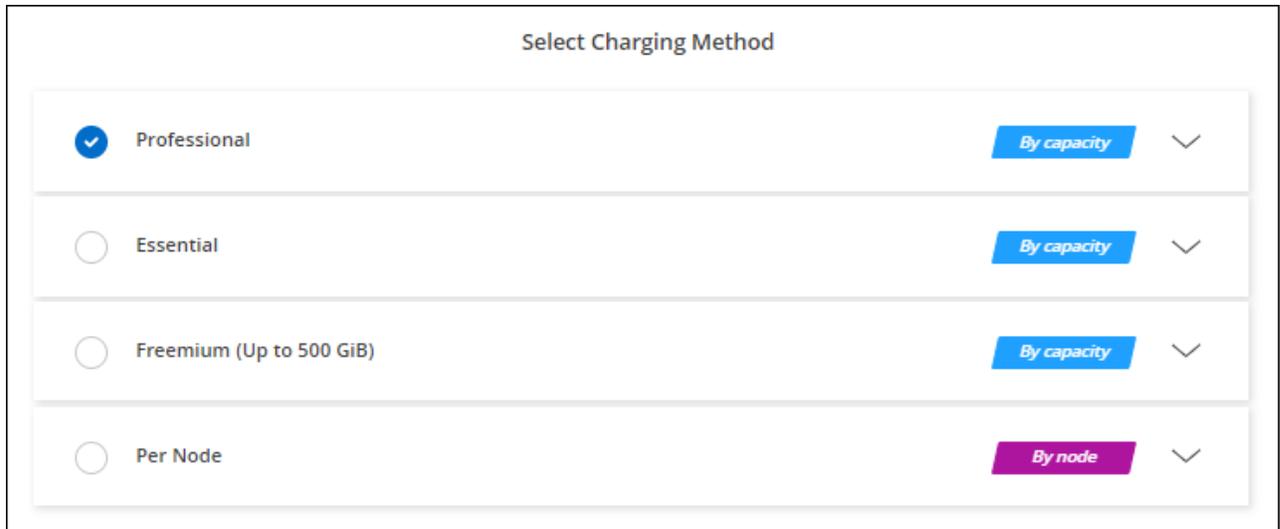
A BlueXP consulta automaticamente o serviço de licenciamento da NetApp para obter detalhes sobre as licenças associadas à sua conta do site de suporte da NetApp. Se não houver erros, o BlueXP adiciona automaticamente as licenças à carteira digital.

A sua licença tem de estar disponível na carteira digital BlueXP antes de a poder utilizar com o Cloud Volumes ONTAP. Se necessário, você pode ["Adicione manualmente a licença à carteira digital BlueXP"](#).

3. Na página Canvas, clique em **Adicionar ambiente de trabalho** e siga as etapas no BlueXP .
 - 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 Google Cloud Marketplace.

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

- b. Depois de voltar ao BlueXP , selecione um pacote baseado na capacidade quando chegar à página métodos de carregamento.



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

Subscrição PAYGO

Pague por hora assinando a oferta no mercado do seu provedor de nuvem.

Quando você cria um ambiente de trabalho do Cloud Volumes ONTAP, o BlueXP solicita que você assine o contrato disponível no Google Cloud Marketplace. Essa assinatura é então associada ao ambiente de trabalho para cobrança. Você pode usar essa mesma assinatura para ambientes de trabalho adicionais.

Passos

1. No menu de navegação à esquerda, selecione **Storage > Canvas**.
2. Na página Canvas, clique em **Adicionar ambiente de trabalho** e siga as etapas no BlueXP .
 - 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 Google Cloud Marketplace.
 - b. Depois de voltar ao BlueXP , selecione um pacote baseado na capacidade quando chegar à página métodos de carregamento.

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 Google Cloud".



Pode gerir as subscrições do Google Cloud Marketplace associadas às suas contas a partir da página Definições > credenciais. ["Saiba como gerenciar suas credenciais e assinaturas do Google Cloud"](#)

Contrato anual

Pague pelo Cloud Volumes ONTAP anualmente comprando um contrato anual.

Passos

1. Contacte o seu representante de vendas da NetApp para adquirir um contrato anual.

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

Depois que o NetApp compartilhar a oferta privada com você, você pode selecionar o plano anual ao se inscrever no Google Cloud Marketplace durante a criação do ambiente de trabalho.

2. Na página Canvas, clique em **Adicionar ambiente de trabalho** e siga as etapas no BlueXP .
 - a. Na página **Detalhes e credenciais**, clique em **Editar credenciais > Adicionar assinatura** e siga as instruções para assinar o plano anual no Google Cloud Marketplace.
 - b. No Google Cloud, selecione o plano anual que foi compartilhado com sua conta e clique em **Subscribe**.
 - c. Depois de voltar ao BlueXP , selecione um pacote baseado na capacidade quando chegar à página métodos de carregamento.

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 Google Cloud".

Inscrição no Keystone

Uma subscrição do Keystone é um serviço baseado em subscrição com pagamento conforme o uso. ["Saiba mais sobre as assinaturas do NetApp Keystone"](#).

Passos

1. Se você ainda não tem uma assinatura, ["Entre em Contato com a NetApp"](#)
2. Para autorizar sua conta de usuário do BlueXP com uma ou mais assinaturas do Keystone NetApp NetApp.
3. Depois que o NetApp autorizar sua conta ["Vincule suas assinaturas para uso com o Cloud Volumes ONTAP"](#), .
4. Na página Canvas, clique em **Adicionar ambiente de trabalho** e siga as etapas no BlueXP .
 - a. Selecione o método de cobrança da assinatura Keystone quando solicitado a escolher um método de cobrança.

Select Charging Method

KeystoneBy capacity^

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1v

ProfessionalBy capacityv

EssentialBy capacityv

Freemium (Up to 500 GiB)By capacityv

Per NodeBy nodev

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

Lançamento do Cloud Volumes ONTAP no Google Cloud

É possível iniciar o Cloud Volumes ONTAP em uma configuração de nó único ou como par de HA no Google Cloud.

Antes de começar

Você precisa do seguinte para criar um ambiente de trabalho.

- Um conector que está em funcionamento.
 - Você deve ter um ["Conector que está associado ao seu projeto ou área de trabalho"](#).
 - ["Você deve estar preparado para deixar o conector funcionando o tempo todo"](#).
 - A conta de serviço associada ao conector ["deve ter as permissões necessárias"](#)
- Uma compreensão da configuração que você deseja usar.

Você deve se preparar escolhendo uma configuração e obtendo informações de rede do Google Cloud do administrador. Para obter detalhes, ["Planejando sua configuração do Cloud Volumes ONTAP"](#) consulte .

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

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

- As APIs do Google Cloud devem ser "[habilitado em seu projeto](#)":
 - API do Cloud Deployment Manager V2
 - API Cloud Logging
 - API do Cloud Resource Manager
 - API do mecanismo de computação
 - API de gerenciamento de identidade e acesso (IAM)

Lançamento de um sistema de nó único no Google Cloud

Crie um ambiente de trabalho no BlueXP para iniciar o Cloud Volumes ONTAP no Google Cloud.

Passos

1. No menu de navegação à esquerda, selecione **Storage > Canvas**.
2. na página do Canvas, clique em **Adicionar ambiente de trabalho** e siga as instruções.
3. **Escolha um local**: Selecione **Google Cloud** e **Cloud Volumes ONTAP**.
4. Se for solicitado, "[Crie um conector](#)".
5. **Detalhes e credenciais**: Selecione um projeto, especifique um nome de cluster, selecione opcionalmente uma conta de serviço, adicione rótulos opcionalmente e especifique credenciais.

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

Campo	Descrição
Nome do ambiente de trabalho	O BlueXP usa o nome do ambiente de trabalho para nomear tanto o sistema Cloud Volumes ONTAP quanto a instância de VM do Google Cloud. Ele também usa o nome como prefixo para o grupo de segurança predefinido, se você selecionar essa opção.
Nome da conta de serviço	Se você planeja usar " categorização de dados " ou " Backup e recuperação do BlueXP " com o Cloud Volumes ONTAP, precisará ativar conta de serviço e selecionar uma conta de serviço que tenha a função de administrador de armazenamento predefinida. " Saiba como criar uma conta de serviço ".
Adicionar etiquetas	Os rótulos são metadados para seus recursos do Google Cloud. O BlueXP adiciona os rótulos ao sistema Cloud Volumes ONTAP e aos recursos do Google Cloud associados ao sistema. Você pode adicionar até quatro rótulos da interface do usuário ao criar um ambiente de trabalho e, em seguida, adicionar mais após a criação. Observe que a API não limita a quatro rótulos ao criar um ambiente de trabalho. Para obter informações sobre etiquetas, " Documentação do Google Cloud: Etiquetagem de recursos " consulte .
Nome de utilizador e palavra-passe	Estas são as credenciais da conta de administrador de cluster do Cloud Volumes ONTAP. Você pode usar essas credenciais para se conectar ao Cloud Volumes ONTAP por meio do Gerenciador de sistemas do ONTAP ou da CLI do ONTAP. Mantenha o nome de usuário padrão <i>admin</i> ou altere-o para um nome de usuário personalizado.

Campo	Descrição
Editar projeto	<p>Selecione o projeto onde você deseja que o Cloud Volumes ONTAP resida. O projeto padrão é o projeto onde o BlueXP reside.</p> <p>Se você não vir nenhum projeto adicional na lista suspensa, você ainda não associou a conta de serviço do BlueXP a outros projetos. Vá para o console do Google Cloud, abra o serviço IAM e selecione o projeto. Adicione a conta de serviço com a função BlueXP a esse projeto. Você precisará repetir esta etapa para cada projeto.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  Esta é a conta de serviço configurada para o BlueXP , "como descrito nesta página". </div> <p>Clique em Adicionar assinatura para associar as credenciais selecionadas a uma assinatura.</p> <p>Para criar um sistema Cloud Volumes ONTAP de pagamento conforme o uso, você precisa selecionar um projeto do Google Cloud associado a uma assinatura do Cloud Volumes ONTAP no Google Cloud Marketplace.</p>

O vídeo a seguir mostra como associar uma assinatura do mercado de pagamento conforme o uso ao seu projeto do Google Cloud. Em alternativa, siga os passos para subscrever localizados na ["Associar uma assinatura do Marketplace às credenciais do Google Cloud"](#) secção.

[Inscreva-se no BlueXP no Google Cloud Marketplace](#)

- Serviços:** Selecione os serviços que deseja usar neste sistema. Para selecionar o backup e a recuperação do BlueXP ou usar a disposição em camadas do BlueXP , você precisa ter especificado a conta de serviço na etapa 3.



Se quiser utilizar WORM e disposição de dados em camadas, desative o backup e a recuperação do BlueXP e implante um ambiente de trabalho do Cloud Volumes ONTAP com a versão 9,8 ou superior.

- Localização e conectividade:** Selecione um local, escolha uma política de firewall e confirme a conectividade de rede com o armazenamento do Google Cloud para disposição em camadas de dados.

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

Campo	Descrição
Verificação de conectividade	Para categorizar dados inativos em um bucket do Google Cloud Storage, a sub-rede na qual o Cloud Volumes ONTAP reside deve ser configurada para o acesso privado do Google. Para obter instruções, "Documentação do Google Cloud: Configurando o acesso privado do Google" consulte .

Campo	Descrição
Política de firewall gerada	<p>Se você permitir que o BlueXP gere a política de firewall para você, precisará escolher como permitir o tráfego:</p> <ul style="list-style-type: none"> • Se você escolher somente VPC selecionada, o filtro de origem para o tráfego de entrada será o intervalo de sub-rede da VPC selecionada e o intervalo de sub-rede da VPC onde o conector reside. Esta é a opção recomendada. • Se você escolher todos os VPCs, o filtro de origem para o tráfego de entrada é o intervalo IP 0,0.0.0/0.
Use a política de firewall existente	<p>Se você usar uma política de firewall existente, certifique-se de que ela inclui as regras necessárias. Link: https://docs.NetApp.com/US-en/BlueXP -cloud-volumes-ONTAP/reference-networking-Cloud Volumes ONTAP.html.</p>

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

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

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

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

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



Se um candidato de lançamento mais recente, disponibilidade geral ou liberação de 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 9.13.1 e 9.13.1 P4 estiver disponível. A atualização não ocorre de uma versão para outra, por exemplo, de 9,13 a 9,14.

11. **Recursos de armazenamento subjacentes:** Escolha configurações para o agregado inicial: Um tipo de disco e o tamanho de cada disco.

O tipo de disco é para o volume inicial. Você pode escolher um tipo de disco diferente para volumes subsequentes.

O tamanho do disco é para todos os discos no agregado inicial e para quaisquer agregados adicionais criados pelo BlueXP quando você usa a opção de provisionamento simples. Você pode criar agregados que usam um tamanho de disco diferente usando a opção Alocação avançada.

Para obter ajuda sobre como escolher um tipo e tamanho de disco, ["Dimensione seu sistema no Google Cloud"](#) consulte .

12. **Flash Cache, velocidade de gravação e WORM:**

- Ative **Flash Cache**, se desejado.



A partir do Cloud Volumes ONTAP 9.13.1, o *Flash Cache* é compatível com os tipos de instância n2-standard-16, n2-standard-32, n2-standard-48 e n2-standard-64. Não é possível desativar o Flash Cache após a implantação.

b. Escolha **normal** ou **alta** velocidade de gravação, se desejado.

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



Alta velocidade de gravação e uma unidade de transmissão máxima (MTU) superior de 8.896 bytes estão disponíveis através da opção **High** write speed. Além disso, o MTU maior do 8.896 requer a seleção de VPC-1, VPC-2 e VPC-3 para a implantação. Para obter mais informações sobre VPC-1, VPC-2 e VPC-3, ["Regras para VPC-1, VPC-2 e VPC-3"](#) consulte .

c. Ative o storage WORM (uma gravação, muitas leituras), se desejado.

O WORM não pode ser ativado se a disposição de dados em camadas foi ativada para o Cloud Volumes ONTAP versões 9,7 e inferiores. Reverter ou fazer downgrade para o Cloud Volumes ONTAP 9,8 é bloqueado depois de ativar WORM e disposição em camadas.

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

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

13. **Disposição em camadas de dados no Google Cloud Platform:** Escolha se deseja habilitar a disposição em camadas de dados no agregado inicial, escolher uma classe de armazenamento para os dados em camadas e, em seguida, selecionar uma conta de serviço que tenha a função de administrador de armazenamento predefinida (necessária para o Cloud Volumes ONTAP 9,7 ou posterior) ou selecionar uma conta do Google Cloud (necessária para o Cloud Volumes ONTAP 9,6).

Observe o seguinte:

- O BlueXP define a conta de serviço na instância do Cloud Volumes ONTAP. Essa conta de serviço fornece permissões para categorização de dados em um bucket do Google Cloud Storage. Certifique-se de adicionar a conta de serviço do Connector como usuário da conta de serviço de disposição em camadas, caso contrário, você não pode selecioná-la no BlueXP
- Para obter ajuda com a adição de uma conta do Google Cloud, ["Configuração e adição de contas do Google Cloud para categorização de dados no 9,6"](#) consulte .
- Você pode escolher uma política específica de disposição em categorias de volume ao criar ou editar um volume.
- Se você desabilitar a disposição em camadas de dados, poderá ativá-la em agregados subsequentes, mas precisará desativar o sistema e adicionar uma conta de serviço a partir do console do Google Cloud.

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

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

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

Alguns dos campos desta página são auto-explicativos. A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Tamanho	O tamanho máximo que você pode inserir depende, em grande parte, se você ativar o provisionamento de thin, o que permite criar um volume maior do que o armazenamento físico atualmente disponível para ele.
Controle de acesso (somente para NFS)	Uma política de exportação define os clientes na sub-rede que podem acessar o volume. Por padrão, o BlueXP insere um valor que fornece acesso a todas as instâncias na sub-rede.
Permissões e utilizadores/grupos (apenas para CIFS)	Esses campos permitem controlar o nível de acesso a um compartilhamento para usuários e grupos (também chamados de listas de controle de acesso ou ACLs). Você pode especificar usuários ou grupos do Windows locais ou de domínio, ou usuários ou grupos UNIX. Se você especificar um nome de usuário do domínio do Windows, você deve incluir o domínio do usuário usando o nome de domínio do formato.
Política de instantâneos	Uma política de cópia Snapshot especifica a frequência e o número de cópias snapshot do NetApp criadas automaticamente. Uma cópia Snapshot do NetApp é uma imagem pontual do sistema de arquivos que não afeta a performance e exige o mínimo de storage. Você pode escolher a política padrão ou nenhuma. Você pode escolher nenhum para dados transitórios: Por exemplo, tempdb para Microsoft SQL Server.
Opções avançadas (somente para NFS)	Selecione uma versão NFS para o volume: NFSv3 ou NFSv4.
Grupo de iniciadores e IQN (apenas para iSCSI)	Os destinos de armazenamento iSCSI são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Os grupos de iniciadores são tabelas de nomes de nós de host iSCSI e controlam quais iniciadores têm acesso a quais LUNs. Os destinos iSCSI se conectam à rede por meio de adaptadores de rede Ethernet (NICs) padrão, placas de mecanismo de descarga TCP (TOE) com iniciadores de software, adaptadores de rede convergidos (CNAs) ou adaptadores de barramento de host dedicados (HBAs) e são identificados por IQNs (iSCSI Qualified Names). Quando cria um volume iSCSI, o BlueXP cria automaticamente um LUN para si. Simplificamos a criação de apenas um LUN por volume, para que não haja gerenciamento envolvido. Depois de criar o volume, "Use o IQN para se conectar ao LUN a partir de seus hosts" .

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

Volume Details, Protection & Protocol

Details & Protection	Protocol
<p>Volume Name: <input style="width: 200px;" type="text" value="vol"/> Size (GB): <input style="width: 80px;" type="text" value="250"/></p> <p>Snapshot Policy: <input style="width: 300px;" type="text" value="default"/></p> <p><small>Default Policy</small></p>	<p style="text-align: center;"> <input type="radio"/> NFS <input checked="" type="radio"/> CIFS <input type="radio"/> iSCSI </p> <hr/> <p>Share name: <input style="width: 150px;" type="text" value="vol_share"/> Permissions: <input style="width: 150px;" type="text" value="Full Control"/></p> <p>Users / Groups: <input style="width: 300px;" type="text" value="engineering"/></p> <p><small>Valid users and groups separated by a semicolon</small></p>

15. **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 em que o servidor CIFS irá ingressar. Se você estiver configurando o active Directory gerenciado pelo Google, o AD pode ser acessado por padrão com o endereço IP 169.254.169.254.
Active Directory Domain para aderir	O FQDN do domínio do active Directory (AD) ao qual você deseja que o servidor CIFS se associe.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores à unidade organizacional especificada (ou) dentro do domínio do AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio AD.
Unidade organizacional	A unidade organizacional dentro do domínio AD a associar ao servidor CIFS. A predefinição é computadores. Para configurar o Microsoft AD gerenciado pelo Google como o servidor AD para Cloud Volumes ONTAP, digite ou computadores, ou nuvem neste campo. " Documentação do Google Cloud: Unidades organizacionais no Google Managed Microsoft AD "
Domínio DNS	O domínio DNS da máquina virtual de storage (SVM) do Cloud Volumes ONTAP. Na maioria dos casos, o domínio é o mesmo que o domínio AD.
NTP Server	Selecione Use active Directory Domain para configurar um servidor NTP usando o DNS do active Directory. Se você precisa configurar um servidor NTP usando um endereço diferente, então você deve usar a API. Para obter mais informações, consulte o " Documentos de automação BlueXP " para obter mais informações. Observe que você pode configurar um servidor NTP somente ao criar um servidor CIFS. Não é configurável depois de criar o servidor CIFS.

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

necessário.

Para obter mais informações, ["Escolha um perfil de uso de volume"](#) consulte e ["Visão geral de categorização de dados"](#).

17. **Rever & aprovar:** Revise e confirme suas seleções.

- a. Reveja os detalhes sobre a configuração.
- b. Clique em **mais informações** para analisar detalhes sobre o suporte e os recursos do Google Cloud que o BlueXP comprará.
- c. Selecione as caixas de verificação **I understand....**
- d. Clique em **Go**.

Resultado

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

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

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

Depois de terminar

- Se você provisionou um compartilhamento CIFS, dê aos usuários ou grupos permissões para os arquivos e pastas e verifique se esses usuários podem acessar o compartilhamento e criar um arquivo.
- Se você quiser aplicar cotas a volumes, use o Gerenciador de sistema do ONTAP ou a CLI do ONTAP.

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

Lançamento de um par de HA no Google Cloud

Crie um ambiente de trabalho no BlueXP para iniciar o Cloud Volumes ONTAP no Google Cloud.

Passos

1. No menu de navegação à esquerda, selecione **Storage > Canvas**.
2. Na página Canvas, clique em **Adicionar ambiente de trabalho** e siga as instruções.
3. **Escolha um local:** Selecione **Google Cloud** e **Cloud Volumes ONTAP HA**.
4. **Detalhes e credenciais:** Selecione um projeto, especifique um nome de cluster, selecione opcionalmente uma conta de serviço, adicione rótulos opcionalmente e especifique credenciais.

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

Campo	Descrição
Nome do ambiente de trabalho	O BlueXP usa o nome do ambiente de trabalho para nomear tanto o sistema Cloud Volumes ONTAP quanto a instância de VM do Google Cloud. Ele também usa o nome como prefixo para o grupo de segurança predefinido, se você selecionar essa opção.

Campo	Descrição
Nome da conta de serviço	Se você pretende usar os " Disposição em camadas do BlueXP " serviços ou " Backup e recuperação do BlueXP ", você precisa ativar a opção conta de serviço e, em seguida, selecionar a conta de serviço que tem a função Administrador de armazenamento predefinido.
Adicionar etiquetas	Os rótulos são metadados para seus recursos do Google Cloud. O BlueXP adiciona os rótulos ao sistema Cloud Volumes ONTAP e aos recursos do Google Cloud associados ao sistema. Você pode adicionar até quatro rótulos da interface do usuário ao criar um ambiente de trabalho e, em seguida, adicionar mais após a criação. Observe que a API não limita a quatro rótulos ao criar um ambiente de trabalho. Para obter informações sobre etiquetas, " Documentação do Google Cloud: Etiketagem de recursos " consulte .
Nome de utilizador e palavra-passe	Estas são as credenciais da conta de administrador de cluster do Cloud Volumes ONTAP. Você pode usar essas credenciais para se conectar ao Cloud Volumes ONTAP por meio do Gerenciador de sistemas do ONTAP ou da CLI do ONTAP. Mantenha o nome de usuário padrão <i>admin</i> ou altere-o para um nome de usuário personalizado.
Editar projeto	<p>Selecione o projeto onde você deseja que o Cloud Volumes ONTAP resida. O projeto padrão é o projeto onde o BlueXP reside.</p> <p>Se você não vir nenhum projeto adicional na lista suspensa, você ainda não associou a conta de serviço do BlueXP a outros projetos. Vá para o console do Google Cloud, abra o serviço IAM e selecione o projeto. Adicione a conta de serviço com a função BlueXP a esse projeto. Você precisará repetir esta etapa para cada projeto.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">  Esta é a conta de serviço configurada para o BlueXP , "como descrito nesta página". </div> <p>Clique em Adicionar assinatura para associar as credenciais selecionadas a uma assinatura.</p> <p>Para criar um sistema Cloud Volumes ONTAP de pagamento conforme o uso, você precisa selecionar um projeto do Google Cloud associado a uma assinatura do Cloud Volumes ONTAP no Google Cloud Marketplace.</p>

O vídeo a seguir mostra como associar uma assinatura do mercado de pagamento conforme o uso ao seu projeto do Google Cloud. Em alternativa, siga os passos para subscrever localizados na "[Associar uma assinatura do Marketplace às credenciais do Google Cloud](#)" secção.

[Inscreva-se no BlueXP no Google Cloud Marketplace](#)

- Serviços:** Selecione os serviços que deseja usar neste sistema. Para selecionar o backup e a recuperação do BlueXP , ou para usar o BlueXP Tiering, você deve ter especificado a conta de serviço na etapa 3.



Se quiser utilizar WORM e disposição de dados em camadas, desative o backup e a recuperação do BlueXP e implante um ambiente de trabalho do Cloud Volumes ONTAP com a versão 9,8 ou superior.

6. **Modelos de implantação HA:** Escolha várias zonas (recomendado) ou uma única zona para a configuração HA. Em seguida, selecione uma região e zonas.

["Saiba mais sobre os modelos de implantação de HA"](#).

7. **Conetividade:** Selecione quatro VPCs diferentes para a configuração de HA, uma sub-rede em cada VPC e, em seguida, escolha uma política de firewall.

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

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

Campo	Descrição
Política gerada	Se você permitir que o BlueXP gere a política de firewall para você, precisará escolher como permitir o tráfego: <ul style="list-style-type: none">• Se você escolher somente VPC selecionada, o filtro de origem para o tráfego de entrada será o intervalo de sub-rede da VPC selecionada e o intervalo de sub-rede da VPC onde o conector reside. Esta é a opção recomendada.• Se você escolher todos os VPCs, o filtro de origem para o tráfego de entrada é o intervalo IP 0,0.0.0/0.
Utilizar existente	Se utilizar uma política de firewall existente, certifique-se de que inclui as regras necessárias. "Saiba mais sobre as regras de firewall do Cloud Volumes ONTAP" .

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

◦ ["Saiba mais sobre as opções de licenciamento para o Cloud Volumes ONTAP"](#).

◦ ["Saiba como configurar o licenciamento"](#).

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

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

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



Se um candidato de lançamento mais recente, disponibilidade geral ou liberação de 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 9.13.1 e 9.13.1 P4 estiver disponível. A atualização não ocorre de uma versão para outra, por exemplo, de 9,13 a 9,14.

11. **Recursos de armazenamento subjacentes:** Escolha configurações para o agregado inicial: Um tipo de disco e o tamanho de cada disco.

O tipo de disco é para o volume inicial. Você pode escolher um tipo de disco diferente para volumes subsequentes.

O tamanho do disco é para todos os discos no agregado inicial e para quaisquer agregados adicionais criados pelo BlueXP quando você usa a opção de provisionamento simples. Você pode criar agregados que usam um tamanho de disco diferente usando a opção Alocação avançada.

Para obter ajuda sobre como escolher um tipo e tamanho de disco, "[Dimensione seu sistema no Google Cloud](#)" consulte .

12. Flash Cache, velocidade de gravação e WORM:

a. Ative **Flash Cache**, se desejado.



A partir do Cloud Volumes ONTAP 9.13.1, o *Flash Cache* é compatível com os tipos de instância n2-standard-16, n2-standard-32, n2-standard-48 e n2-standard-64. Não é possível desativar o Flash Cache após a implantação.

b. Escolha **normal** ou **alta** velocidade de gravação, se desejado.

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



Alta velocidade de gravação e uma unidade de transmissão máxima (MTU) superior de 8.896 bytes estão disponíveis através da opção de velocidade de gravação **High** com os tipos de instância n2-standard-16, n2-standard-32, n2-standard-48 e n2-standard-64. Além disso, o MTU maior do 8.896 requer a seleção de VPC-1, VPC-2 e VPC-3 para a implantação. A alta velocidade de gravação e uma MTU de 8.896 dependem de recursos e não podem ser desativadas individualmente em uma instância configurada. Para obter mais informações sobre VPC-1, VPC-2 e VPC-3, "[Regras para VPC-1, VPC-2 e VPC-3](#)" consulte .

c. Ative o storage WORM (uma gravação, muitas leituras), se desejado.

O WORM não pode ser ativado se a disposição de dados em camadas foi ativada para o Cloud Volumes ONTAP versões 9,7 e inferiores. Reverter ou fazer downgrade para o Cloud Volumes ONTAP 9,8 é bloqueado depois de ativar WORM e disposição em camadas.

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

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

13. Disposição em camadas de dados no Google Cloud:

Escolha se deseja habilitar a disposição em camadas de dados no agregado inicial, escolher uma classe de armazenamento para os dados em camadas e, em seguida, selecione uma conta de serviço que tenha a função de administrador de armazenamento predefinida.

Observe o seguinte:

- O BlueXP define a conta de serviço na instância do Cloud Volumes ONTAP. Essa conta de serviço fornece permissões para categorização de dados em um bucket do Google Cloud Storage. Certifique-se de adicionar a conta de serviço do Connector como usuário da conta de serviço de disposição em camadas, caso contrário, você não pode selecioná-la no BlueXP .
- Você pode escolher uma política específica de disposição em categorias de volume ao criar ou editar um volume.
- Se você desabilitar a disposição em camadas de dados, poderá ativá-la em agregados subsequentes, mas precisará desativar o sistema e adicionar uma conta de serviço a partir do console do Google Cloud.

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

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

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

Alguns dos campos desta página são auto-explicativos. A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Tamanho	O tamanho máximo que você pode inserir depende, em grande parte, se você ativar o provisionamento de thin, o que permite criar um volume maior do que o armazenamento físico atualmente disponível para ele.
Controle de acesso (somente para NFS)	Uma política de exportação define os clientes na sub-rede que podem acessar o volume. Por padrão, o BlueXP insere um valor que fornece acesso a todas as instâncias na sub-rede.
Permissões e utilizadores/grupos (apenas para CIFS)	Esses campos permitem controlar o nível de acesso a um compartilhamento para usuários e grupos (também chamados de listas de controle de acesso ou ACLs). Você pode especificar usuários ou grupos do Windows locais ou de domínio, ou usuários ou grupos UNIX. Se você especificar um nome de usuário do domínio do Windows, você deve incluir o domínio do usuário usando o nome de domínio do formato.
Política de instantâneos	Uma política de cópia Snapshot especifica a frequência e o número de cópias snapshot do NetApp criadas automaticamente. Uma cópia Snapshot do NetApp é uma imagem pontual do sistema de arquivos que não afeta a performance e exige o mínimo de storage. Você pode escolher a política padrão ou nenhuma. Você pode escolher nenhum para dados transitórios: Por exemplo, tempdb para Microsoft SQL Server.
Opções avançadas (somente para NFS)	Selecione uma versão NFS para o volume: NFSv3 ou NFSv4.
Grupo de iniciadores e IQN (apenas para iSCSI)	Os destinos de armazenamento iSCSI são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Os grupos de iniciadores são tabelas de nomes de nós de host iSCSI e controlam quais iniciadores têm acesso a quais LUNs. Os destinos iSCSI se conectam à rede por meio de adaptadores de rede Ethernet (NICs) padrão, placas de mecanismo de descarga TCP (TOE) com iniciadores de software, adaptadores de rede convergidos (CNAs) ou adaptadores de barramento de host dedicados (HBAs) e são identificados por IQNs (iSCSI Qualified Names). Quando cria um volume iSCSI, o BlueXP cria automaticamente um LUN para si. Simplificamos a criação de apenas um LUN por volume, para que não haja gerenciamento envolvido. Depois de criar o volume, "Use o IQN para se conectar ao LUN a partir de seus hosts" .

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

Volume Details, Protection & Protocol

Details & Protection	Protocol
<p>Volume Name: <input style="width: 80%;" type="text" value="vol"/> Size (GB): <input style="width: 50%;" type="text" value="250"/></p> <p>Snapshot Policy: <input style="width: 80%;" type="text" value="default"/></p> <p><small>Default Policy</small></p>	<p style="text-align: center;"> NFS CIFS iSCSI </p> <p>Share name: <input style="width: 80%;" type="text" value="vol_share"/> Permissions: <input style="width: 50%;" type="text" value="Full Control"/></p> <p>Users / Groups: <input style="width: 80%;" type="text" value="engineering"/></p> <p><small>Valid users and groups separated by a semicolon</small></p>

15. **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 em que o servidor CIFS irá ingressar. Se você estiver configurando o active Directory gerenciado pelo Google, o AD pode ser acessado por padrão com o endereço IP 169.254.169.254.
Active Directory Domain para aderir	O FQDN do domínio do active Directory (AD) ao qual você deseja que o servidor CIFS se associe.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores à unidade organizacional especificada (ou) dentro do domínio do AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio AD.
Unidade organizacional	A unidade organizacional dentro do domínio AD a associar ao servidor CIFS. A predefinição é computadores. Para configurar o Microsoft AD gerenciado pelo Google como o servidor AD para Cloud Volumes ONTAP, digite ou computadores, ou nuvem neste campo. "Documentação do Google Cloud: Unidades organizacionais no Google Managed Microsoft AD"
Domínio DNS	O domínio DNS da máquina virtual de storage (SVM) do Cloud Volumes ONTAP. Na maioria dos casos, o domínio é o mesmo que o domínio AD.
NTP Server	Selecione Use active Directory Domain para configurar um servidor NTP usando o DNS do active Directory. Se você precisa configurar um servidor NTP usando um endereço diferente, então você deve usar a API. Consulte "Documentos de automação BlueXP " para obter mais informações. Observe que você pode configurar um servidor NTP somente ao criar um servidor CIFS. Não é configurável depois de criar o servidor CIFS.

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

necessário.

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

17. **Rever & aprovar:** Revise e confirme suas seleções.

- a. Reveja os detalhes sobre a configuração.
- b. Clique em **mais informações** para analisar detalhes sobre o suporte e os recursos do Google Cloud que o BlueXP comprará.
- c. Selecione as caixas de verificação **I understand....**
- d. Clique em **Go**.

Resultado

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

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

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

Depois de terminar

- Se você provisionou um compartilhamento CIFS, dê aos usuários ou grupos permissões para os arquivos e pastas e verifique se esses usuários podem acessar o compartilhamento e criar um arquivo.
- Se você quiser aplicar cotas a volumes, use o Gerenciador de sistema do ONTAP ou a CLI do ONTAP.

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

Verificação de imagem do Google Cloud Platform

Visão geral da verificação de imagens do Google Cloud

A verificação de imagem do Google Cloud está em conformidade com os requisitos de segurança aprimorados do NetApp. Foram feitas alterações no script gerando as imagens para assinar a imagem ao longo do caminho usando chaves privadas especificamente geradas para esta tarefa. Você pode verificar a integridade da imagem do Google Cloud usando o resumo assinado e o certificado público do Google Cloud, que pode ser baixado ["NSS"](#) para uma versão específica.



A verificação de imagem do Google Cloud é suportada no software Cloud Volumes ONTAP versão 9.13.0 ou superior.

Converta imagem para o formato RAW no Google Cloud

A imagem que está a ser utilizada para implementar novas instâncias, atualizações ou a ser utilizada em imagens existentes será partilhada com os clientes através ["O site de suporte da NetApp \(NSS\)"](#)do . O resumo assinado e os certificados estarão disponíveis para download através do portal NSS. Certifique-se de que está a transferir o resumo e

os certificados para a versão correta correspondente à imagem partilhada pelo suporte da NetApp. Por exemplo, as imagens 9.13.0D terão um resumo assinado 9.13.0D e certificados disponíveis no NSS.

Por que esse passo é necessário?

As imagens do Google Cloud não podem ser baixadas diretamente. Para verificar a imagem em relação ao resumo assinado e aos certificados, você precisa ter um mecanismo para comparar os dois arquivos e baixar a imagem. Para fazer isso, você deve exportar/converter a imagem em um formato Disk.Raw e salvar os resultados em um bucket de storage no Google Cloud. O arquivo Disk.RAW é tarred e gzip no processo.

A conta de usuário/serviço precisará do Privileges para executar o seguinte:

- Acesso ao bucket de armazenamento do Google
- Escreva para o bucket do Google Storage
- Criar trabalhos de compilação na nuvem (usados durante o processo de exportação)
- Acesso à imagem pretendida
- Criar tarefas de exportação de imagem

Para verificar a imagem, ela deve ser convertida em um formato Disk.Raw e, em seguida, baixada.

Use a linha de comando do Google Cloud para exportar a imagem do Google Cloud

A maneira preferida de exportar uma imagem para o Cloud Storage é usar o "[comando de exportação de imagens de computação gcloud](#)". Este comando pega a imagem fornecida e converte-a em um arquivo Disk.Raw que fica em tarred e gzip. O arquivo gerado é salvo no URL de destino e pode ser baixado para verificação.

O usuário/conta deve ter Privileges para acessar e gravar no bucket desejado, exportar a imagem e compilações na nuvem (usadas pelo Google para exportar a imagem) para executar esta operação.

- Exportar imagem do Google Cloud usando gcloud*

Clique para apresentar

```
$ gcloud compute images export \  
  --destination-uri DESTINATION_URI \  
  --image IMAGE_NAME  
  
# For our example:  
$ gcloud compute images export \  
  --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-  
gcp-demo \  
  --image example-user-20230120115139  
  
## DEMO ##  
# Step 1 - Optional: Checking access and listing objects in the  
destination bucket  
$ gsutil ls gs://example-user-export-image-bucket/  
  
# Step 2 - Exporting the desired image to the bucket  
$ gcloud compute images export --image example-user-export-image-demo  
--destination-uri gs://example-user-export-image-bucket/export-  
demo.tar.gz  
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-  
project/locations/us-central1/builds/xxxxxxxxxxxxx].  
Logs are available at [https://console.cloud.google.com/cloud-  
build/builds;region=us-central1/xxxxxxxxxxxxx?project=xxxxxxxxxxxxx].  
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-  
export-image-demo" from project "example-demo-project".  
[image-export]: 2023-01-25T18:13:49Z Validating workflow  
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"  
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-  
export-disk"  
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z  
Validating step "setup-disks"  
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z  
Validating step "run-image-export-export-disk"  
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z  
Validating step "wait-for-inst-image-export-export-disk"  
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z  
Validating step "copy-image-object"  
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z  
Validating step "delete-inst"  
[image-export]: 2023-01-25T18:13:51Z Validation Complete  
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-  
project  
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

```
[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch:
["ExportFailed:"] (this is not an error), StatusMatch: "GCEExport:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
```

```
StatusMatch found: "GCEExport: <serial-output key:'source-size-gb'  
value:'10'>"  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Running export tool."  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size  
will most likely be much smaller."  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Beginning export process..."  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Copying \"/dev/sdb\" to gs://example-  
demo-project-example-bkt-us/example-image-export-20230125-18:13:49-  
r88px/outs/image-export-export-disk.tar.gz."  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Using \"/root/upload\" as the buffer  
prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Creating gzipped image of \"/dev/sdb\"."  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec),  
total written size: 992 MiB (198 MiB/sec)"  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec),  
total written size: 1.5 GiB (17 MiB/sec)"  
[image-export.image-export-export-disk.wait-for-inst-image-export-  
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance  
"inst-image-export-export-disk-image-export-image-export--r88px":  
StatusMatch found: "GCEExport: Finished creating gzipped image of  
\"/dev/sdb\" in 48.956433327s [213 MiB/s] with a compression ratio of  
6."
```

```

[image-export.image-export-export-disk.wait-for-inst-image-export-export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": StatusMatch found: "GCEExport: Finished export in 48.957347731s"
[image-export.image-export-export-disk.wait-for-inst-image-export-export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": StatusMatch found: "GCEExport: <serial-output key:'target-size-gb' value:'2'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": SuccessMatch found "ExportSuccess"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step "copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step "delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk" (IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z Workflow "image-export" finished cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz

# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION

```

```
$ gcloud storage cp gs://example-user-export-image-bucket/export-  
demo.tar.gz CVO_GCP_Signed_Digest.tar.gz  
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to  
file://CVO_GCP_Signed_Digest.tar.gz  
Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s
```

```
Average throughput: 213.3MiB/s
```

```
$ ls -l  
total 1565036  
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44  
CVO_GCP_Signed_Digest.tar.gz
```

- Extraia arquivos compactados*

```
# Extracting files from the digest  
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```



Para obter mais informações sobre como exportar uma imagem pelo Google Cloud, "[Google Cloud doc sobre a exportação de uma imagem](#)" consulte .

Verificação de assinatura de imagem

Verifique as imagens assinadas pelo Google Cloud

Para verificar a imagem assinada do Google Cloud exportada, você deve baixar o arquivo de resumo da imagem do NSS para validar o arquivo disk.RAW e o conteúdo do arquivo de resumo.

Resumo do fluxo de trabalho de verificação de imagem assinada

Veja a seguir uma visão geral do processo de fluxo de trabalho de verificação de imagem assinada pelo Google Cloud.

- "NSS" No , faça o download do arquivo do Google Cloud que contém os seguintes arquivos:
 - Resumo assinado (.sig)
 - Certificado contendo a chave pública (.pem)
 - Cadeia de certificados (.pem)

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

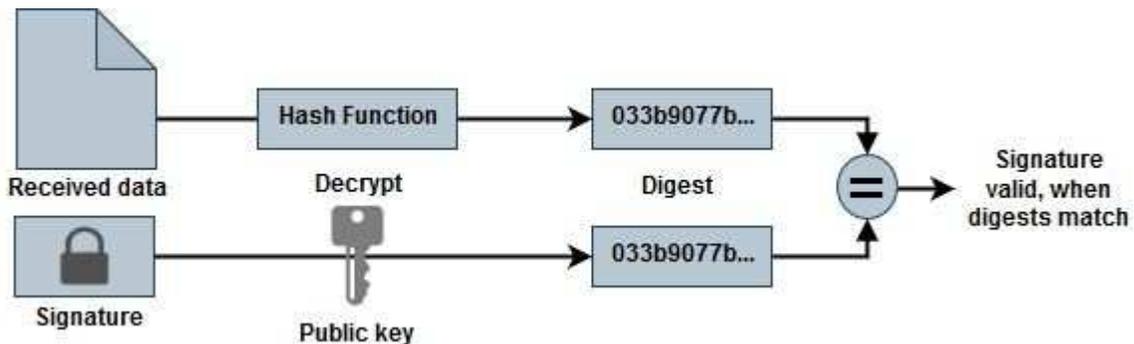
DOWNLOAD GCP-9-15-0P1_PKG.TAR.GZ [7.49 KB]

[View and download checksums](#)

DOWNLOAD AZURE-9-15-0P1_PKG.TAR.GZ [7.64 KB]

[View and download checksums](#)

- Baixe o arquivo convertido disk.RAW
- Valide o certificado usando a cadeia de certificados
- Valide o resumo assinado usando o certificado conter a chave pública
 - Descriptografar o resumo assinado usando a chave pública para extrair o resumo do arquivo de imagem
 - Crie um resumo do arquivo disk.RAW baixado
 - Compare os dois arquivos de resumo para validação



Verificação do conteúdo do arquivo Disk.RAW e do arquivo digest usando OpenSSL

Você pode verificar o arquivo Disk.RAW baixado do Google Cloud contra o conteúdo do arquivo digest disponível através do "NSS" usando OpenSSL.



Os comandos OpenSSL para validar a imagem são compatíveis com máquinas Linux, Mac os e Windows.

Passos

1. Verifique o certificado usando OpenSSL.

Clique para apresentar

```
# Step 1 - Optional, but recommended: Verify the certificate using
OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a
directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in <Certificate-
Chain.pem>)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OSCP request for the certificate
$ openssl ocsf -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsf -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -reqout req.der

# Step 1.4 - Optional: Check the new file "req.der" has been
generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OSCP Manager using openssl to send the
OCSP request
$ openssl ocsf -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocspl -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -url ${ocsp_url} -resp_text
-respout resp.der
```

OCSP Response Data:

OCSP Response Status: successful (0x0)

Response Type: Basic OCSP Response

Version: 1 (0x0)

Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2

Produced At: Jan 19 15:14:00 2023 GMT

Responses:

Certificate ID:

Hash Algorithm: sha1

Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A

Issuer Key Hash: CE894F8251AA15A28462CA312361D261F8FE78

Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5

Cert Status: good

This Update: Jan 19 15:00:00 2023 GMT

Next Update: Jan 26 14:59:59 2023 GMT

Signature Algorithm: sha512WithRSAEncryption

```
0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:
```

```

e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
  This Update: Jan 19 15:00:00 2023 GMT
  Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK

```

2. Coloque o arquivo disk.RAW baixado, a assinatura e os certificados em um diretório.
3. Extraia a chave pública do certificado usando OpenSSL.
4. Descriptografar a assinatura usando a chave pública extraída e verificar o conteúdo do arquivo disk.RAW baixado.

Clique para apresentar

```
# Step 1 - Place the downloaded disk.raw, the signature and the
certificates in a directory
$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) >
(public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-
0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and
verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature
(signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary
../sample_file.txt
Verification Failure
```

Use o Cloud Volumes ONTAP

Gerenciamento de licenças

Gerenciar licenças baseadas em capacidade

Gerencie suas licenças baseadas em capacidade da carteira digital BlueXP para garantir que sua conta NetApp tenha capacidade suficiente para seus sistemas Cloud Volumes ONTAP.

Licenças baseadas em capacidade permitem que você pague por Cloud Volumes ONTAP por TIB de capacidade.

A carteira digital *BlueXP* permite gerenciar licenças para Cloud Volumes ONTAP a partir de um único local. Você pode adicionar novas licenças e atualizar as licenças existentes.



Embora o uso real e a medição dos produtos e serviços gerenciados no BlueXP sejam sempre calculados em GiB e TIB, os termos GB/GiB e TB/TIB são usados de forma intercambiável. Isso é refletido nas listagens do Cloud Marketplace, cotações de preços, descrições de listagem e em outra documentação de suporte

["Saiba mais sobre as licenças do Cloud Volumes ONTAP"](#).

Como as licenças são adicionadas à carteira digital BlueXP

Depois de adquirir uma licença do seu representante de vendas da NetApp, a NetApp enviará um e-mail com o número de série e os detalhes adicionais do licenciamento.

Enquanto isso, o BlueXP 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 BlueXP adiciona automaticamente as licenças à carteira digital.

Se o BlueXP não conseguir adicionar a licença, você precisará adicioná-los manualmente à carteira digital. Por exemplo, se o conector estiver instalado em um local que não tenha acesso à Internet, você precisará adicionar as licenças por conta própria. [Saiba como adicionar licenças compradas à sua conta](#).

Veja a capacidade consumida na sua conta

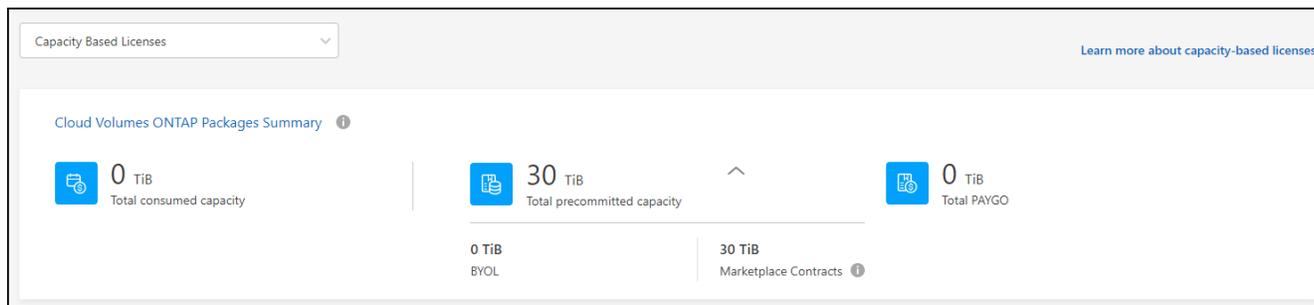
A carteira digital BlueXP mostra a capacidade total consumida na sua conta e a capacidade consumida pelo pacote de licenciamento. Isso pode ajudá-lo a entender como você está sendo cobrado e se você precisa comprar capacidade adicional.

Passos

1. No menu de navegação BlueXP, selecione **Governança > carteira digital**.
2. Na guia **Cloud Volumes ONTAP**, mantenha **licenças baseadas em capacidade** selecionadas.
3. Veja o resumo dos pacotes, que mostra a capacidade consumida, a capacidade total pré-comprometida e a capacidade total de pagamento conforme o uso (PAYGO).
 - *Capacidade total consumida* é a capacidade total provisionada de todos os sistemas Cloud Volumes ONTAP em sua conta do NetApp. O carregamento é baseado no tamanho provisionado de cada volume, independentemente do espaço local, usado, armazenado ou efetivo dentro do volume.

- *Capacidade total pré-comprometida* é a capacidade total licenciada (traga sua própria licença (BYOL) ou Contrato de mercado) que você comprou na NetApp.
- *Total PAYGO* é a capacidade total provisionada usando assinaturas do mercado de nuvem. O carregamento via PAYGO é usado somente se a capacidade consumida for superior à capacidade licenciada ou se não houver licença BYOL disponível na carteira digital BlueXP .

Aqui está um exemplo de um resumo dos pacotes do Cloud Volumes ONTAP na carteira digital do BlueXP :



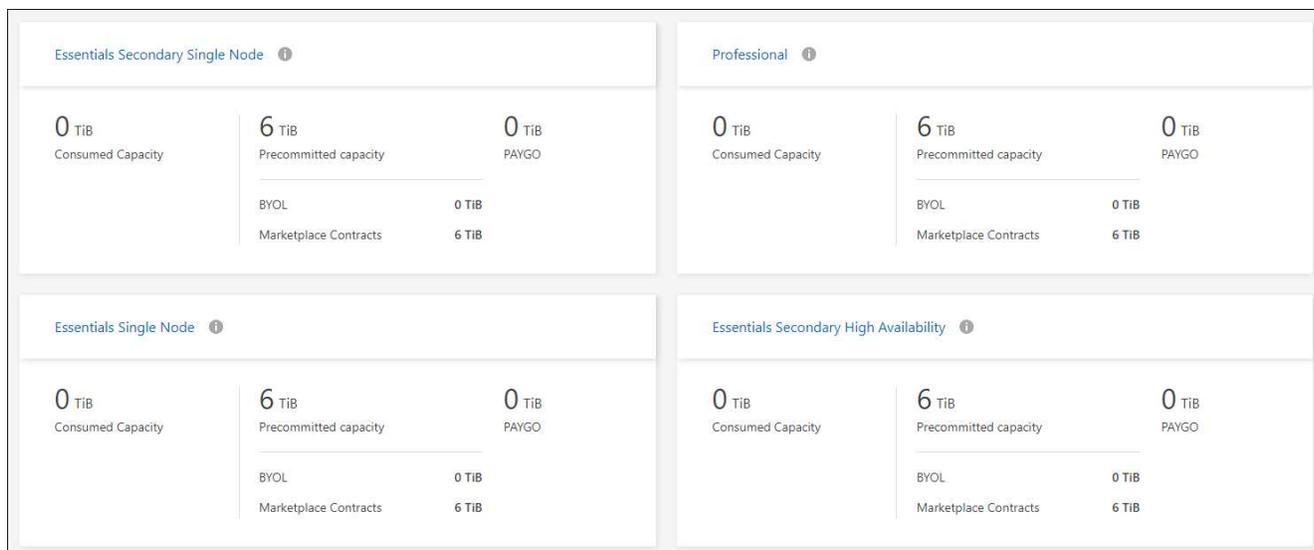
4. No resumo, visualize a capacidade consumida para cada um dos seus pacotes de licenciamento.

- *Capacidade consumida* mostra a capacidade dos volumes para esse pacote. Para obter mais detalhes sobre um pacote específico, passe o Mouse sobre a dica de ferramenta.

Para compreender melhor as capacidades apresentadas para o pacote Essentials, deve estar familiarizado com o funcionamento do carregamento. "[Saiba mais sobre o carregamento do pacote Essentials](#)".

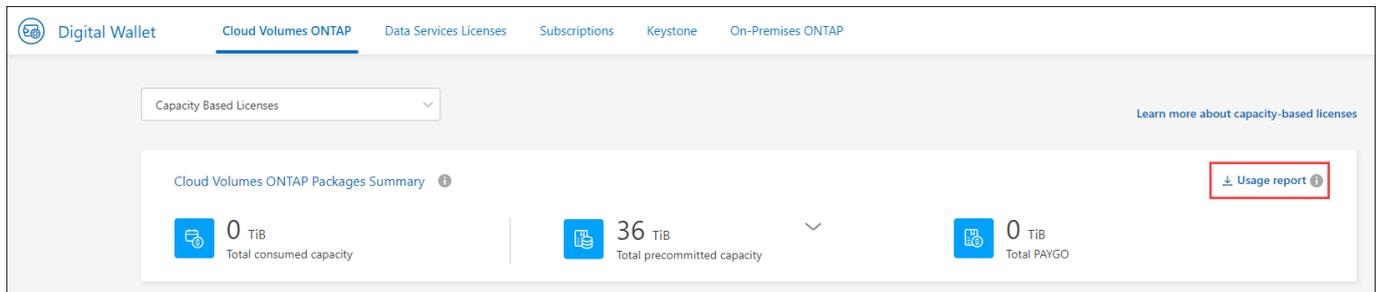
- *Capacidade pré-comprometida* é a capacidade licenciada (BYOL ou Contrato de mercado) que você comprou na NetApp.
 - *BYOL* mostra a capacidade licenciada que você comprou da NetApp para esse tipo de pacote.
 - *Marketplace Contracts* mostra a capacidade licenciada que você comprou com um contrato de mercado para este tipo de pacote.
- *PAYGO* mostra a capacidade consumida pelo modelo de consumo de licença.

Aqui está um exemplo para uma conta que tem vários pacotes de licenciamento:



Transfira relatórios de utilização

Pode transferir quatro relatórios de utilização da carteira digital BlueXP . Esses relatórios de uso fornecem detalhes de capacidade de suas assinaturas e informam como você está sendo cobrado pelos recursos em suas assinaturas do Cloud Volumes ONTAP. Os relatórios transferíveis captam dados num momento e podem ser facilmente compartilhados com outras pessoas.



Os seguintes relatórios estão disponíveis para download. Os valores de capacidade mostrados estão em TiB.

- **Uso de alto nível:** Este relatório mostra exatamente o que está no cartão "Resumo de Pacotes Cloud Volumes ONTAP" na carteira digital. Inclui as seguintes informações:
 - Capacidade total consumida
 - Capacidade total pré-comprometida
 - Capacidade BYOL total
 - Capacidade total dos contratos do mercado
 - Capacidade total PAYGO
- *** Uso do pacote Cloud Volumes ONTAP*:** Este relatório mostra exatamente o que está nos cartões de pacote na carteira digital. Inclui as seguintes informações para cada pacote, exceto o pacote de e/S otimizado:
 - Capacidade total consumida
 - Capacidade total pré-comprometida
 - Capacidade BYOL total
 - Capacidade total dos contratos do mercado
 - Capacidade total PAYGO
- **Uso de VMs de armazenamento:** Este relatório mostra como a capacidade carregada é dividida em sistemas Cloud Volumes ONTAP e máquinas virtuais de armazenamento (SVMs). Esta informação não está disponível em qualquer ecrã da carteira digital. Inclui as seguintes informações:
 - ID e nome do ambiente de trabalho (aparece como UUID)
 - Nuvem
 - ID da conta NetApp
 - Configuração do ambiente de trabalho
 - Nome do SVM
 - Capacidade provisionada
 - Redução da capacidade de carga
 - Prazo de cobrança do mercado

- Pacote ou recurso Cloud Volumes ONTAP
- Carregando o nome da assinatura do SaaS Marketplace
- Cobrança do ID de assinatura do SaaS Marketplace
- Tipo de workload
- **Uso de volumes:** Este relatório mostra como a capacidade de carga é dividida pelos volumes em um ambiente de trabalho. Esta informação não está disponível em qualquer ecrã da carteira digital. Inclui as seguintes informações:
 - ID e nome do ambiente de trabalho (aparece como UUID)
 - Nome SVN
 - ID do volume
 - Tipo de volume
 - Capacidade provisionada de volume



Os volumes do FlexClone não estão incluídos neste relatório porque esses tipos de volumes não incorrem em cobranças.

Passos

1. No menu de navegação BlueXP , selecione **Governança > carteira digital**.
2. Na guia **Cloud Volumes ONTAP**, mantenha **licenças baseadas em capacidade** selecionadas e clique em **Relatório de uso**.

O relatório de uso é baixado.

3. Abra o arquivo baixado para acessar os relatórios.

Adicione licenças compradas à sua conta

Se você não vir suas licenças compradas na carteira digital BlueXP , precisará adicionar as licenças ao BlueXP para que a capacidade esteja disponível para o Cloud Volumes ONTAP.

O que você vai precisar

- Você precisa fornecer ao BlueXP o número de série da licença ou do arquivo de licença.
- Se pretender introduzir o número de série, primeiro tem de "[Adicione sua conta do site de suporte da NetApp ao BlueXP](#)". Esta é a conta do site de suporte da NetApp que está autorizada a acessar o número de série.

Passos

1. No menu de navegação BlueXP , selecione **Governança > carteira digital**.
2. Na guia **Cloud Volumes ONTAP**, mantenha **licenças baseadas em capacidade** selecionadas e clique em **Adicionar licença**.
3. Introduza o número de série da sua licença com base na capacidade ou carregue o ficheiro de licença.

Se você inseriu um número de série, também precisará selecionar a conta do site de suporte da NetApp autorizada a acessar o número de série.

4. Clique em **Adicionar licença**.

Atualizar uma licença baseada em capacidade

Se você adquiriu capacidade adicional ou estendeu o prazo de sua licença, o BlueXP atualizará automaticamente a licença na carteira digital. Não há nada que você precise fazer.

No entanto, se você implantou o BlueXP em um local que não tem acesso à Internet, precisará atualizar manualmente a licença no BlueXP .

O que você vai precisar

O arquivo de licença (ou *Files* se você tiver um par de HA).



Para obter mais informações sobre como obter um arquivo de licença, ["Obtenha um ficheiro de licença do sistema"](#) consulte .

Passos

1. No menu de navegação BlueXP , selecione **Governança > carteira digital**.
2. Na guia **Cloud Volumes ONTAP**, clique no menu de ação ao lado da licença e selecione **Atualizar licença**.
3. Carregue o ficheiro de licença.
4. Clique em **Upload License**.

Alterar os métodos de carregamento

O licenciamento baseado em capacidade está disponível na forma de um *pacote*. Ao criar um ambiente de trabalho Cloud Volumes ONTAP, você pode escolher entre vários pacotes de licenciamento com base nas necessidades da sua empresa. Se suas necessidades mudarem depois de criar o ambiente de trabalho, você pode alterar o pacote a qualquer momento. Por exemplo, você pode mudar do pacote Essentials para o pacote Professional.

["Saiba mais sobre pacotes de licenciamento baseados em capacidade"](#).

Sobre esta tarefa

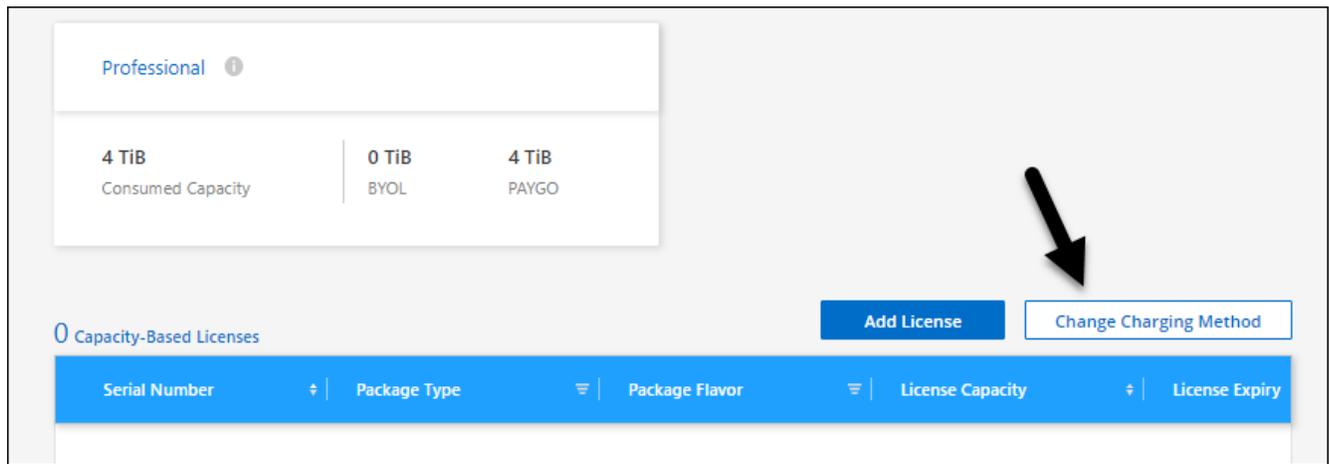
- A alteração do método de cobrança não afeta se você é cobrado por meio de uma licença comprada da NetApp (BYOL) ou da assinatura do mercado do seu provedor de nuvem de pagamento conforme o uso (PAYGO).

O BlueXP sempre tenta cobrar uma licença primeiro. Se uma licença não estiver disponível, ela cobra contra uma assinatura do mercado. Nenhuma "conversão" é necessária para a assinatura BYOL para o mercado ou vice-versa.

- Se você tiver uma oferta privada ou contrato do mercado do seu provedor de nuvem, mudar para um método de cobrança que não esteja incluído no seu contrato resultará em cobrança contra BYOL (se você comprou uma licença da NetApp) ou PAYGO.

Passos

1. No menu de navegação BlueXP , selecione **Governança > carteira digital**.
2. No separador **Cloud Volumes ONTAP**, clique em **Change Charging Method** (alterar método de carregamento).



3. Selecione um ambiente de trabalho, escolha o novo método de carregamento e, em seguida, confirme que a alteração do tipo de pacote afetará as taxas de serviço.

Change Charging Method

Select a working environment

CloudVolumesONTAP2

Current Cloud Volumes ONTAP charging method

Freemium

Select new Cloud Volumes ONTAP charging method

Essential

I understand that changing the package type will affect service charges

Change Charging Method Cancel

4. Clique em **alterar método de carregamento**.

Resultado

O BlueXP altera o método de carregamento do sistema Cloud Volumes ONTAP.

Você também pode notar que a carteira digital da BlueXP atualiza a capacidade consumida para cada tipo de pacote para contabilizar a alteração que você acabou de fazer.

Remova uma licença baseada em capacidade

Se uma licença baseada em capacidade expirou e não estiver mais em uso, você poderá removê-la a qualquer momento.

Para saber o que acontece com os dados do Cloud Volumes ONTAP ao expirar ou remover a licença, "[Este artigo da base de conhecimento \(KB\)](#)" consulte .

Passos

1. No menu de navegação BlueXP , selecione **Governança > carteira digital**.
2. Na guia **Cloud Volumes ONTAP**, clique no menu de ação ao lado da licença e selecione **Remover licença**.
3. Clique em **Remover** para confirmar.

Gerenciar assinaturas do Keystone

Gerencie suas assinaturas do Keystone a partir da carteira digital BlueXP habilitando assinaturas para uso com o Cloud Volumes ONTAP e solicitando alterações na capacidade comprometida dos níveis de serviço da sua assinatura. A solicitação de capacidade adicional para um nível de serviço fornece mais storage para clusters ONTAP no local ou para sistemas Cloud Volumes ONTAP.

O NetApp Keystone é um serviço flexível baseado em subscrição com pagamento conforme o uso que oferece uma experiência de nuvem híbrida para clientes que preferem despesas operacionais a despesas operacionais de capital ou leasing.

["Saiba mais sobre o Keystone"](#)

Autorize sua conta

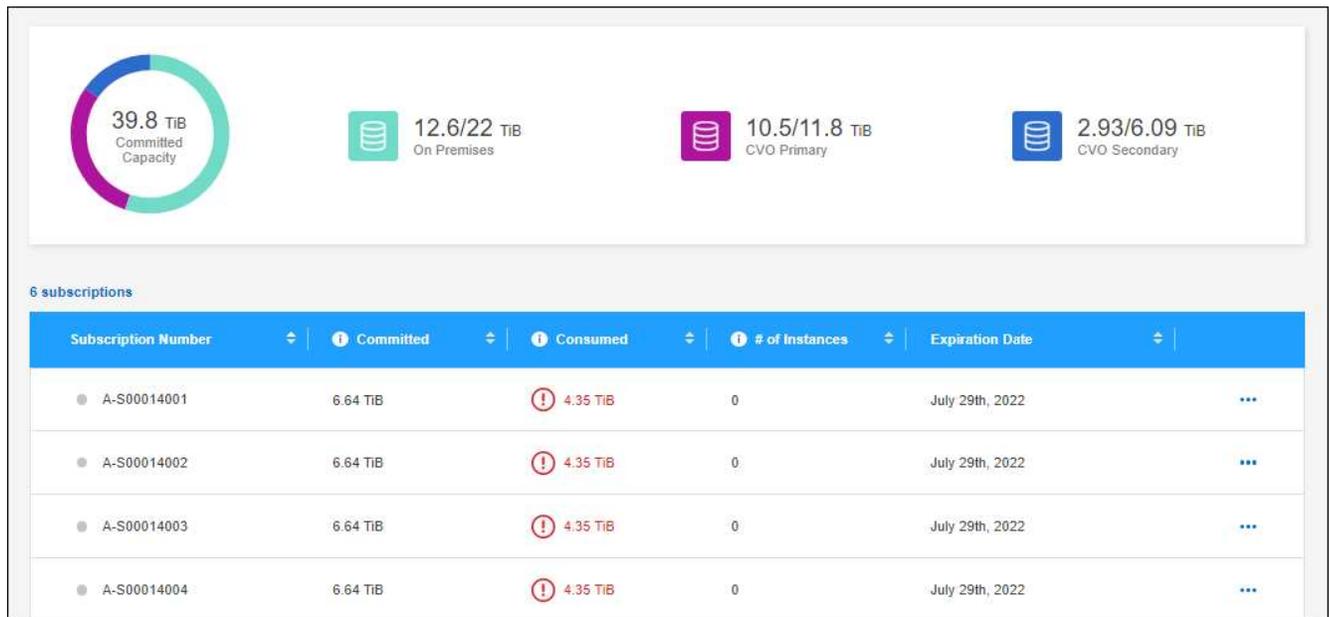
Antes de usar e gerenciar assinaturas do Keystone no BlueXP , entre em Contato com a NetApp para autorizar sua conta de usuário do BlueXP com suas assinaturas do Keystone.

Passos

1. No menu de navegação BlueXP , selecione **Governança > carteira digital**.
2. Selecione **Keystone**.
3. Se você vir a página **bem-vindo ao NetApp Keystone**, envie um e-mail para o endereço listado na página.

Um representante da NetApp processará o seu pedido autorizando a sua conta de utilizador a aceder às subscrições.

4. Volte para a **Keystone Subscription** para ver suas assinaturas.



Vincular uma assinatura

Depois que o NetApp autorizar sua conta, você poderá vincular as assinaturas do Keystone para uso com o Cloud Volumes ONTAP. Esta ação permite aos utilizadores selecionar a subscrição como método de carregamento para novos sistemas Cloud Volumes ONTAP.

Passos

1. No menu de navegação BlueXP , selecione **Governança > carteira digital**.
2. Selecione **Keystone**.
3. Para a assinatura que você deseja vincular, clique **...** e selecione **Link**.

Subscription Number	Committed	Consumed	# of Instances	Expiration Date
A-S00014001	6.64 TiB	4.35 TiB	0	July 29th, 2022
A-S00014002	6.64 TiB	4.35 TiB	0	July 29th, 2022
A-S00014003	6.64 TiB	4.35 TiB	0	July 29th, 2022

Resultado

A assinatura agora está vinculada à sua organização ou conta do BlueXP e está disponível para selecionar ao criar um ambiente de trabalho do Cloud Volumes ONTAP.

Solicite mais ou menos capacidade comprometida

Se você quiser alterar a capacidade comprometida dos níveis de serviço da sua subscrição, pode enviar uma solicitação para a NetApp diretamente da BlueXP . A solicitação de capacidade adicional para um nível de serviço fornece mais storage para clusters no local ou para sistemas Cloud Volumes ONTAP.

Passos

1. No menu de navegação BlueXP , selecione **Governança > carteira digital**.

2. Selecione **Keystone**.
3. Para a assinatura que você deseja ajustar a capacidade, clique **...** e selecione **Exibir detalhes e editar**.
4. Insira a capacidade comprometida solicitada para uma ou mais assinaturas.

Subscription Modification for A-S00014001

Service Level	Current Committed Capacity	Current Consumed Capacity	Requested Committed Capacity
Extreme	0.977 TiB	0.293 TiB	<input type="text" value="Enter amount"/> TiB
Premium	0.977 TiB	0.488 TiB	<input type="text" value="Enter amount"/> TiB
Performance	0 TiB	0 TiB	<input type="text" value="Enter amount"/> TiB
Standard	0.732 TiB	0.439 TiB	<input type="text" value="Enter amount"/> TiB
Value	0.977 TiB	⚠ 0.879 TiB	<input type="text" value="Enter amount"/> TiB
Data Tiering	0 TiB	0 TiB	<input type="text" value="Enter amount"/> TiB
CVO Primary	1.96 TiB	⚠ 1.76 TiB	<input type="text" value="3"/> TiB
CVO Secondary	1.02 TiB	0.488 TiB	<input type="text" value="Enter amount"/> TiB

Additional Information

Is there anything else we should know about your request?
Please be as descriptive as possible.

Enter your notes here

5. Role para baixo, insira quaisquer detalhes adicionais para a solicitação e clique em **Enviar**.

Resultado

Sua solicitação cria um ticket no sistema do NetApp para processamento.

Monitorar o uso

O dashboard do consultor digital do BlueXP permite monitorar o uso da assinatura do Keystone e gerar relatórios.

["Saiba mais sobre como monitorar o uso de assinaturas"](#)

Desvincular uma assinatura

Se você não quiser mais usar uma assinatura do Keystone com BlueXP, pode desvincular a assinatura. Observe que você só pode desvincular uma assinatura que não esteja anexada a uma assinatura Cloud Volumes ONTAP existente.

Passos

1. No menu de navegação BlueXP , selecione **Governança > carteira digital**.
2. Selecione **Keystone**.
3. Para a assinatura que você deseja desvincular, clique **...** e selecione **Unlink**.

Resultado

A assinatura é desvinculada da sua organização ou conta do BlueXP e não está mais disponível para selecionar ao criar um ambiente de trabalho do Cloud Volumes ONTAP.

Gerenciar licenças baseadas em nós

Gerencie licenças baseadas em nós na carteira digital BlueXP para garantir que cada sistema Cloud Volumes ONTAP tenha uma licença válida com a capacidade necessária.

Licenças baseadas em nós são o modelo de licenciamento da geração anterior (e não disponível para novos clientes):

- Traga suas próprias licenças de licença (BYOL) adquiridas na NetApp
- Assinaturas de pagamento conforme o uso (PAYGO) por hora a partir do mercado do seu provedor de nuvem

A carteira digital *BlueXP* permite gerenciar licenças para Cloud Volumes ONTAP a partir de um único local. Você pode adicionar novas licenças e atualizar as licenças existentes.

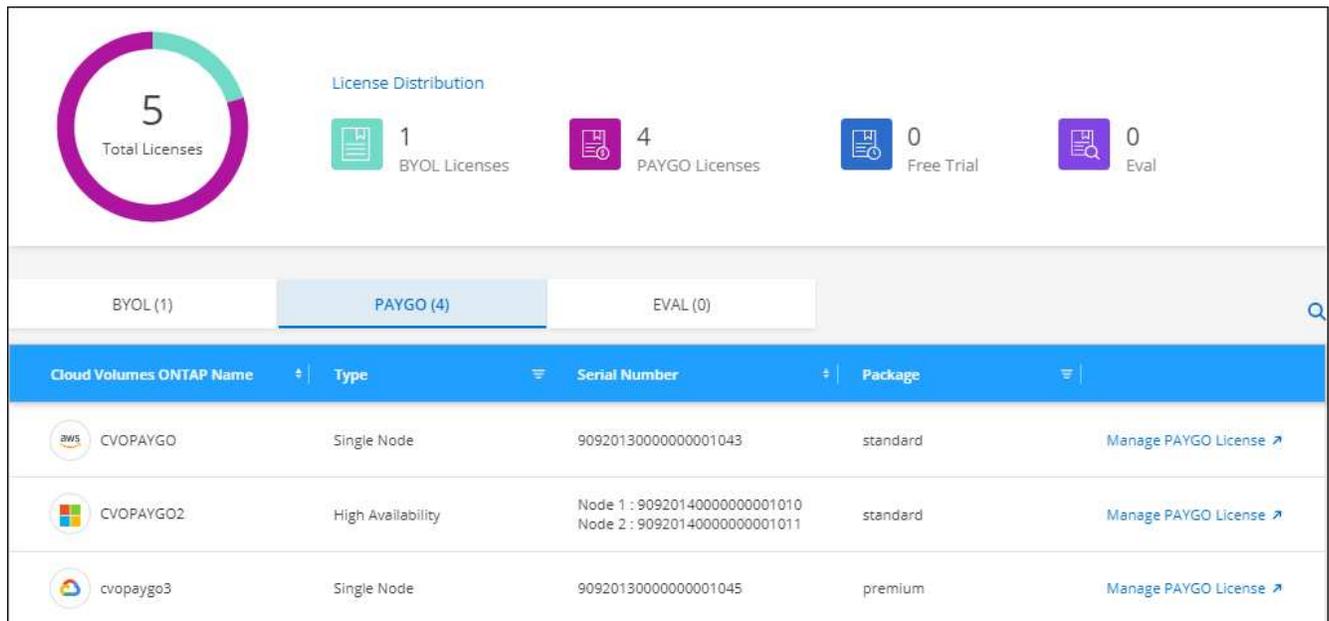
["Saiba mais sobre as licenças do Cloud Volumes ONTAP"](#).

Gerenciar licenças do PAYGO

A página da carteira digital da BlueXP permite-lhe ver detalhes sobre cada um dos seus sistemas PAYGO Cloud Volumes ONTAP, incluindo o número de série e o tipo de licença PAYGO.

Passos

1. No menu de navegação BlueXP , selecione **Governança > carteira digital**.
2. Na guia **Cloud Volumes ONTAP** , selecione **licenças baseadas em nós** na lista suspensa.
3. Clique em **PAYGO**.
4. Veja detalhes na tabela sobre cada uma das suas licenças PAYGO.



5. Se necessário, clique em **Gerenciar licença PAYGO** para alterar a licença PAYGO ou para alterar o tipo de instância.

Gerenciar licenças do BYOL

Gerencie as licenças que você comprou diretamente do NetApp adicionando e removendo licenças de sistema e licenças de capacidade extra.

Adicionar licenças não atribuídas

Adicione uma licença baseada em nós à carteira digital BlueXP para que você possa selecionar a licença ao criar um novo sistema Cloud Volumes ONTAP. A carteira digital identifica essas licenças como *não atribuídas*.

Passos

1. No menu de navegação BlueXP, selecione **Governança > carteira digital**.
2. Na guia **Cloud Volumes ONTAP**, selecione **licenças baseadas em nós** na lista suspensa.
3. Clique em **Unassigned**.
4. Clique em **Adicionar licenças não atribuídas**.
5. Introduza o número de série da licença ou carregue o ficheiro da licença.

Se você ainda não tiver o arquivo de licença, consulte a seção abaixo.

6. Clique em **Adicionar licença**.

Resultado

O BlueXP adiciona a licença à carteira digital. A licença será identificada como não atribuída até que você a associe a um novo sistema Cloud Volumes ONTAP. Depois que isso acontece, a licença passa para a guia **BYOL** na carteira digital.

Troque licenças não atribuídas baseadas em nós

Se você tiver uma licença não atribuída baseada em nó para Cloud Volumes ONTAP que não tenha usado, poderá trocar a licença convertendo-a em uma licença de backup e recuperação do BlueXP, uma licença de

classificação do BlueXP ou uma licença de disposição em camadas do BlueXP .

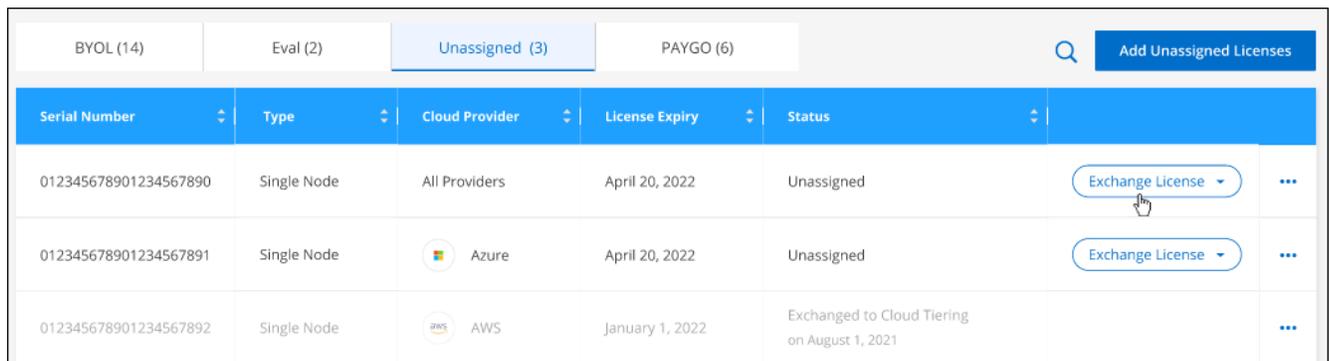
A troca da licença revoga a licença Cloud Volumes ONTAP e cria uma licença equivalente a dólar para o serviço:

- O licenciamento de um par de HA do Cloud Volumes ONTAP é convertido para uma licença de serviço de dados TIB de 51 TB
- O licenciamento para um nó único do Cloud Volumes ONTAP é convertido em uma licença de serviço de dados TIB de 32 TB

A licença convertida tem a mesma data de validade que a licença Cloud Volumes ONTAP.

Passos

1. No menu de navegação BlueXP , selecione **Governança > carteira digital**.
2. Na guia **Cloud Volumes ONTAP** , selecione **licenças baseadas em nós** na lista suspensa.
3. Clique em **Unassigned**.
4. Clique em **Licença de Troca**.



Serial Number	Type	Cloud Provider	License Expiry	Status	
012345678901234567890	Single Node	All Providers	April 20, 2022	Unassigned	Exchange License ▾
012345678901234567891	Single Node	Azure	April 20, 2022	Unassigned	Exchange License ▾
012345678901234567892	Single Node	AWS	January 1, 2022	Exchanged to Cloud Tiering on August 1, 2021	...

5. Selecione o serviço com o qual deseja trocar a licença.
6. Se for solicitado, selecione uma licença adicional para o par de HA.
7. Leia o consentimento legal e clique em **agree**.

Resultado

O BlueXP converte a licença não atribuída para o serviço selecionado. Você pode exibir a nova licença na guia **licenças de serviços de dados**.

Obtenha um ficheiro de licença do sistema

Na maioria dos casos, o BlueXP pode obter automaticamente seu arquivo de licença usando sua conta do site de suporte da NetApp. Mas se não puder, você precisará fazer o upload manual do arquivo de licença. Se não tiver o ficheiro de licença, pode obtê-lo a partir do NetApp.com.

Passos

1. Acesse ao "[Gerador de arquivos de licença NetApp](#)" e inicie sessão utilizando as suas credenciais do site de suporte da NetApp.
2. Introduza a sua palavra-passe, escolha o seu produto, introduza o número de série, confirme que leu e aceitou a política de privacidade e, em seguida, clique em **Enviar**.

Exemplo

License Generator

The following fields are pre-populated based on the NetApp SSO login provided.
To download the corresponding NetApp license file, re-enter your SSO password along with the correct Product Line and Product Serial number.

First Name	<input type="text" value="Ben"/>
Last Name	<input type="text"/>
Company	<input type="text" value="Network Appliance, Inc"/>
Email Address	<input type="text"/>
Username	<input type="text"/>

Product Line*

- ONTAP Select - Standard
- ONTAP Select - Premium
- ONTAP Select - Premium XL
- Cloud Volumes ONTAP for AWS (single node)
- Cloud Volumes ONTAP for AWS (HA)
- Cloud Volumes ONTAP for GCP (single node or HA)
- Cloud Volumes ONTAP for Microsoft Azure (single node)
- Cloud Volumes ONTAP for Microsoft Azure (HA)
- Service Level Manager - SLO Advanced
- StorageGRID Webscale
- StorageGRID WhiteBox
- SnapCenter Standard (capacity-based)

Not only is protecting your data required by law, but it's also the right thing to do. [Global Data Privacy Notice](#)

I have read NetApp's new [Global Data Privacy Notice](#) and agree that NetApp may use my personal data.

- Escolha se você deseja receber o arquivo JSON serialnumber.NLF por e-mail ou download direto.

Atualizar uma licença de sistema

Quando você renova uma assinatura BYOL entrando em Contato com um representante da NetApp, o BlueXP obtém automaticamente a nova licença do NetApp e a instala no sistema Cloud Volumes ONTAP.

Se o BlueXP não conseguir acessar o arquivo de licença pela conexão segura à Internet, você pode obter o arquivo sozinho e, em seguida, carregar o arquivo manualmente para o BlueXP .

Passos

- No menu de navegação BlueXP , selecione **Governança > carteira digital**.
- Na guia **Cloud Volumes ONTAP**, selecione **licenças baseadas em nós** na lista suspensa.
- Na guia **BYOL**, expanda os detalhes de um sistema Cloud Volumes ONTAP.
- Clique no menu de ação ao lado da licença do sistema e selecione **Atualizar Licença**.
- Carregue o ficheiro de licença (ou ficheiros se tiver um par de HA).
- Clique em **Atualizar licença**.

Resultado

O BlueXP atualiza a licença no sistema Cloud Volumes ONTAP.

Gerenciar licenças de capacidade extra

Você pode comprar licenças de capacidade extra para um sistema BYOL da Cloud Volumes ONTAP para alocar mais de 368 TIB de capacidade fornecido com uma licença de sistema BYOL. Por exemplo, você pode comprar uma capacidade de licença extra para alocar até 736 TIB de capacidade para o Cloud Volumes

ONTAP. Ou você pode comprar três licenças de capacidade extra para obter até 1,4 PIB.

O número de licenças que você pode comprar para um único sistema de nó ou par de HA é ilimitado.

Adicione licenças de capacidade

Compre uma licença de capacidade extra entrando em Contato conosco através do ícone de bate-papo no canto inferior direito do BlueXP . Depois de comprar a licença, você pode aplicá-la a um sistema Cloud Volumes ONTAP.

Passos

1. No menu de navegação BlueXP , selecione **Governança > carteira digital**.
2. Na guia **Cloud Volumes ONTAP**, selecione **licenças baseadas em nós** na lista suspensa.
3. Na guia **BYOL**, expanda os detalhes de um sistema Cloud Volumes ONTAP.
4. Clique em **Adicionar licença de capacidade**.
5. Introduza o número de série ou carregue o ficheiro de licença (ou ficheiros se tiver um par de HA).
6. Clique em **Adicionar licença de capacidade**.

Atualizar licenças de capacidade

Se você estendeu o prazo de uma licença de capacidade extra, precisará atualizar a licença no BlueXP .

Passos

1. No menu de navegação BlueXP , selecione **Governança > carteira digital**.
2. Na guia **Cloud Volumes ONTAP**, selecione **licenças baseadas em nós** na lista suspensa.
3. Na guia **BYOL**, expanda os detalhes de um sistema Cloud Volumes ONTAP.
4. Clique no menu de ação ao lado da licença de capacidade e selecione **Atualizar licença**.
5. Carregue o ficheiro de licença (ou ficheiros se tiver um par de HA).
6. Clique em **Atualizar licença**.

Remover licenças de capacidade

Se uma licença de capacidade extra expirou e não está mais em uso, você pode removê-la a qualquer momento.

Passos

1. No menu de navegação BlueXP , selecione **Governança > carteira digital**.
2. Na guia **Cloud Volumes ONTAP**, selecione **licenças baseadas em nós** na lista suspensa.
3. Na guia **BYOL**, expanda os detalhes de um sistema Cloud Volumes ONTAP.
4. Clique no menu de ação ao lado da licença de capacidade e selecione **Remover licença**.
5. Clique em **Remover**.

Converta uma licença Eval em um BYOL

Uma licença de avaliação é boa por 30 dias. Você pode aplicar uma nova licença BYOL além da licença de avaliação para uma atualização no local.

Quando você converte uma licença do Eval para um BYOL, o BlueXP reinicia o sistema Cloud Volumes

ONTAP.

- Para um sistema de nó único, a reinicialização resulta em interrupção de e/S durante o processo de reinicialização.
- Para um par de HA, a reinicialização inicia o takeover e a giveback para continuar fornecendo e/S aos clientes.

Passos

1. No menu de navegação BlueXP , selecione **Governança > carteira digital**.
2. Na guia **Cloud Volumes ONTAP** , selecione **licenças baseadas em nós** na lista suspensa.
3. Clique em **Eval**.
4. Na tabela, clique em **Converter para Licença BYOL** para um sistema Cloud Volumes ONTAP.
5. Introduza o número de série ou carregue o ficheiro de licença.
6. Clique em **Converter Licença**.

Resultado

O BlueXP inicia o processo de conversão. O Cloud Volumes ONTAP reinicia automaticamente como parte desse processo. Quando for feita uma cópia de segurança, as informações de licenciamento refletirão a nova licença.

Mudança entre PAYGO e BYOL

A conversão de um sistema do licenciamento por nó PAYGO para o licenciamento por nó BYOL (e vice-versa) não é suportada. Se você quiser alternar entre uma assinatura paga conforme o uso e uma assinatura BYOL, precisará implantar um novo sistema e replicar dados do sistema existente para o novo sistema.

Passos

1. Crie um novo ambiente de trabalho do Cloud Volumes ONTAP.
2. Configure uma replicação de dados única entre os sistemas para cada volume que você precisa replicar.

["Saiba como replicar dados entre sistemas"](#)

3. Encerre o sistema Cloud Volumes ONTAP que você não precisa mais excluindo o ambiente de trabalho original.

["Saiba como excluir um ambiente de trabalho do Cloud Volumes ONTAP"](#).

Tópico relacionado

<https://docs.netapp.com/pt-br/bluexp-cloud-volumes-ontap/concept-licensing.html#end-of-availability-of-node-based-licenses> > "Término da disponibilidade de licenças baseadas em nós"
[xref:./task-convert-node-capacity.html](#) > "Converta licenças baseadas em nós em capacidade"

Administração de volume e LUN

Criar volumes FlexVol

Se você precisar de mais storage depois de iniciar o sistema Cloud Volumes ONTAP inicial, poderá criar novos volumes FlexVol para NFS, CIFS ou iSCSI a partir do BlueXP .

O BlueXP fornece várias maneiras de criar um novo volume:

- Especifique detalhes para um novo volume e deixe que o BlueXP processe os agregados de dados subjacentes para você. [Saiba mais](#)
- Crie um volume em um agregado de dados de sua escolha. [Saiba mais](#)
- Crie um volume no segundo nó em uma configuração de HA. [Saiba mais](#)

Antes de começar

Algumas notas sobre o provisionamento de volume:

- Quando cria um volume iSCSI, o BlueXP cria automaticamente um LUN para si. Simplificamos a criação de apenas um LUN por volume, para que não haja gerenciamento envolvido. Depois de criar o volume, ["Use o IQN para se conectar ao LUN a partir de seus hosts"](#).
- Você pode criar LUNs adicionais no Gerenciador de sistemas do ONTAP ou na CLI do ONTAP.
- Se você quiser usar o CIFS na AWS, você deve ter configurado o DNS e o Active Directory. Para obter detalhes, ["Requisitos de rede para o Cloud Volumes ONTAP para AWS"](#) consulte .
- Se a configuração do Cloud Volumes ONTAP oferecer suporte ao recurso volumes elásticos do Amazon EBS, talvez você queira ["saiba mais sobre o que acontece quando você cria um volume"](#).

Crie um volume

A maneira mais comum de criar um volume é especificar o tipo de volume que você precisa e, em seguida, o BlueXP lida com a alocação de disco para você. Mas você também tem a opção de escolher o agregado específico no qual deseja criar o volume.

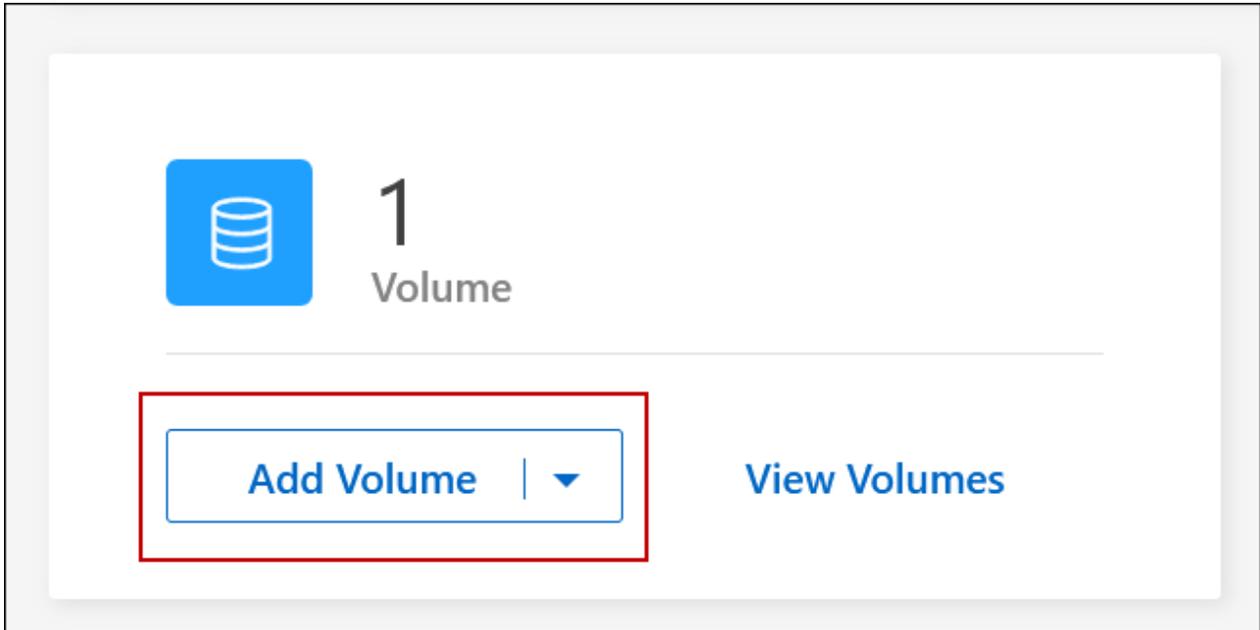
Passos

1. No menu de navegação à esquerda, selecione **Storage > Canvas**.
2. Na página tela, clique duas vezes no nome do sistema Cloud Volumes ONTAP no qual você deseja provisionar um FlexVol volume.
3. Crie um novo volume deixando o BlueXP lidar com a alocação de disco para você ou escolher um agregado específico para o volume.

A escolha de um agregado específico é recomendada somente se você tiver um bom entendimento dos agregados de dados em seu sistema Cloud Volumes ONTAP.

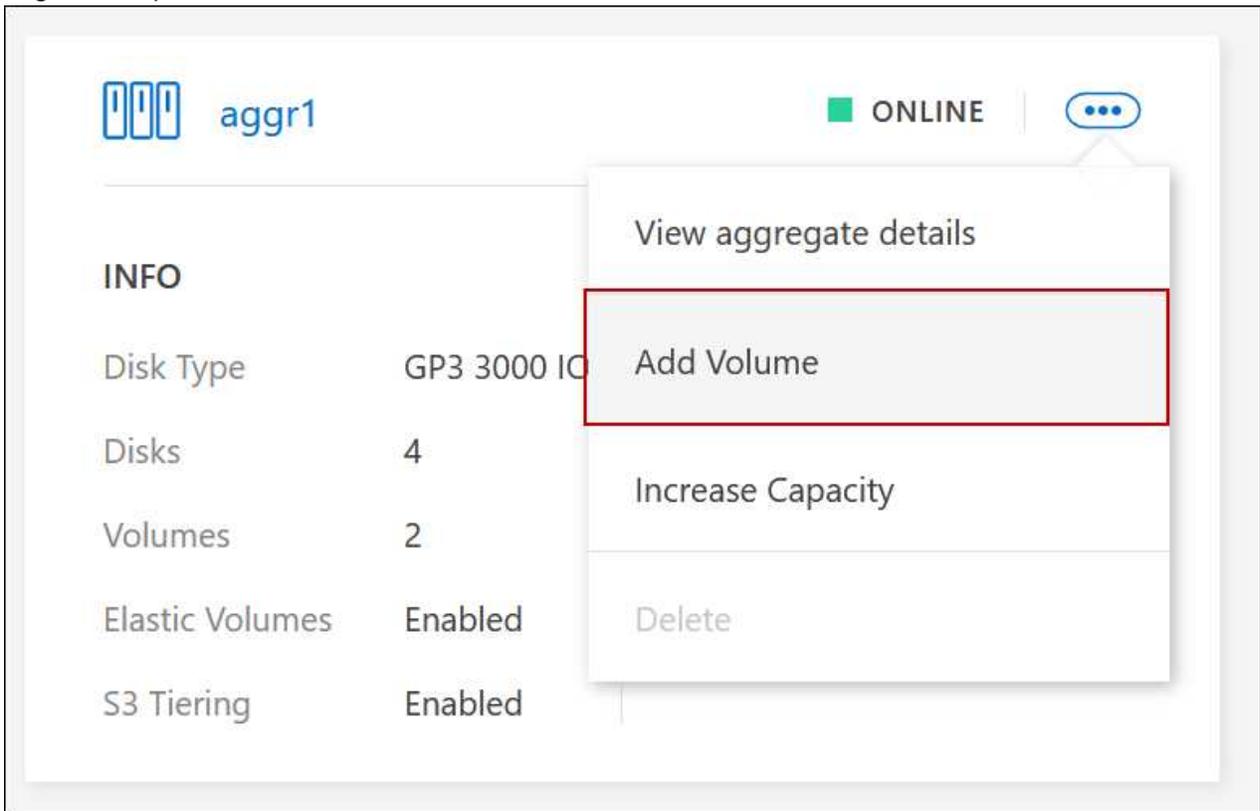
Qualquer agregado

Na guia Visão geral, navegue até o mosaico volumes e clique em **Adicionar volume**.



Agregado específico

Na guia agregados, navegue até o bloco agregado desejado. Clique no ícone do menu e, em seguida, clique em **Adicionar volume**.



4. Siga as etapas do assistente para criar o volume.

a. **Detalhes, proteção e Tags:** Insira detalhes básicos sobre o volume e selecione uma política de

snapshot.

Alguns dos campos desta página são auto-explicativos. A lista a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Nome do volume	O nome identificável que pode introduzir para o novo volume.
Tamanho do volume	O tamanho máximo que você pode inserir depende, em grande parte, se você ativar o provisionamento de thin, o que permite criar um volume maior do que o armazenamento físico atualmente disponível para ele.
VM de storage (SVM)	Uma VM de armazenamento é uma máquina virtual em execução no ONTAP que fornece serviços de armazenamento e dados aos seus clientes. Você pode saber isso como um SVM ou um vserver. O Cloud Volumes ONTAP é configurado com uma VM de storage por padrão, mas algumas configurações oferecem suporte a VMs de storage adicionais. Você pode especificar a VM de armazenamento para o novo volume.
Política de instantâneos	Uma política de cópia Snapshot especifica a frequência e o número de cópias snapshot do NetApp criadas automaticamente. Uma cópia Snapshot do NetApp é uma imagem pontual do sistema de arquivos que não afeta a performance e exige o mínimo de storage. Você pode escolher a política padrão ou nenhuma. Você pode escolher nenhum para dados transitórios: Por exemplo, tempdb para Microsoft SQL Server.

- b. **Protocolo:** Escolha um protocolo para o volume (NFS, CIFS ou iSCSI) e, em seguida, forneça as informações necessárias.

Se você selecionar CIFS e um servidor não estiver configurado, o BlueXP solicitará que você configure a conectividade CIFS depois de clicar em **Avançar**.

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

As seções a seguir descrevem os campos para os quais você pode precisar de orientação. As descrições são organizadas por protocolo.

NFS

Controle de acesso

Escolha uma política de exportação personalizada para disponibilizar o volume aos clientes.

Política de exportação

Define os clientes na sub-rede que podem acessar o volume. Por padrão, o BlueXP insere um valor que fornece acesso a todas as instâncias na sub-rede.

CIFS

Permissões e usuários/grupos

Permite controlar o nível de acesso a um compartilhamento SMB para usuários e grupos (também chamado de listas de controle de acesso ou ACLs). Você pode especificar usuários ou grupos do Windows locais ou de domínio, ou usuários ou grupos UNIX. Se você especificar um nome de usuário do domínio do Windows, você deve incluir o domínio do usuário usando o nome de domínio/nome de usuário do formato.

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 em que o servidor CIFS irá ingressar.

Se você estiver configurando o Active Directory gerenciado pelo Google, o AD pode ser acessado por padrão com o endereço IP 169.254.169.254.

Active Directory Domain para aderir

O FQDN do domínio do Active Directory (AD) ao qual você deseja que o servidor CIFS se associe.

Credenciais autorizadas para ingressar no domínio

O nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores à unidade organizacional especificada (ou) dentro do domínio do AD.

Nome NetBIOS do servidor CIFS

Um nome de servidor CIFS exclusivo no domínio AD.

Unidade organizacional

A unidade organizacional dentro do domínio AD a associar ao servidor CIFS. A predefinição é computadores.

- Para configurar o AWS Managed Microsoft AD como o servidor AD para Cloud Volumes ONTAP, digite neste campo.
- Para configurar os Serviços de domínio do Azure AD como o servidor AD para o Cloud Volumes ONTAP, digite **computadores AADDC** ou **usuários AADDC** neste campo. ["Documentação do Azure: Crie uma unidade organizacional \(ou\) em um domínio gerenciado dos Serviços de domínio do Azure AD"](#)
- Para configurar o Microsoft AD gerenciado pelo Google como o servidor AD para Cloud Volumes ONTAP, digite **ou computadores, ou nuvem** neste campo. ["Documentação do Google Cloud: Unidades organizacionais no Google Managed Microsoft AD"](#)

Domínio DNS

O domínio DNS da máquina virtual de storage (SVM) do Cloud Volumes ONTAP. Na maioria dos casos, o domínio é o mesmo que o domínio AD.

NTP Server

Selecione **Use ativo Directory Domain** para configurar um servidor NTP usando o DNS do ativo Directory. Se você precisa configurar um servidor NTP usando um endereço diferente, então você deve usar a API. Para obter informações, consulte "[Documentos de automação BlueXP](#)" a .

Observe que você pode configurar um servidor NTP somente ao criar um servidor CIFS. Não é configurável depois de criar o servidor CIFS.

ISCSI

LUN

Os destinos de armazenamento iSCSI são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Quando cria um volume iSCSI, o BlueXP cria automaticamente um LUN para si. Simplificamos a criação de apenas um LUN por volume, para que não haja gerenciamento envolvido. Depois de criar o volume, "[Use o IQN para se conectar ao LUN a partir de seus hosts](#)".

Grupo de iniciadores

Grupos de iniciadores (grupos de iniciadores) especificam quais hosts podem acessar LUNs especificados no sistema de armazenamento

Iniciador do host (IQN)

Os destinos iSCSI se conectam à rede por meio de adaptadores de rede Ethernet (NICs) padrão, placas de mecanismo de descarga TCP (TOE) com iniciadores de software, adaptadores de rede convergidos (CNAs) ou adaptadores de barramento de host dedicados (HBAs) e são identificados por nomes qualificados iSCSI (IQNs).

- a. * Tipo de disco*: Escolha um tipo de disco subjacente para o volume com base nas suas necessidades de desempenho e requisitos de custo.
 - "[Dimensionamento do seu sistema na AWS](#)"
 - "[Dimensionamento do seu sistema no Azure](#)"
 - "[Dimensionamento do seu sistema no Google Cloud](#)"

5. **Perfil de uso e Política de disposição em categorias**: Escolha se deseja ativar ou desativar os recursos de eficiência de armazenamento no volume e, em seguida, selecione um "[política de disposição em camadas de volume](#)".

O ONTAP inclui vários recursos de eficiência de storage que podem reduzir a quantidade total de storage de que você precisa. Os recursos de eficiência de storage da NetApp oferecem os seguintes benefícios:

Thin Provisioning

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

Deduplicação

Melhora a eficiência localizando blocos idênticos de dados e substituindo-os por referências a um único bloco compartilhado. Essa técnica reduz os requisitos de capacidade de storage eliminando blocos

redundantes de dados que residem no mesmo volume.

Compactação

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

6. **Review:** Reveja os detalhes sobre o volume e clique em **Add**.

Resultado

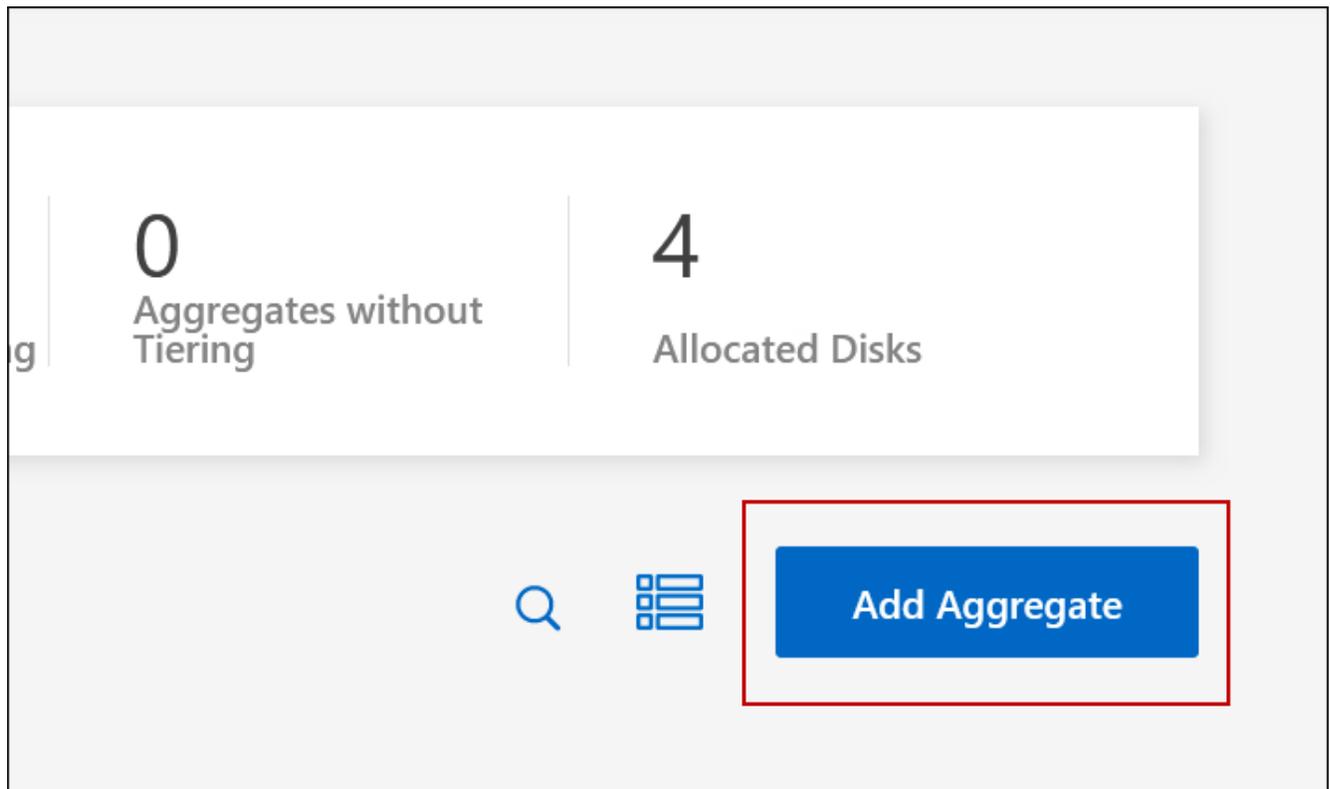
O BlueXP cria o volume no sistema Cloud Volumes ONTAP.

Crie um volume no segundo nó em uma configuração de HA

Por padrão, o BlueXP cria volumes no primeiro nó em uma configuração de HA. Se você precisar de uma configuração ativo-ativo, na qual ambos os nós fornecem dados aos clientes, será necessário criar agregados e volumes no segundo nó.

Passos

1. No menu de navegação à esquerda, selecione **Storage > Canvas**.
2. Na página tela, clique duas vezes no nome do ambiente de trabalho do Cloud Volumes ONTAP no qual você deseja gerenciar agregados.
3. Na guia agregados, clique em **Adicionar agregado**.
4. Na tela *Adicionar agregado*, crie o agregado.



5. No nó inicial, escolha o segundo nó no par de HA.
6. Depois que o BlueXP criar o agregado, selecione-o e clique em **criar volume**.
7. Insira os detalhes do novo volume e clique em **criar**.

Resultado

O BlueXP cria o volume no segundo nó no par de HA.



Para pares de HA implantados em várias zonas de disponibilidade da AWS, é necessário montar o volume nos clientes usando o endereço IP flutuante do nó no qual o volume reside.

Depois de criar um volume

Se você provisionou um compartilhamento CIFS, dê aos usuários ou grupos permissões para os arquivos e pastas e verifique se esses usuários podem acessar o compartilhamento e criar um arquivo.

Para aplicar cotas a volumes, use o Gerenciador de sistemas do ONTAP ou a CLI do ONTAP. As cotas permitem restringir ou rastrear o espaço em disco e o número de arquivos usados por um usuário, grupo ou qtree.

Gerenciar volumes existentes

O BlueXP permite gerenciar volumes e servidores CIFS. Ele também solicita que você mova volumes para evitar problemas de capacidade.

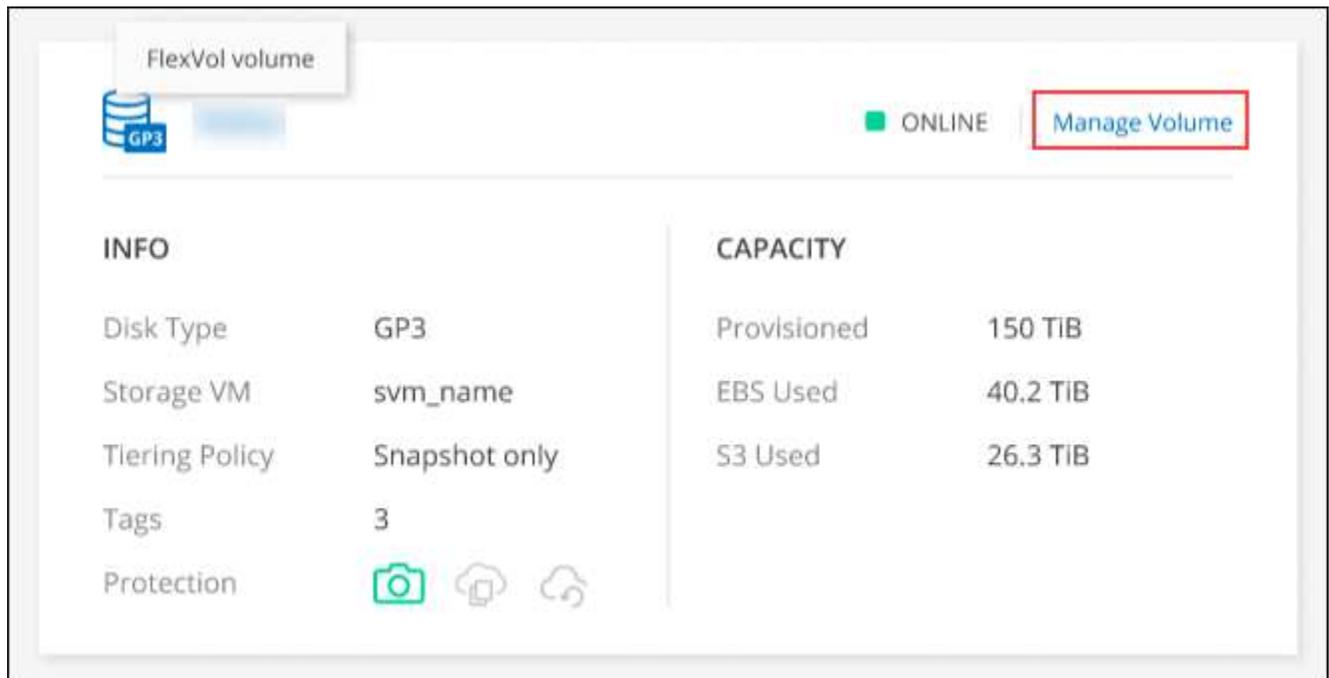
Você pode gerenciar volumes no modo de exibição padrão do BlueXP ou no modo de exibição avançado. A visualização padrão fornece um conjunto limitado de opções para modificar seus volumes. A visualização avançada fornece nível avançado de gerenciamento, como clonagem, redimensionamento, alteração de configurações para anti-ransomware, análises, proteção e controle de atividades, além da movimentação de volumes entre camadas. Para obter informações, "[Administrar o Cloud Volumes ONTAP usando a visualização avançada](#)" consulte .

Gerenciar volumes

Com a visualização padrão do BlueXP , você pode gerenciar volumes de acordo com suas necessidades de storage. Você pode exibir, editar, clonar, restaurar e excluir volumes.

Passos

1. No menu de navegação à esquerda, selecione **Storage > Canvas**.
2. Na página Canvas, clique duas vezes no ambiente de trabalho do Cloud Volumes ONTAP no qual você deseja gerenciar volumes.
3. No ambiente de trabalho, clique na guia **volumes**.



4. Na guia volumes, navegue até o título do volume desejado e clique em **Gerenciar volume** para acessar o painel direito Gerenciar volumes.

Tarefa	Ação
Exibir informações sobre um volume	Em ações de volume no painel Gerenciar volumes, clique em Exibir detalhes do volume .
Obtenha o comando NFS mount	<ol style="list-style-type: none"> Em ações de volume no painel Gerenciar volumes, clique em Mount Command. Clique em Copiar.
Clonar um volume	<ol style="list-style-type: none"> Em ações de volume no painel Gerenciar volumes, clique em Clone o volume. Modifique o nome do clone conforme necessário e clique em Clone. <p>Esse processo cria um volume FlexClone. Um volume FlexClone é uma cópia gravável e pontual que usa espaço reduzido porque usa um pouco de espaço para metadados e, em seguida, consome espaço adicional apenas à medida que os dados são alterados ou adicionados.</p> <p>Para saber mais sobre o FlexClone volumes, consulte o "Guia de gerenciamento de storage lógico do ONTAP 9".</p>

Tarefa	Ação
<p>Editar um volume (somente volumes de leitura e gravação)</p>	<p>a. Em ações de volume no painel Gerenciar volumes, clique em Editar configurações de volume</p> <p>b. Modifique a política Snapshot do volume, a versão do protocolo NFS, a lista de controle de acesso NFS (política de exportação) ou as permissões de compartilhamento e clique em aplicar.</p> <p> Se você precisar de políticas de snapshot personalizadas, poderá criá-las usando o Gerenciador de sistemas do ONTAP.</p>
<p>Eliminar um volume</p>	<p>a. Em ações de volume no painel Gerenciar volumes, clique em Excluir o volume.</p> <p>b. Na janela Excluir volume , digite o nome do volume que deseja excluir.</p> <p>c. Clique em Delete novamente para confirmar.</p>
<p>Criar uma cópia Snapshot sob demanda</p>	<p>a. Em ações de proteção no painel Gerenciar volumes, clique em criar uma cópia Snapshot.</p> <p>b. Altere o nome, se necessário, e clique em criar.</p>
<p>Restaure os dados de uma cópia Snapshot para um novo volume</p>	<p>a. Em ações de proteção no painel Gerenciar volumes, clique em Restaurar a partir da cópia Snapshot.</p> <p>b. Selecione uma cópia Snapshot, insira um nome para o novo volume e clique em Restore.</p>
<p>Altere o tipo de disco subjacente</p>	<p>a. Em ações avançadas no painel Gerenciar volumes, clique em alterar tipo de disco.</p> <p>b. Selecione o tipo de disco e clique em alterar.</p> <p> O BlueXP move o volume para um agregado existente que usa o tipo de disco selecionado ou cria um novo agregado para o volume.</p>
<p>Alterar a política de disposição em camadas</p>	<p>a. Em ações avançadas no painel Gerenciar volumes, clique em alterar Diretiva de disposição em categorias.</p> <p>b. Selecione uma política diferente e clique em alterar.</p> <p> O BlueXP move o volume para um agregado existente que usa o tipo de disco selecionado com disposição em camadas ou cria um novo agregado para o volume.</p>

Tarefa	Ação
Eliminar um volume	<ol style="list-style-type: none">Selecione um volume e, em seguida, clique em Delete.Digite o nome do volume na caixa de diálogo.Clique em Delete novamente para confirmar.

Redimensione um volume

Por padrão, um volume aumenta automaticamente para um tamanho máximo quando está fora do espaço. O valor padrão é 1.000, o que significa que o volume pode crescer para 11 vezes seu tamanho. Este valor é configurável nas definições do conector.

Se você precisar redimensionar seu volume, você pode fazê-lo a partir da visualização avançada no BlueXP .

Passos

- Abra a visualização avançada para redimensionar um volume através do Gerenciador de sistema do ONTAP. "[Como começar](#)" Consulte a .
- No menu de navegação à esquerda, selecione **armazenamento > volumes**.
- Na lista de volumes, identifique o que você deve redimensionar.
- Clique no ícone de opções  .
- Selecione **Redimensionar**.
- Na tela **Redimensionar volume**, edite a porcentagem de capacidade e reserva Instantânea conforme necessário. Você pode comparar o espaço disponível existente com a capacidade modificada.
- Clique em **Salvar**.

Resize volume ✕

CAPACITY

25
⇅

GiB
▼

SNAPSHOT RESERVE %

1
⇅

Existing	New
DATA SPACE	DATA SPACE
20 GiB	24.75 GiB
SNAPSHOT RESERVE	SNAPSHOT RESERVE
0 Bytes	256 MiB

Cancel
Save

Certifique-se de levar em consideração os limites de capacidade do seu sistema à medida que você redimensiona volumes. Acesse ao ["Notas de versão do Cloud Volumes ONTAP"](#) para obter mais informações.

Modifique o servidor CIFS

Se você alterar seus servidores DNS ou domínio do active Directory, será necessário modificar o servidor CIFS no Cloud Volumes ONTAP para que ele possa continuar a servir armazenamento aos clientes.

Passos

1. Na guia Visão geral do ambiente de trabalho, clique na guia recurso sob o painel direito.
2. No campo Configuração CIFS, clique no ícone **lápiz** para exibir a janela Configuração CIFS.
3. Especifique as configurações para o servidor CIFS:

Tarefa	Ação
Selecione Storage VM (SVM)	A seleção da máquina virtual de storage (SVM) do Cloud volume ONTAP exibe suas informações de CIFS configuradas.
Ative Directory Domain para aderir	O FQDN do domínio do active Directory (AD) ao qual você deseja que o servidor CIFS se associe.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores à unidade organizacional especificada (ou) dentro do domínio do AD.

Tarefa	Ação
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 ativo Directory e os controladores de domínio para o domínio em que o servidor CIFS será conectado. Ifdef::gcp[] se você estiver configurando o Google Managed ativo Directory, o AD pode ser acessado por padrão com o endereço IP 169.254.169.254. Endif::gcp[]
Domínio DNS	O domínio DNS da máquina virtual de storage (SVM) do Cloud Volumes ONTAP. Na maioria dos casos, o domínio é o mesmo que o domínio AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio AD.
Unidade organizacional	A unidade organizacional dentro do domínio AD a associar ao servidor CIFS. A predefinição é computadores. <ul style="list-style-type: none"> • Para configurar o AWS Managed Microsoft AD como o servidor AD para Cloud Volumes ONTAP, digite neste campo. • Para configurar os Serviços de domínio do Azure AD como o servidor AD para o Cloud Volumes ONTAP, digite computadores AADDC ou usuários AADDC neste campo. "Documentação do Azure: Crie uma unidade organizacional (ou) em um domínio gerenciado dos Serviços de domínio do Azure AD" • Para configurar o Microsoft AD gerenciado pelo Google como o servidor AD para Cloud Volumes ONTAP, digite ou computadores, ou nuvem neste campo. "Documentação do Google Cloud: Unidades organizacionais no Google Managed Microsoft AD"

4. Clique em **Definir**.

Resultado

O Cloud Volumes ONTAP atualiza o servidor CIFS com as alterações.

Mover um volume

Mova volumes para utilização de capacidade, performance aprimorada e atender a contratos de nível de serviço.

Você pode mover um volume no Gerenciador de sistemas do ONTAP selecionando um volume e o agregado de destino, iniciando a operação de movimentação de volume e, opcionalmente, monitorando a tarefa de movimentação de volume. Ao usar o System Manager, uma operação de movimentação de volume é concluída automaticamente.

Passos

1. Use o Gerenciador de sistema do ONTAP ou a CLI do ONTAP para mover os volumes para o agregado.

Na maioria das situações, você pode usar o System Manager para mover volumes.

Para obter instruções, consulte "[Guia expresso de movimentação de volume do ONTAP 9](#)"a .

Mover um volume quando o BlueXP exibir uma mensagem Ação necessária

O BlueXP pode exibir uma mensagem Ação necessária que diz que mover um volume é necessário para evitar problemas de capacidade, mas que você precisa corrigir o problema sozinho. Se isso acontecer, você precisa identificar como corrigir o problema e mover um ou mais volumes.



O BlueXP exibe essas mensagens de Ação necessária quando um agregado atingiu 90% da capacidade usada. Se a disposição de dados estiver ativada, as mensagens serão exibidas quando um agregado atingir 80% da capacidade usada. Por padrão, 10% de espaço livre é reservado para categorização de dados. ["Saiba mais sobre a taxa de espaço livre para categorização de dados"](#).

Passos

1. [Identificar como corrigir problemas de capacidade.](#)
2. Com base em suas análises, mova volumes para evitar problemas de capacidade:
 - [Mova volumes para outro sistema para evitar problemas de capacidade.](#)
 - [Mova volumes para outro agregado para evitar problemas de capacidade.](#)

Identificar como corrigir problemas de capacidade

Se o BlueXP não puder fornecer recomendações para mover um volume para evitar problemas de capacidade, identifique os volumes que você precisa mover e se deve movê-los para outro agregado no mesmo sistema ou para outro sistema.

Passos

1. Exiba as informações avançadas na mensagem Ação necessária para identificar o agregado que atingiu seu limite de capacidade.

Por exemplo, as informações avançadas devem dizer algo semelhante ao seguinte: O agregado aggr1 atingiu seu limite de capacidade.

2. Identifique um ou mais volumes para sair do agregado:
 - a. No ambiente de trabalho, clique na guia **agregados**.
 - b. Navegue até o bloco agregado desejado e clique em ... (**Ícone de elipses**) > **Ver detalhes de agregados**.
 - c. Na guia Visão geral da tela Detalhes agregados, revise o tamanho de cada volume e escolha um ou mais volumes para sair do agregado.

Você deve escolher volumes grandes o suficiente para liberar espaço no agregado para evitar problemas de capacidade adicionais no futuro.

Aggregate Details	
aggr1	
Overview	Capacity Allocation
State	online
Home Node	iblog1-01
Encryption Type	cloudEncrypted
Volumes	2 ^
	www_iblog1_root (1 GiB)
	iblog1 (500 GiB)

- Se o sistema não tiver atingido o limite de disco, você deve mover os volumes para um agregado existente ou um novo agregado no mesmo sistema.

Para obter informações, [Mova volumes para outro agregado para evitar problemas de capacidade](#) consulte .

- Se o sistema tiver atingido o limite de disco, proceda de uma das seguintes formas:
 - Exclua todos os volumes não utilizados.
 - Reorganize volumes para liberar espaço em um agregado.

Para obter informações, [Mova volumes para outro agregado para evitar problemas de capacidade](#) consulte .

- Mova dois ou mais volumes para outro sistema que tenha espaço.

Para obter informações, [Mova volumes para outro agregado para evitar problemas de capacidade](#) consulte .

Mova volumes para outro sistema para evitar problemas de capacidade

Você pode mover um ou mais volumes para outro sistema Cloud Volumes ONTAP para evitar problemas de capacidade. Talvez seja necessário fazer isso se o sistema atingir seu limite de disco.

Sobre esta tarefa

Pode seguir os passos desta tarefa para corrigir a seguinte mensagem Ação necessária:

Mover um volume é necessário para evitar problemas de capacidade; no entanto, o BlueXP não pode executar esta ação para você porque o sistema atingiu o limite de disco.

Passos

1. Identifique um sistema Cloud Volumes ONTAP que tenha capacidade disponível ou implante um novo sistema.
2. Arraste e solte o ambiente de trabalho de origem no ambiente de trabalho de destino para executar uma replicação de dados única do volume.

Para obter informações, "[Replicação de dados entre sistemas](#)" consulte .

3. Vá para a página Status da replicação e, em seguida, quebre a relação do SnapMirror para converter o volume replicado de um volume de proteção de dados para um volume de leitura/gravação.

Para obter informações, "[Gerenciamento de cronogramas e relacionamentos de replicação de dados](#)" consulte .

4. Configure o volume para acesso aos dados.

Para obter informações sobre como configurar um volume de destino para acesso a dados, consulte o "[Guia expresso de recuperação de desastres em volume do ONTAP 9](#)".

5. Eliminar o volume original.

Para obter informações, "[Gerenciar volumes](#)" consulte .

Mova volumes para outro agregado para evitar problemas de capacidade

Você pode mover um ou mais volumes para outro agregado para evitar problemas de capacidade.

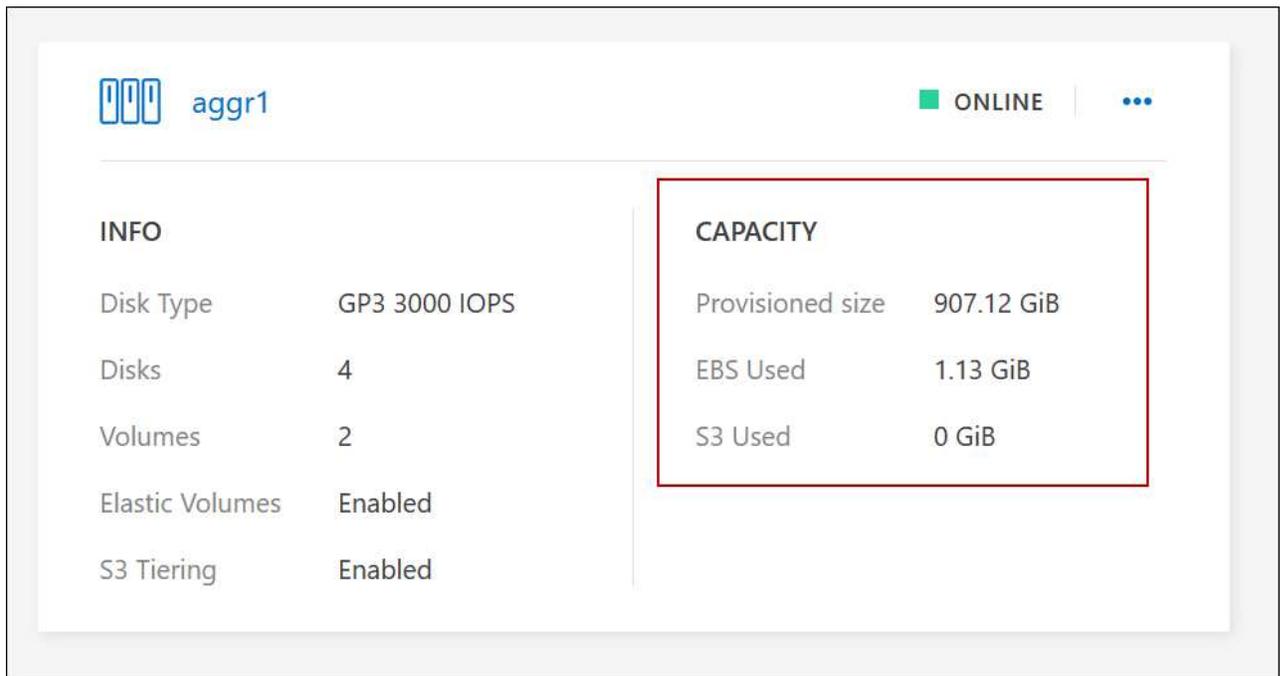
Sobre esta tarefa

Pode seguir os passos desta tarefa para corrigir a seguinte mensagem Ação necessária:

É necessário mover dois ou mais volumes para evitar problemas de capacidade. No entanto, o BlueXP não pode executar essa ação para você.

Passos

1. Verifique se um agregado existente tem capacidade disponível para os volumes que você precisa mover:
 - a. No ambiente de trabalho, clique na guia **agregados**.
 - b. Navegue até o bloco agregado desejado e clique em ... (**Ícone de elipses**) > **Ver detalhes de agregados**.
 - c. No bloco agregado, exiba a capacidade disponível (tamanho provisionado menos capacidade agregada usada).



2. Se necessário, adicione discos a um agregado existente:
 - a. Selecione o agregado e, em seguida, clique no ... (**Ícone de elipses**) > **Adicionar discos**.
 - b. Selecione o número de discos a serem adicionados e clique em **Add**.
3. Se nenhum agregado tiver capacidade disponível, crie um novo agregado.

Para obter informações, "[Criando agregados](#)" consulte .

4. Use o Gerenciador de sistema do ONTAP ou a CLI do ONTAP para mover os volumes para o agregado.
5. Na maioria das situações, você pode usar o System Manager para mover volumes.

Para obter instruções, consulte "[Guia expresso de movimentação de volume do ONTAP 9](#)"a .

Razões pelas quais um movimento de volume pode ter um desempenho lento

Mover um volume pode demorar mais tempo do que o esperado se qualquer uma das seguintes condições for verdadeira para o Cloud Volumes ONTAP:

- O volume é um clone.
- O volume é um pai de um clone.
- O agregado de origem ou destino tem um disco HDD (st1) otimizado para taxa de transferência única.
- Um dos agregados usa um esquema de nomenclatura mais antigo para objetos. Ambos os agregados têm que usar o mesmo formato de nome.

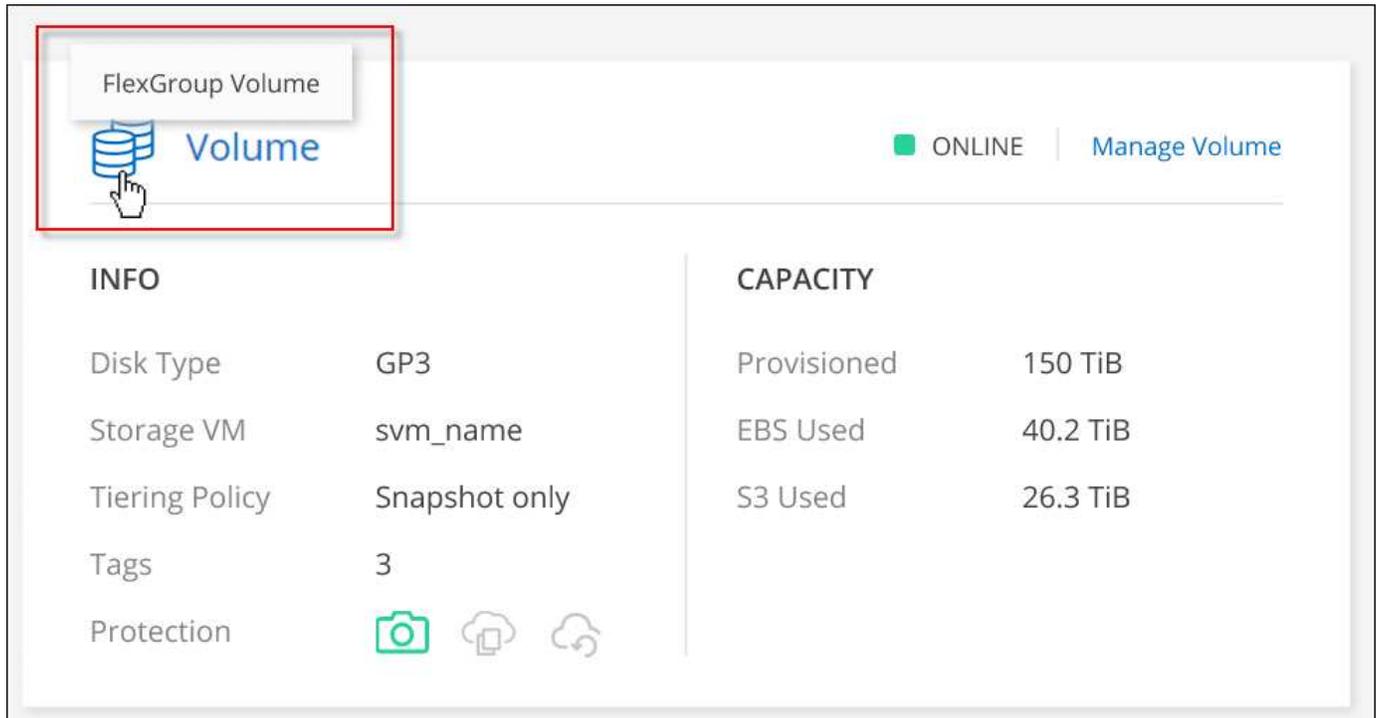
Um esquema de nomenclatura mais antigo é usado se a categorização de dados tiver sido habilitada em um agregado na versão 9,4 ou anterior.

- As configurações de criptografia não correspondem aos agregados de origem e destino, ou uma rechavear está em andamento.
- A opção *-Tiering-policy* foi especificada na movimentação de volume para alterar a política de disposição em camadas.

- A opção `-generate-destination-key` foi especificada na movimentação de volume.

Visualizar volumes do FlexGroup

Você pode visualizar os volumes do FlexGroup criados pelo Gerenciador de sistemas do ONTAP ou pela CLI do ONTAP diretamente na guia volumes no BlueXP. Idêntico às informações fornecidas para os volumes FlexVol, o BlueXP fornece informações detalhadas para volumes FlexGroup criados através de um bloco volumes dedicado. No bloco volumes, você pode identificar cada grupo de volumes do FlexGroup por meio do texto do cursor do ícone. Além disso, você pode identificar e classificar volumes FlexGroup na visualização de lista volumes na coluna estilo de volume.



INFO		CAPACITY	
Disk Type	GP3	Provisioned	150 TiB
Storage VM	svm_name	EBS Used	40.2 TiB
Tiering Policy	Snapshot only	S3 Used	26.3 TiB
Tags	3		
Protection	  		



Atualmente, você só pode exibir volumes FlexGroup existentes no BlueXP. A capacidade de criar volumes do FlexGroup no BlueXP não está disponível, mas planejada para um lançamento futuro.

Disposição em camadas dos dados inativos em storage de objetos de baixo custo

Você pode reduzir os custos de storage do Cloud Volumes ONTAP combinando uma camada de desempenho de SSD ou HDD para dados ativos com uma camada de capacidade de storage de objetos para dados inativos. A disposição de dados em categorias é baseada na tecnologia FabricPool. Para obter uma visão geral de alto nível, ["Visão geral de categorização de dados"](#) consulte .

Para configurar a disposição de dados em categorias, você precisa fazer o seguinte:

1

Escolha uma configuração suportada

A maioria das configurações é compatível. Se você tem um sistema Cloud Volumes ONTAP executando a versão mais recente, então você deve ser bom para ir. ["Saiba mais"](#).

2

Garanta a conectividade entre o Cloud Volumes ONTAP e o storage de objetos

- Para a AWS, você precisará de um VPC Endpoint para S3. [Saiba mais](#).
- Para o Azure, você não precisará fazer nada, desde que o BlueXP tenha as permissões necessárias. [Saiba mais](#).
- Para o Google Cloud, você precisa configurar a sub-rede para o Acesso Privado do Google e configurar uma conta de serviço. [Saiba mais](#).

3

Garanta que você tenha um agregado com a disposição em categorias ativada

A disposição de dados em categorias deve ser habilitada em um agregado para permitir a disposição de dados em categorias em um volume. Você deve estar ciente dos requisitos para novos volumes e volumes existentes. [Saiba mais](#).

4

Escolha uma política de disposição em categorias ao criar, modificar ou replicar um volume

O BlueXP solicita que você escolha uma política de disposição em categorias ao criar, modificar ou replicar um volume.

- ["Disposição em camadas dos dados em volumes de leitura-gravação"](#)
- ["Disposição de dados em camadas em volumes de proteção de dados"](#)

O que não é necessário para a disposição em camadas de dados? 8217

- Não é necessário instalar uma licença de recurso para habilitar a disposição em camadas de dados.
- Não é necessário criar um armazenamento de objetos para o nível de capacidade. BlueXP faz isso por você.
- Não é necessário habilitar a disposição em camadas de dados no nível do sistema.

O BlueXP cria um armazenamento de objetos para dados inativos quando o sistema é criado, [desde que não haja problemas de conectividade ou permissões](#). Depois disso, basta habilitar a disposição de dados em categorias em volumes (e, em alguns casos, [em agregados](#)).



Configurações compatíveis com categorização de dados

Você pode habilitar a disposição de dados em categorias usando configurações e recursos específicos.

Suporte na AWS

- A disposição de dados em categorias é compatível com a AWS a partir do Cloud Volumes ONTAP 9,2.
- A categoria de performance pode ser SSDs de uso geral (GP3 ou GP2) ou SSDs IOPS provisionados (IO1).



A disposição em camadas dos dados no storage de objetos não é recomendada quando se usa HDDs otimizados para taxa de transferência (st1).

Suporte no Azure

- A disposição de dados em categorias é compatível com o Azure da seguinte forma:
 - Versão 9,4 em com sistemas de nó único
 - Versão 9,6 em com pares de HA
- A camada de desempenho pode ser discos gerenciados SSD Premium, discos gerenciados SSD padrão ou discos gerenciados HDD padrão.

Suporte no Google Cloud

- A disposição de dados em categorias é compatível com o Google Cloud a partir do Cloud Volumes ONTAP 9,6.
- A camada de performance pode ser discos persistentes de SSD, discos persistentes balanceados ou discos persistentes padrão.

Interoperabilidade de recursos

- A disposição de dados em categorias é compatível com tecnologias de criptografia.
- O thin Provisioning deve estar ativado em volumes.

Requisitos

Dependendo do seu fornecedor de nuvem, certas conexões e permissões devem ser configuradas para que o Cloud Volumes ONTAP possa categorizar dados inativos no storage de objetos.

Requisitos para categorizar dados inativos no AWS S3

Certifique-se de que o Cloud Volumes ONTAP tem uma ligação ao S3. A melhor maneira de fornecer essa conexão é criando um endpoint VPC para o serviço S3. Para obter instruções, consulte ["Documentação da AWS: Criando um endpoint do Gateway"](#) a .

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

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

Requisitos para categorizar dados inativos no storage Azure Blob

Você não precisa configurar uma conexão entre o nível de performance e o nível de capacidade, desde que o BlueXP tenha as permissões necessárias. O BlueXP habilita um endpoint de serviço VNet para você se a função personalizada para o conector tiver estas permissões:

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

As permissões são incluídas na função personalizada por padrão. ["Veja a permissão do Azure para o conector"](#)

Requisitos para categorizar dados inativos em um bucket do Google Cloud Storage

- A sub-rede em que o Cloud Volumes ONTAP reside deve ser configurada para o acesso privado do Google. Para obter instruções, "[Documentação do Google Cloud: Configurando o acesso privado do Google](#)" consulte .
- Uma conta de serviço deve ser anexada ao Cloud Volumes ONTAP.

"[Saiba como configurar esta conta de serviço](#)".

Você será solicitado a selecionar essa conta de serviço ao criar um ambiente de trabalho do Cloud Volumes ONTAP.

Se você não selecionar uma conta de serviço durante a implantação, será necessário encerrar o Cloud Volumes ONTAP, acessar o console do Google Cloud e anexar a conta de serviço às instâncias do Cloud Volumes ONTAP. Em seguida, é possível habilitar a disposição de dados em categorias conforme descrito na próxima seção.

- Para criptografar o bucket com chaves de criptografia gerenciadas pelo cliente, habilite o bucket de storage do Google Cloud para usar a chave.

"[Saiba como usar chaves de criptografia gerenciadas pelo cliente com o Cloud Volumes ONTAP](#)".

Habilitando a disposição de dados em categorias após a implementação dos requisitos

O BlueXP cria um armazenamento de objetos para dados inativos quando o sistema é criado, desde que não haja problemas de conectividade ou permissões. Se você não implementar os requisitos listados acima até depois de criar o sistema, precisará habilitar manualmente a disposição em camadas por meio da API ou do Gerenciador de sistema do ONTAP, que cria o armazenamento de objetos.



A capacidade de habilitar a disposição em camadas por meio da interface de usuário do BlueXP estará disponível em uma versão futura do Cloud Volumes ONTAP.

Garantir que a disposição em camadas seja ativada em agregados

A disposição de dados em categorias deve ser habilitada em um agregado para permitir a disposição de dados em categorias em um volume. Você deve estar ciente dos requisitos para novos volumes e volumes existentes.

• Novos volumes

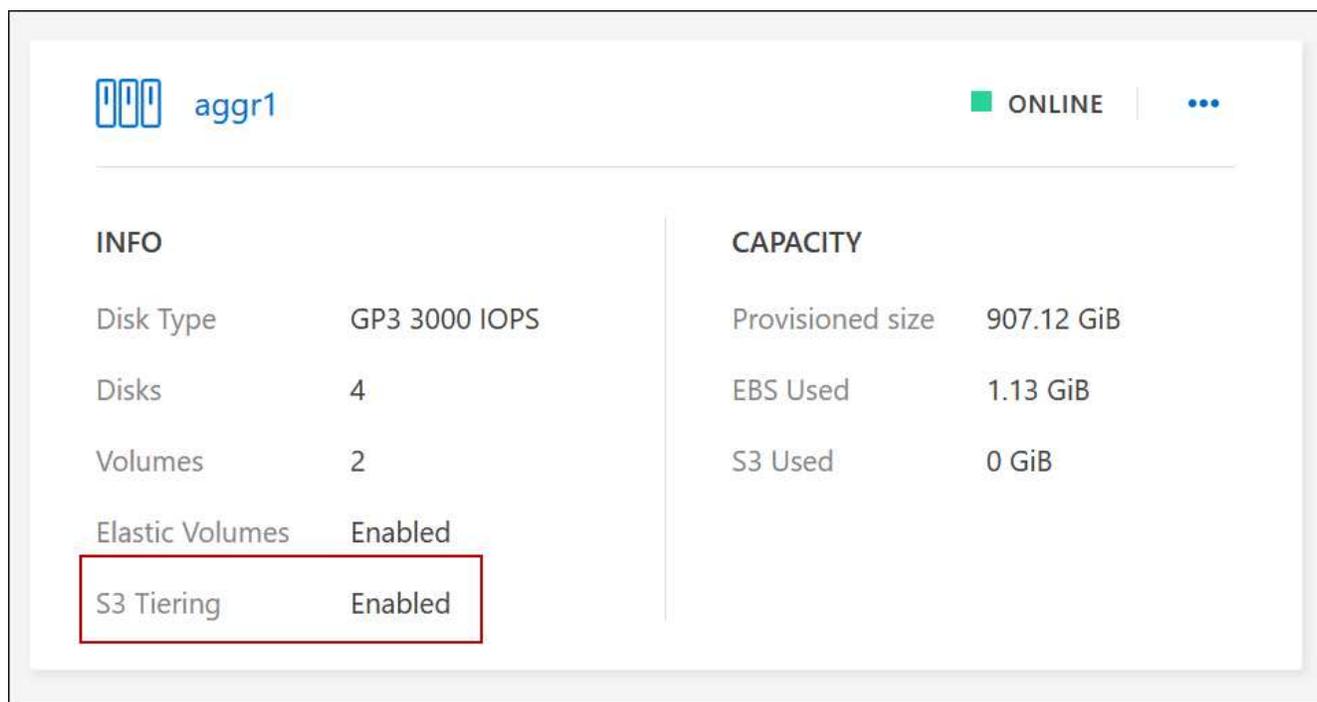
Se você está habilitando a disposição de dados em categorias em um novo volume, não precisa se preocupar em ativar a disposição de dados em categorias em um agregado. O BlueXP cria o volume em um agregado existente que tem a disposição em camadas ativada ou cria um novo agregado para o volume se um agregado habilitado para disposição em camadas de dados ainda não existir.

• Volumes existentes

Se você quiser habilitar a disposição em categorias de dados em um volume existente, precisará garantir que a disposição em categorias de dados esteja habilitada no agregado subjacente. Se a categorização de dados não estiver habilitada no agregado existente, você precisará usar o Gerenciador de sistema do ONTAP para anexar um agregado existente ao armazenamento de objetos.

Etapas para confirmar se a disposição em categorias está ativada em um agregado

1. Abra o ambiente de trabalho no BlueXP .
2. Clique na guia agregados.
3. Navegue até o bloco desejado e verifique se a disposição em camadas está ativada ou desativada no agregado.



Etapas para habilitar a disposição em camadas em um agregado

1. No Gerenciador do sistema ONTAP, clique em **armazenamento > camadas**.
2. Clique no menu de ação do agregado e selecione **Anexar camadas na nuvem**.
3. Selecione o nível de nuvem a anexar e clique em **Salvar**.

O que se segue?

Agora, você pode habilitar a disposição de dados em volumes novos e existentes, conforme explicado na próxima seção.

Disposição em camadas dos dados de volumes de leitura-gravação

O Cloud Volumes ONTAP pode categorizar dados inativos em volumes de leitura-gravação para storage de objetos econômico, liberando a categoria de performance para dados ativos.

Passos

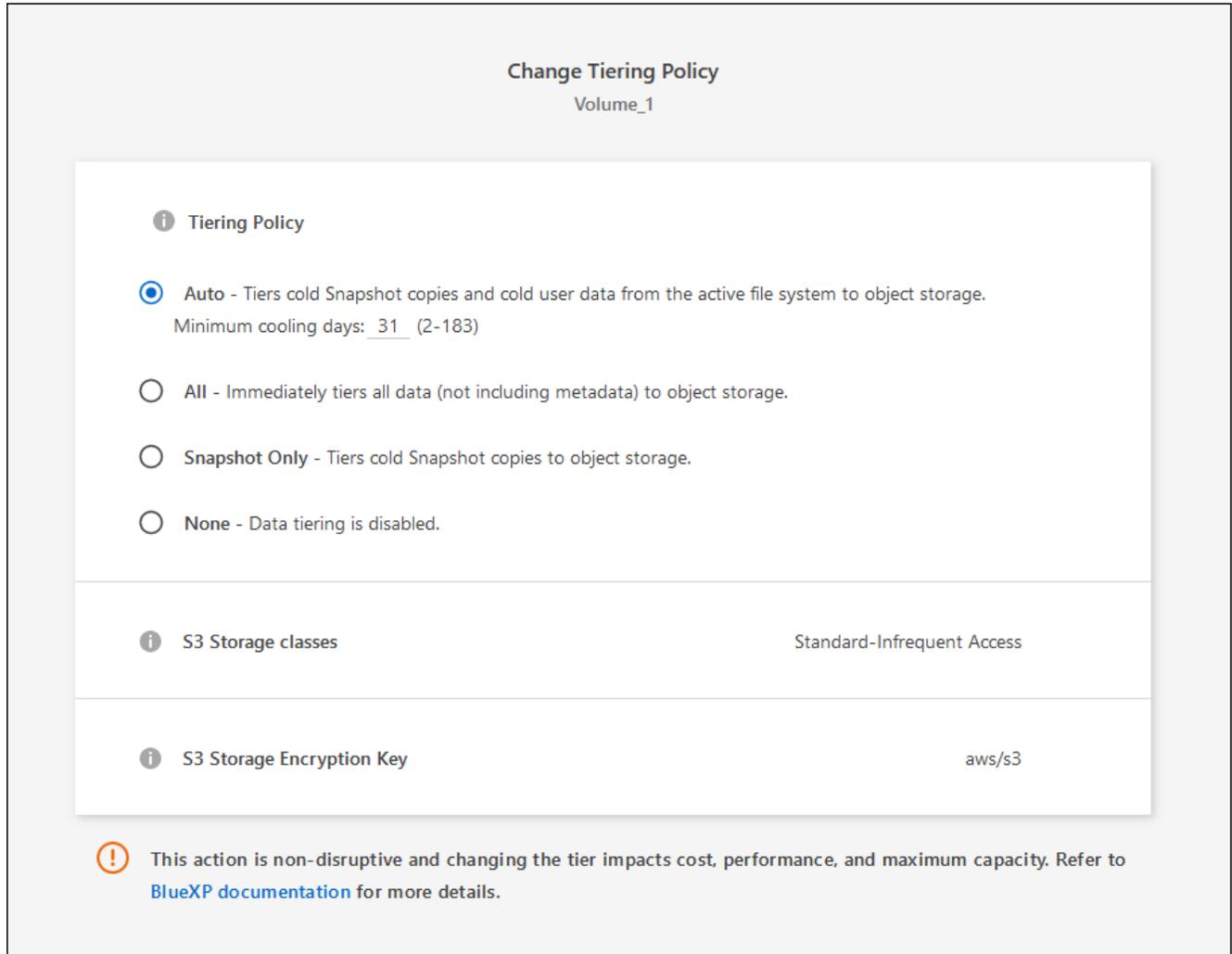
1. Na guia volumes no ambiente de trabalho, crie um novo volume ou altere o nível de um volume existente:

Tarefa	Ação
Crie um novo volume	Clique em Adicionar novo volume .
Modificar um volume existente	Selecione o bloco de volume desejado, clique em Gerenciar volume para acessar o painel direito Gerenciar volumes e, em seguida, clique em ações avançadas e alterar política de disposição em camadas no painel direito.

2. Selecione uma política de disposição em camadas.

Para obter uma descrição dessas políticas, "[Visão geral de categorização de dados](#)" consulte .

Exemplo



O BlueXP cria um novo agregado para o volume se um agregado habilitado para categorização de dados ainda não existir.

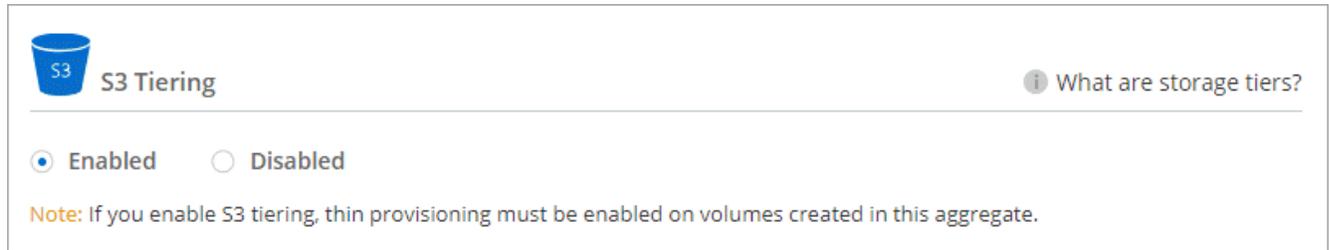
Disposição de dados em camadas em volumes de proteção de dados

O Cloud Volumes ONTAP pode categorizar dados de um volume de proteção de dados em uma categoria de capacidade. Se você ativar o volume de destino, os dados serão movidos gradualmente para o nível de performance à medida que forem lidos.

Passos

1. No menu de navegação à esquerda, selecione **Storage > Canvas**.
2. Na página Canvas, selecione o ambiente de trabalho que contém o volume de origem e arraste-o para o ambiente de trabalho para o qual você deseja replicar o volume.
3. Siga as instruções até chegar à página de disposição em categorias e habilitar a disposição de dados em categorias no storage de objetos.

Exemplo



Para obter ajuda com a replicação de dados, "[Replicação de dados de e para a nuvem](#)" consulte .

Alteração da classe de armazenamento para dados em camadas

Depois de implantar o Cloud Volumes ONTAP, você poderá reduzir os custos de storage alterando a classe de storage para dados inativos que não foram acessados por 30 dias. Os custos de acesso são maiores se você acessar os dados, então você deve levar isso em consideração antes de alterar a classe de storage.

A classe de armazenamento para dados em camadas é de todo o sistema, it não por volume.

Para obter informações sobre classes de armazenamento suportadas, "[Visão geral de categorização de dados](#)" consulte .

Passos

1. No ambiente de trabalho, clique no ícone de menu e, em seguida, clique em **classes de armazenamento ou disposição em camadas de armazenamento Blob**.
2. Escolha uma classe de armazenamento e clique em **Salvar**.

Alteração da taxa de espaço livre para categorização de dados

A taxa de espaço livre para categorização de dados define quanto espaço livre é necessário para SSDs/HDDs do Cloud Volumes ONTAP ao dispor dados em categorias para o storage de objetos. A configuração padrão é 10% de espaço livre, mas você pode ajustar a configuração com base em seus requisitos.

Por exemplo, você pode escolher menos de 10% de espaço livre para garantir que você esteja utilizando a capacidade adquirida. O BlueXP pode então comprar discos adicionais para você quando for necessária capacidade adicional (até atingir o limite de disco para o agregado).

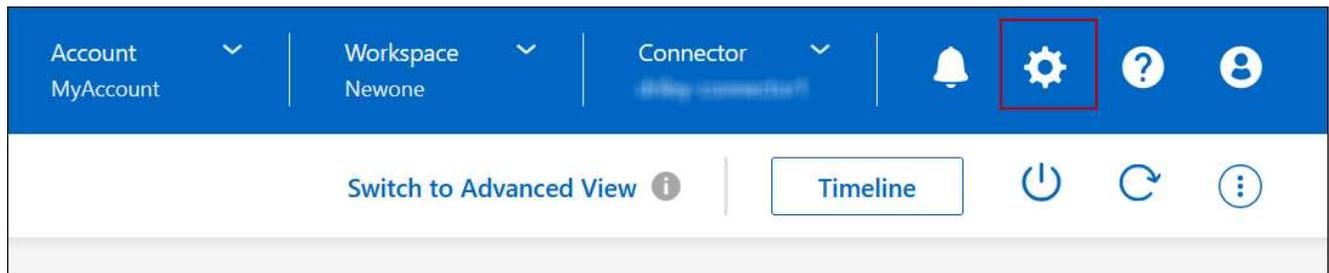


Se não houver espaço suficiente, o Cloud Volumes ONTAP não poderá mover os dados e você poderá sofrer degradação no desempenho. Qualquer alteração deve ser feita com cuidado. Se você não tiver certeza, entre em Contato com o suporte da NetApp para obter orientação.

A proporção é importante para cenários de recuperação de desastre porque, à medida que os dados são lidos do armazenamento de objetos, o Cloud Volumes ONTAP move os dados para SSDs/HDDs para fornecer melhor performance. Se não houver espaço suficiente, o Cloud Volumes ONTAP não poderá mover os dados. Leve isso em consideração ao alterar a taxa para que você possa atender aos requisitos de negócios.

Passos

1. No canto superior direito do console BlueXP , clique no ícone **Configurações** e selecione **Configurações do Cloud Volumes ONTAP**.



2. Em **capacidade**, clique em **limites de capacidade agregada - taxa de espaço livre para categorização de dados**.
3. Altere a taxa de espaço livre com base em suas necessidades e clique em **Salvar**.

Alterar o período de resfriamento da política de disposição automática em camadas

Se você habilitou a disposição de dados em categorias em um volume Cloud Volumes ONTAP usando a política de disposição em camadas *auto*, poderá ajustar o período de resfriamento padrão com base nas necessidades da sua empresa. Essa ação é suportada apenas usando a CLI e a API do ONTAP.

O período de resfriamento é o número de dias em que os dados do usuário em um volume devem permanecer inativos antes de serem considerados "frios" e movidos para o storage de objetos.

O período de resfriamento padrão da política de disposição automática em categorias é de 31 dias. Pode alterar o período de arrefecimento da seguinte forma:

- 9,8 dias ou mais tarde: 2 dias a 183 dias
- 9,7 ou mais cedo: 2 dias a 63 dias

Passo

1. Use o parâmetro *minimumCoolingDays* com sua solicitação de API ao criar um volume ou modificar um volume existente.

Conete um LUN a um host

Quando cria um volume iSCSI, o BlueXP cria automaticamente um LUN para si. Simplificamos a criação de apenas um LUN por volume, para que não haja gerenciamento envolvido. Depois de criar o volume, use o IQN para se conectar ao LUN a partir de seus hosts.

Observe o seguinte:

- O gerenciamento automático de capacidade do BlueXP não se aplica a LUNs. Quando o BlueXP cria um LUN, ele desativa o recurso de crescimento automático.
- Você pode criar LUNs adicionais no Gerenciador de sistemas do ONTAP ou na CLI do ONTAP.

Passos

1. No menu de navegação à esquerda, selecione **Storage > Canvas**.
2. Na página Canvas, clique duas vezes no ambiente de trabalho do Cloud Volumes ONTAP no qual você deseja gerenciar volumes.
3. No ambiente de trabalho, clique na guia **volumes**.

4. Na guia volumes, navegue até o título do volume desejado e clique em **Gerenciar volume** para acessar o painel direito Gerenciar volumes.
5. Clique em **Target IQN**.
6. Clique em **Copiar** para copiar o nome IQN.
7. Configure uma conexão iSCSI do host para o LUN.
 - ["Configuração expressa ONTAP 9 iSCSI para Red Hat Enterprise Linux: Iniciando as sessões iSCSI com o destino"](#)
 - ["Configuração expressa iSCSI ONTAP 9 para Windows: Iniciar sessões iSCSI com o destino"](#)
 - ["Configuração de host SAN ONTAP"](#)

Acelere o acesso aos dados com o FlexCache volumes

Um volume FlexCache é um volume de storage que armazena em cache dados de leitura de SMB e NFS de um volume de origem (ou origem). Leituras subsequentes para os dados armazenados em cache resultam em acesso mais rápido a esses dados.

Você pode usar o FlexCache volumes para acelerar o acesso aos dados ou descarregar tráfego de volumes acessados com muita facilidade. Os volumes FlexCache ajudam a melhorar o desempenho, especialmente quando os clientes precisam acessar os mesmos dados repetidamente, porque os dados podem ser fornecidos diretamente sem ter que acessar o volume de origem. O FlexCache volumes funciona bem com workloads do sistema com uso intenso de leitura.

O BlueXP fornece o gerenciamento do FlexCache volumes com o ["Armazenamento em cache de volume BlueXP"](#) serviço.

Você também pode usar a CLI ou o Gerenciador de sistemas do ONTAP ONTAP para criar e gerenciar o FlexCache volumes:

- ["Guia de energia do FlexCache volumes para acesso mais rápido aos dados"](#)
- ["Criando volumes FlexCache no Gerenciador de sistemas"](#)



Trabalhe com o FlexCache quando a origem for criptografada

Ao configurar o FlexCache em um sistema Cloud Volumes ONTAP onde o volume de origem é criptografado, etapas adicionais são necessárias para garantir que o volume FlexCache possa acessar e armazenar adequadamente os dados criptografados.

O que você vai precisar

1. **Configuração de criptografia:** Certifique-se de que o volume de origem esteja totalmente criptografado e operacional. Para sistemas Cloud Volumes ONTAP, isso envolve a integração com serviços de gerenciamento de chaves específicos da nuvem.

Para a AWS, isso geralmente significa usar o AWS Key Management Service (KMS). Para obter informações, "[Gerencie chaves com o AWS Key Management Service](#)" consulte .

Para o Azure, você precisa configurar o Azure Key Vault para criptografia de volume do NetApp (NVE). Para obter informações, "[Gerencie chaves com o Azure Key Vault](#)" consulte .

Para o Google Cloud, é o Google Cloud Key Management Service. Para obter informações, "[Gerencie chaves com o Cloud Key Management Service do Google](#)" consulte .

1. **Serviços de gerenciamento de chaves:** Antes de criar um volume FlexCache, verifique se os serviços de gerenciamento de chaves estão configurados corretamente no sistema Cloud Volumes ONTAP. Esta configuração é essencial para que o volume FlexCache descriptografe os dados do volume de origem.
2. **Licenciamento:** Confirme se uma licença FlexCache válida está disponível e ativada no sistema Cloud Volumes ONTAP.
3. **Versão ONTAP:** Certifique-se de que a versão ONTAP do seu sistema Cloud Volumes ONTAP suporte FlexCache com volumes criptografados. Consulte a matriz de compatibilidade ou mais recente "[Notas de versão do ONTAP](#)" para obter mais informações.
4. **Configuração de rede:** Certifique-se de que a configuração de rede permite uma comunicação perfeita entre o volume de origem e o volume FlexCache. Isso inclui roteamento adequado e resolução DNS em

um ambiente de nuvem.

Passos

Crie um volume FlexCache no seu sistema Cloud Volumes ONTAP com um volume de origem criptografado. Para obter instruções detalhadas e considerações adicionais, consulte as seguintes seções:

- ["Guia de energia do FlexCache volumes para acesso mais rápido aos dados"](#)
- ["Criando volumes FlexCache no Gerenciador de sistemas"](#)

Administração de agregados

Criar agregados

Você mesmo pode criar agregados ou permitir que o BlueXP faça isso por você quando cria volumes. O benefício de criar agregados por conta própria é que você pode escolher o tamanho de disco subjacente, que permite dimensionar seu agregado para a capacidade ou a performance de que precisa.



Todos os discos e agregados devem ser criados e excluídos diretamente do BlueXP . Você não deve executar essas ações de outra ferramenta de gerenciamento. Isso pode afetar a estabilidade do sistema, dificultar a capacidade de adicionar discos no futuro e, potencialmente, gerar taxas redundantes de provedores de nuvem.

Passos

1. No menu de navegação à esquerda, selecione **Storage > Canvas**.
2. Na página tela, clique duas vezes no nome da instância do Cloud Volumes ONTAP na qual você deseja gerenciar agregados.
3. Na guia agregados, clique em **Adicionar agregado** e especifique detalhes para o agregado.

AWS

- Se você for solicitado a escolher um tipo de disco e tamanho de disco, "[Planeje sua configuração do Cloud Volumes ONTAP na AWS](#)" consulte .
- Se você for solicitado a inserir o tamanho da capacidade do agregado, então você estará criando um agregado em uma configuração que suporte o recurso volumes elásticos do Amazon EBS. A captura de tela a seguir mostra um exemplo de um novo agregado composto por GP3 discos.

1 Disk Type 2 Aggregate details 3 Tiering Data 4 Review

Select Disk Type

Disk Type

GP3 - General Purpose SSD Dynamic Performance

 **General Purpose SSD (gp3) Disk Properties**

Description: General purpose SSD volume that balances price and performance (performance level is independent of storage capacity)

IOPS Value  Throughput MB/s 

12000  250 

["Saiba mais sobre o suporte para volumes elásticos"](#).

Azure

Para obter ajuda sobre o tipo de disco e o tamanho do disco, "[Planeje sua configuração do Cloud Volumes ONTAP no Azure](#)" consulte .

Google Cloud

Para obter ajuda sobre o tipo de disco e o tamanho do disco, "[Planeje sua configuração do Cloud Volumes ONTAP no Google Cloud](#)" consulte .

4. Clique em **Go** e, em seguida, clique em **Approve and Purchase**.

Gerenciar agregados

Gerencie os agregados adicionando discos, visualizando informações sobre os agregados e excluindo-os.



Todos os discos e agregados devem ser criados e excluídos diretamente do BlueXP. Você não deve executar essas ações de outra ferramenta de gerenciamento. Isso pode afetar a estabilidade do sistema, dificultar a capacidade de adicionar discos no futuro e, potencialmente, gerar taxas redundantes de provedores de nuvem.

Antes de começar

Se você quiser excluir um agregado, primeiro você deve ter excluído os volumes no agregado.

Sobre esta tarefa

Se um agregado estiver sem espaço, você poderá mover volumes para outro agregado usando o Gerenciador de sistema do ONTAP.

Passos

1. No menu de navegação à esquerda, selecione **Storage > Canvas**.
2. Na página Canvas, clique duas vezes no ambiente de trabalho do Cloud Volumes ONTAP no qual você deseja gerenciar agregados.
3. No ambiente de trabalho, clique na guia **agregados**.
4. Na guia agregados, navegue até o título desejado e clique em ... (**ícone de elipses**).

5. Gerencie seus agregados:

Tarefa	Ação
Exibir informações sobre um agregado	Sob o ... (Ícone de elipses), clique em Exibir detalhes de agregados .

Tarefa	Ação
Crie um volume em um agregado específico	Sob o ... (Ícone de elipses), clique em Adicionar volume .
Adicione discos a um agregado	<p>a. Sob o ... (Ícone de elipses), clique em Add Disks (Adicionar discos).</p> <p>b. Selecione o número de discos que deseja adicionar e clique em Adicionar.</p> <div style="display: flex; align-items: center; margin-top: 10px;">  <p>Todos os discos em um agregado devem ter o mesmo tamanho.</p> </div>
Aumente a capacidade de um agregado que suporte volumes elásticos do Amazon EBS	<p>a. Sob o ... (Ícone de elipses), clique em aumentar a capacidade.</p> <p>b. Introduza a capacidade adicional que pretende adicionar e, em seguida, clique em aumentar.</p> <p>Observe que você deve aumentar a capacidade do agregado em um mínimo de 256 GiB ou 10% do tamanho do agregado.</p> <p>Por exemplo, se você tem um agregado de 1,77 TiB, 10% é de 181 GiB. Isso é inferior a 256 GiB, então o tamanho do agregado deve ser aumentado pelo mínimo de 256 GiB.</p>
Excluir um agregado	<p>a. Selecione um bloco agregado que não contenha nenhum volume clique em ... (Ícone de elipses) > Eliminar.</p> <p>b. Clique em Delete novamente para confirmar.</p>

Gerencie as configurações de capacidade em um conector

Cada conector tem configurações que determinam como ele gerencia a capacidade agregada do Cloud Volumes ONTAP.

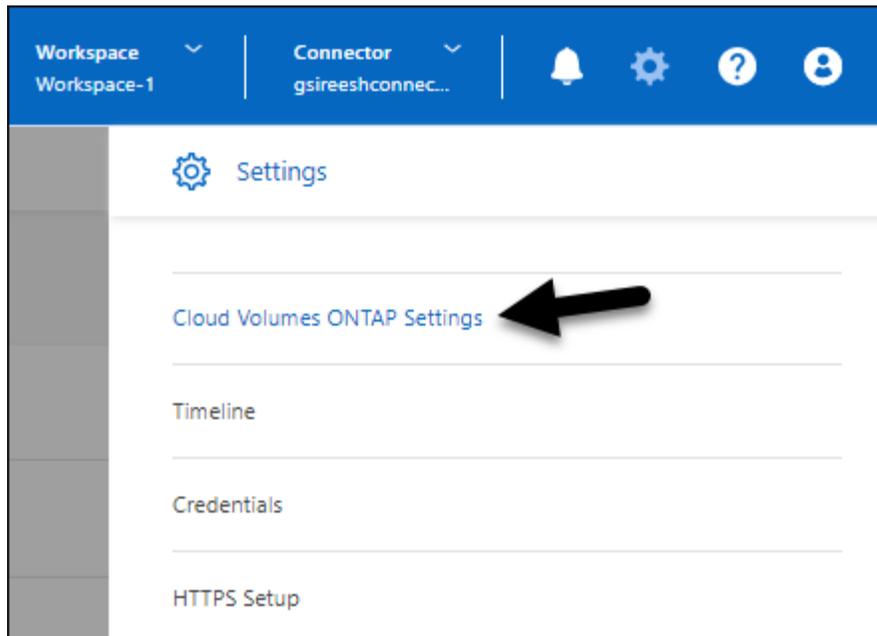
Essas configurações afetam todos os sistemas Cloud Volumes ONTAP gerenciados por um conector. Se você tiver outro conector, ele pode ser configurado de forma diferente.

Permissões necessárias

A Organização BlueXP ou o administrador da conta Privileges são necessários para modificar as configurações do Cloud Volumes ONTAP.

Passos

1. No canto superior direito do console BlueXP, clique no ícone Configurações e selecione **Configurações do Cloud Volumes ONTAP**.



2. Em **Capacity**, modifique qualquer uma das seguintes configurações:

Modo de gerenciamento de capacidade

Escolha se o BlueXP notifica você sobre decisões de capacidade de storage ou se o BlueXP gerencia automaticamente os requisitos de capacidade para você.

["Saiba como o modo de gerenciamento de capacidade funciona"](#).

Limite capacidade agregada - rácio espaço livre

Essa proporção é um parâmetro chave nas decisões de gerenciamento de capacidade, e entender seu impactos é essencial independentemente de você estar em um modo automático ou manual de gerenciamento de capacidade. Recomenda-se definir esse limite considerando suas necessidades de storage específicas e o crescimento esperado para manter um equilíbrio entre a utilização de recursos e o custo.

No modo manual, se a taxa de espaço livre em um agregado cair abaixo do limite especificado, ele aciona uma notificação, alertando você que você deve tomar medidas para resolver a baixa taxa de espaço livre. É importante monitorar essas notificações e gerenciar manualmente a capacidade agregada para evitar interrupções no serviço e garantir o desempenho ideal.

A razão de espaço livre é calculada da seguinte forma: $(\text{Capacidade agregada} - \text{capacidade total utilizada no agregado}) / \text{capacidade agregada}$

["Gerenciamento automático de capacidade"](#) Consulte para saber agora a capacidade é gerenciada automaticamente no Cloud Volumes ONTAP.

Limites de capacidade agregada - taxa de espaço livre para categorização de dados

Define quanto espaço livre é necessário na camada de performance (discos) ao categorizar dados em uma camada de capacidade (storage de objetos).

A proporção é importante para cenários de recuperação de desastres. À medida que os dados são lidos na camada de capacidade, a Cloud Volumes ONTAP migra os dados para a camada de performance a fim de fornecer melhor performance. Se não houver espaço suficiente, o Cloud Volumes ONTAP não poderá mover os dados.

3. Clique em **Salvar**.

Administração da VM de storage

Gerenciar VMs de storage no BlueXP

Uma VM de armazenamento é uma máquina virtual em execução no ONTAP que fornece serviços de armazenamento e dados aos seus clientes. Você pode saber isso como um *SVM* ou um *vserver*. O Cloud Volumes ONTAP é configurado com uma VM de storage por padrão, mas algumas configurações oferecem suporte a VMs de storage adicionais.

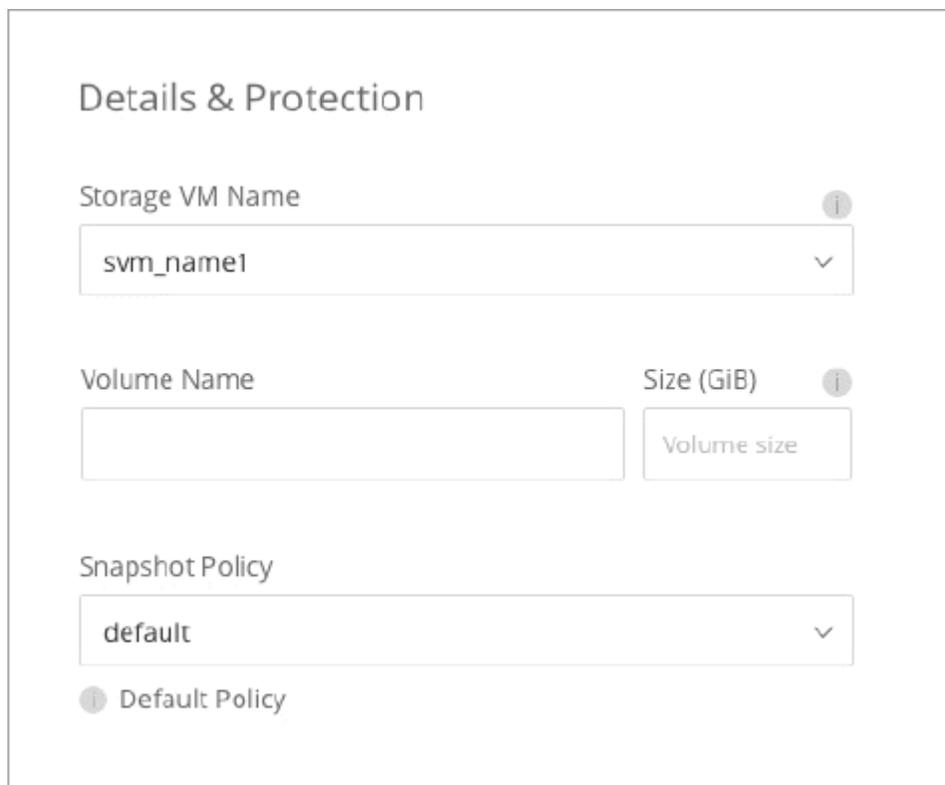
Número suportado de VMs de storage

Várias VMs de storage são compatíveis com certas configurações. Vá para "[Notas de versão do Cloud Volumes ONTAP](#)" a para verificar o número suportado de VMs de armazenamento para a sua versão do Cloud Volumes ONTAP.

Trabalhar com várias VMs de storage

O BlueXP dá suporte a quaisquer VMs de storage adicionais criadas pelo Gerenciador de sistemas do ONTAP ou pela CLI do ONTAP.

Por exemplo, a imagem a seguir mostra como você pode escolher uma VM de armazenamento ao criar um volume.



The screenshot shows a configuration interface titled "Details & Protection". It contains the following elements:

- Storage VM Name:** A dropdown menu with "svm_name1" selected and a downward arrow.
- Volume Name:** An empty text input field.
- Size (GiB):** A text input field containing "Volume size" and a button labeled "Volume size".
- Snapshot Policy:** A dropdown menu with "default" selected and a downward arrow.
- Default Policy:** A link with an information icon and the text "Default Policy".

E a imagem a seguir mostra como você pode escolher uma VM de storage ao replicar um volume para outro sistema.

Destination Volume Name

Destination Storage VM Name

Destination Aggregate

Modifique o nome da VM de armazenamento padrão

O BlueXP nomeia automaticamente a VM de storage única que cria para o Cloud Volumes ONTAP. No Gerenciador de sistemas do ONTAP, na CLI ou na API do ONTAP, você pode modificar o nome da VM de storage se tiver padrões rígidos de nomenclatura. Por exemplo, talvez você queira que o nome corresponda ao nome das VMs de storage dos clusters do ONTAP.

Crie VMs de storage de fornecimento de dados para o Cloud Volumes ONTAP na AWS

Uma VM de armazenamento é uma máquina virtual em execução no ONTAP que fornece serviços de armazenamento e dados aos seus clientes. Você pode saber isso como um *SVM* ou um *vserver*. O Cloud Volumes ONTAP é configurado com uma VM de storage por padrão, mas algumas configurações oferecem suporte a VMs de storage adicionais.

Para criar VMs de storage adicionais de fornecimento de dados, você precisa alocar endereços IP na AWS e executar comandos ONTAP com base na configuração do Cloud Volumes ONTAP.

Número suportado de VMs de storage

Várias VMs de storage são compatíveis com configurações Cloud Volumes ONTAP específicas, começando com a versão 9,7. Vá para "[Notas de versão do Cloud Volumes ONTAP](#)" a para verificar o número suportado de VMs de armazenamento para a sua versão do Cloud Volumes ONTAP.

Todas as outras configurações do Cloud Volumes ONTAP oferecem suporte a uma VM de storage de fornecimento de dados e a uma VM de storage de destino usada para recuperação de desastres. Você pode ativar a VM de storage de destino para acesso aos dados se houver uma interrupção na VM de storage de origem.

Verifique os limites da sua configuração

Cada instância do EC2 suporta um número máximo de endereços IPv4 privados por interface de rede. Você precisa verificar o limite antes de alocar endereços IP na AWS para a nova VM de armazenamento.

Passos

1. Vá para "[Limites de armazenamento seção nas Notas de versão do Cloud Volumes ONTAP](#)".
2. Identifique o número máximo de endereços IP por interface para o tipo de instância.
3. Anote esse número porque você precisará dele na próxima seção quando alocar endereços IP na AWS.

Alocar endereços IP na AWS

Os endereços IPv4 privados devem ser atribuídos à porta e0a na AWS antes de criar LIFs para a nova VM de storage.

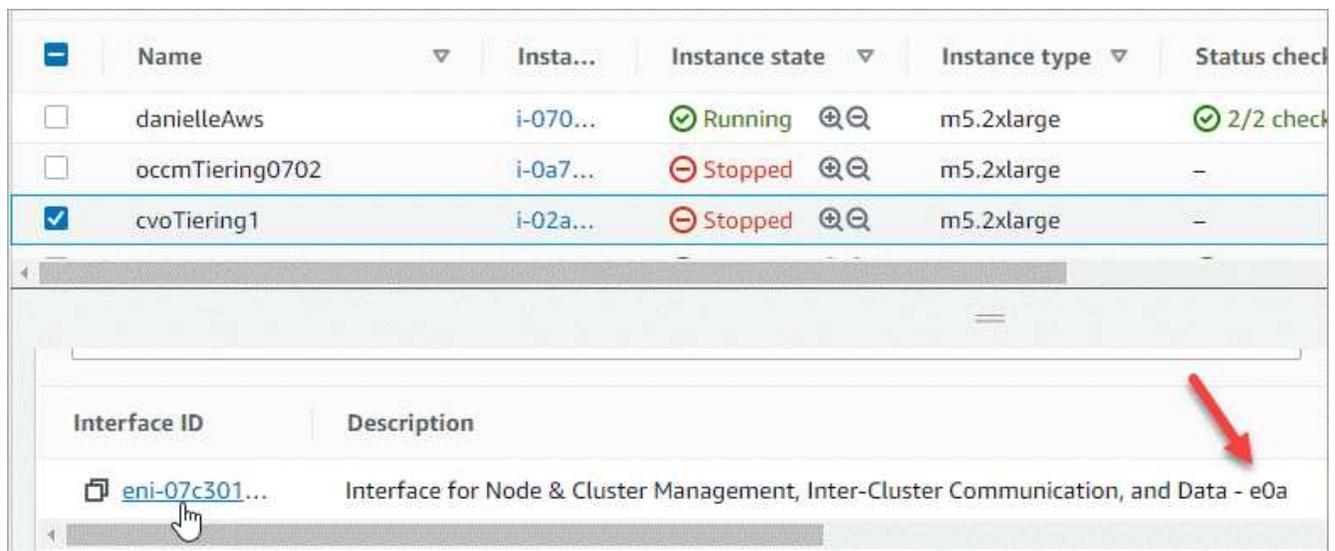
Observe que um LIF de gerenciamento opcional para uma VM de storage requer um endereço IP privado em um sistema de nó único e em um par de HA em uma única AZ. Esse LIF de gerenciamento fornece uma conexão com ferramentas de gerenciamento como o SnapCenter.

Passos

1. Faça login na AWS e abra o serviço EC2.
2. Selecione a instância do Cloud Volumes ONTAP e clique em **rede**.

Se você estiver criando uma VM de storage em um par de HA, selecione o nó 1.

3. Role para baixo até **interfaces de rede** e clique no **ID da interface** para a porta e0a.



4. Selecione a interface de rede e clique em **ações > Gerenciar endereços IP**.
5. Expanda a lista de endereços IP para e0a.
6. Verifique os endereços IP:
 - a. Conte o número de endereços IP alocados para confirmar se a porta tem espaço para IPs adicionais.

Você deve ter identificado o número máximo de endereços IP suportados por interface na seção anterior desta página.

- b. Opcional: Vá para a CLI do ONTAP para Cloud Volumes ONTAP e execute **network interface show** para confirmar que cada um desses endereços IP está em uso.

Se um endereço IP não estiver em uso, você poderá usá-lo com a nova VM de armazenamento.

7. De volta ao Console da AWS, clique em **Assign new IP address** (atribuir novo endereço IP) para atribuir endereços IP adicionais com base na quantidade necessária para a nova VM de armazenamento.
 - Sistema de nó único: É necessário um IP privado secundário não utilizado.

Um IP privado secundário opcional é necessário se você quiser criar um LIF de gerenciamento na VM de armazenamento.
 - Par DE HA em uma única AZ: Um IP privado secundário não utilizado é necessário no nó 1.

Um IP privado secundário opcional é necessário se você quiser criar um LIF de gerenciamento na VM de armazenamento.
 - Par HA em vários AZs: Um IP privado secundário não utilizado é necessário em cada nó.
8. Se você estiver alocando o endereço IP em um par de HA em uma única AZ, habilite **permitir que endereços IPv4 privados secundários sejam reatribuídos**.
9. Clique em **Salvar**.
10. Se você tiver um par de HA em vários AZs, precisará repetir estas etapas para o nó 2.

Crie uma VM de storage em um único sistema de nó

Essas etapas criam uma nova VM de storage em um sistema de nó único. Um endereço IP privado é necessário para criar um LIF nas e outro endereço IP privado opcional é necessário se você quiser criar um LIF de gerenciamento.

Passos

1. Crie a VM de armazenamento e uma rota para a VM de armazenamento.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2  
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway  
subnet_gateway
```

2. Crie um nas LIF.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-data-files -home-port e0a -address private_ip_x -netmask  
node1Mask -lif ip_nas_2 -home-node cvo-node
```

Onde *private_IP_x* é um IP privado secundário não utilizado no e0a.

3. Opcional: Crie um LIF de gerenciamento de VM de storage.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node
```

Onde *private_IP_y* é outro IP privado secundário não utilizado no e0a.

4. Atribua um ou mais agregados à VM de storage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Essa etapa é necessária porque a nova VM de storage precisa ter acesso a pelo menos um agregado antes de criar volumes na VM de storage.

Criar uma VM de storage em um par de HA em uma única AZ

Essas etapas criam uma nova VM de storage em um par de HA em uma única AZ. Um endereço IP privado é necessário para criar um LIF nas e outro endereço IP privado opcional é necessário se você quiser criar um LIF de gerenciamento.

Ambos os LIFs são alocados no nó 1. Os endereços IP privados podem se mover entre nós se ocorrerem falhas.

Passos

1. Crie a VM de armazenamento e uma rota para a VM de armazenamento.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. Crie um nas LIF no nó 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node1
```

Onde *private_IP_x* é um IP privado secundário não utilizado no e0a do cvo-node1. Esse endereço IP pode ser relocado para o e0a do cvo-node2 em caso de aquisição, pois os arquivos-dados-padrão da política de serviço indicam que os IPs podem migrar para o nó do parceiro.

3. Opcional: Crie um LIF de gerenciamento de VM de storage no nó 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

Onde *private_IP_y* é outro IP privado secundário não utilizado no e0a.

4. Atribua um ou mais agregados à VM de storage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Essa etapa é necessária porque a nova VM de storage precisa ter acesso a pelo menos um agregado antes de criar volumes na VM de storage.

5. Se você estiver executando o Cloud Volumes ONTAP 9.11.1 ou posterior, modifique as políticas de serviço de rede para a VM de storage.

A modificação dos serviços é necessária porque garante que o Cloud Volumes ONTAP possa usar o iSCSI LIF para conexões de gerenciamento de saída.

```

network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client

```

Crie uma VM de storage em um par de HA em vários AZs

Essas etapas criam uma nova VM de storage em um par de HA em vários AZs.

Um endereço IP *flutuante* é necessário para um LIF nas e é opcional para um LIF de gerenciamento. Esses endereços IP flutuantes não exigem que você aloque IPs privados na AWS. Em vez disso, os IPs flutuantes são configurados automaticamente na tabela de rotas da AWS para apontar para o ENI de um nó específico na mesma VPC.

Para que os IPs flutuantes funcionem com o ONTAP, um endereço IP privado deve ser configurado em cada VM de armazenamento em cada nó. Isso se reflete nas etapas abaixo em que um iSCSI LIF é criado no nó 1 e no nó 2.

Passos

1. Crie a VM de armazenamento e uma rota para a VM de armazenamento.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. Crie um nas LIF no nó 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_nas_floating_2 -home-node cvo-node1
```

- O endereço IP flutuante deve estar fora dos blocos CIDR para todos os VPCs na região da AWS na qual você implementa a configuração de HA. 192.168.209.27 é um exemplo de endereço IP flutuante. ["Saiba mais sobre como escolher um endereço IP flutuante"](#).
- `-service-policy default-data-files` Indica que os IPs podem migrar para o nó do parceiro.

3. Opcional: Crie um LIF de gerenciamento de VM de storage no nó 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

4. Crie um iSCSI LIF no nó 1.

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmask node1Mask -lif
ip_node1_iscsi_2 -home-node cvo-node1
```

- Este iSCSI LIF é necessário para suportar a migração de LIF dos IPs flutuantes na VM de armazenamento. Ele não precisa ser um iSCSI LIF, mas não pode ser configurado para migrar entre nós.
- `-service-policy default-data-block` Indica que um endereço IP não migra entre nós.
- `Private_ip` é um endereço IP privado secundário não utilizado no eth0 (e0a) do `cvo_node1`.

5. Crie um iSCSI LIF no nó 2.

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmaskNode2Mask -lif
ip_node2_iscsi_2 -home-node cvo-node2
```

- Este iSCSI LIF é necessário para suportar a migração de LIF dos IPs flutuantes na VM de armazenamento. Ele não precisa ser um iSCSI LIF, mas não pode ser configurado para migrar entre nós.
- `-service-policy default-data-block` Indica que um endereço IP não migra entre nós.
- `Private_ip` é um endereço IP privado secundário não utilizado no eth0 (e0a) do `cvo_node2`.

6. Atribua um ou mais agregados à VM de storage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Essa etapa é necessária porque a nova VM de storage precisa ter acesso a pelo menos um agregado antes de criar volumes na VM de storage.

7. Se você estiver executando o Cloud Volumes ONTAP 9.11.1 ou posterior, modifique as políticas de serviço de rede para a VM de storage.

A modificação dos serviços é necessária porque garante que o Cloud Volumes ONTAP possa usar o iSCSI LIF para conexões de gerenciamento de saída.

```

network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client

```

Crie VMs de storage de fornecimento de dados para o Cloud Volumes ONTAP no Azure

Uma VM de armazenamento é uma máquina virtual em execução no ONTAP que fornece serviços de armazenamento e dados aos seus clientes. Você pode saber isso como um *SVM* ou um *vserver*. O Cloud Volumes ONTAP é configurado com uma VM de storage por padrão, mas há suporte para VMs de storage adicionais ao executar o Cloud Volumes ONTAP no Azure.

Para criar VMs de storage adicionais de fornecimento de dados, você precisa alocar endereços IP no Azure e executar comandos ONTAP para criar a VM de storage e LIFs de dados.



Para executar tarefas adicionais relacionadas à NIC, você pode atribuir uma função de colaborador de rede ou uma função personalizada com permissões apropriadas no Azure. Para obter mais informações sobre essas permissões relacionadas à NIC, consulte o ["Documentação do Microsoft Azure"](#).

Número suportado de VMs de storage

Várias VMs de storage são compatíveis com configurações Cloud Volumes ONTAP específicas, começando com a versão 9.9.0. Vá para ["Notas de versão do Cloud Volumes ONTAP"](#) a para verificar o número suportado de VMs de armazenamento para a sua versão do Cloud Volumes ONTAP.

Todas as outras configurações do Cloud Volumes ONTAP oferecem suporte a uma VM de storage de fornecimento de dados e a uma VM de storage de destino usada para recuperação de desastres. Você pode ativar a VM de storage de destino para acesso aos dados se houver uma interrupção na VM de storage de origem.

Alocar endereços IP no Azure

Você precisa alocar endereços IP no Azure antes de criar uma VM de storage e alocar LIFs.

Sistema de nó único

Os endereços IP devem ser atribuídos ao nic0 no Azure antes de criar uma VM de armazenamento e alocar LIFs.

Você precisará criar um endereço IP para acesso a LIF de dados e outro endereço IP opcional para um LIF de gerenciamento de VM de storage (SVM). Esse LIF de gerenciamento fornece uma conexão com ferramentas de gerenciamento como o SnapCenter.

Passos

1. Faça login no portal do Azure e abra o serviço **Virtual Machine**.
2. Clique no nome da VM Cloud Volumes ONTAP.
3. Clique em **Networking**.
4. Clique no nome da interface de rede para nic0.
5. Em **Configurações**, clique em **configurações IP**.
6. Clique em **Add**.
7. Introduza um nome para a configuração IP, selecione **Dynamic** e, em seguida, clique em **OK**.
8. Clique no nome da configuração IP que você acabou de criar, altere a atribuição * para **estática** e clique em **Salvar**.

É melhor usar um endereço IP estático porque um IP estático garante que o endereço IP não mudará, o que pode ajudar a evitar interrupções desnecessárias para o seu aplicativo.

Se você quiser criar um LIF de gerenciamento de SVM, repita estas etapas para criar um endereço IP adicional.

Depois de terminar

Copie os endereços IP privados que você acabou de criar. Você precisará especificar esses endereços IP ao criar LIFs para a nova VM de armazenamento.

Par de HA

Para pares de alta disponibilidade (HA), você deve acessar cada VM de storage (SVM) no cluster e criar IPs correspondentes em nic0 para cada SVM. A forma como você aloca endereços IP para um par de HA depende do protocolo de storage que você está usando. No modo HA, os usuários devem garantir que os endereços IP estejam corretamente configurados para suportar failover e redundância, o que é essencial para manter a alta disponibilidade e confiabilidade do sistema de storage.

ISCSI

Os endereços IP iSCSI devem ser atribuídos ao nic0 no Azure antes de criar uma VM de armazenamento e alocar LIFs. Os IPs para iSCSI são atribuídos a nic0 e não ao balanceador de carga porque o iSCSI usa o ALUA para failover.

Você precisará criar os seguintes endereços IP:

- Um endereço IP para acesso iSCSI data LIF a partir do nó 1
- Um endereço IP para acesso iSCSI data LIF a partir do nó 2
- Um endereço IP opcional para um LIF de gerenciamento da SVM

Esse LIF de gerenciamento fornece uma conexão com ferramentas de gerenciamento como o SnapCenter.

Passos

1. Faça login no portal do Azure e abra o serviço **Virtual Machine**.
2. Clique no nome da VM do Cloud Volumes ONTAP para o nó 1.
3. Clique em **Networking**.
4. Clique no nome da interface de rede para nic0.
5. Em **Configurações**, clique em **configurações IP**.
6. Clique em **Add**.
7. Introduza um nome para a configuração IP, selecione **Dynamic** e, em seguida, clique em **OK**.
8. Clique no nome da configuração IP que você acabou de criar, altere a atribuição * para **estática** e clique em **Salvar**.

É melhor usar um endereço IP estático porque um IP estático garante que o endereço IP não mudará, o que pode ajudar a evitar interrupções desnecessárias para o seu aplicativo.

9. Repita estas etapas no nó 2.
10. Se você quiser criar um LIF de gerenciamento de SVM, repita estas etapas no nó 1.

NFS

Os endereços IP usados para NFS são alocados no balanceador de carga para que os endereços IP possam migrar para o outro nó caso ocorram eventos de failover.

Você precisará criar os seguintes endereços IP:

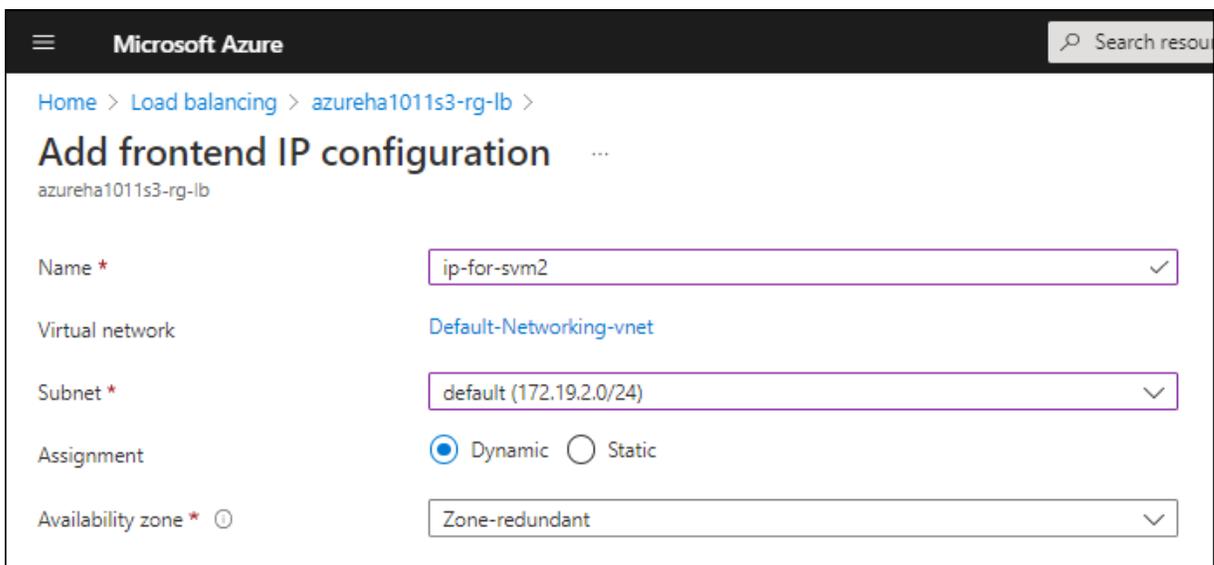
- Um endereço IP para acesso de LIF de dados nas a partir do nó 1
- Um endereço IP para acesso de LIF de dados nas a partir do nó 2
- Um endereço IP opcional para um LIF de gerenciamento de VM de storage (SVM)

Os iSCSI LIFs são necessários para a comunicação DNS mesmo quando o protocolo iSCSI não é usado. Um iSCSI LIF é usado para esse fim porque não migra no failover.

Esse LIF de gerenciamento fornece uma conexão com ferramentas de gerenciamento como o SnapCenter.

Passos

1. No portal do Azure, abra o serviço **Load Balancers**.
2. Clique no nome do balanceador de carga do par de HA.
3. Crie uma configuração de IP frontend para acesso de LIF de dados do nó 1, outra para acesso de LIF de dados do nó 2 e outro IP frontend opcional para um LIF de gerenciamento de VM de armazenamento (SVM).
 - a. Em **Settings**, clique em **Frontend IP Configuration**.
 - b. Clique em **Add**.
 - c. Digite um nome para o IP frontend, selecione a sub-rede para o par de HA Cloud Volumes ONTAP, deixe **Dinâmico** selecionado e, em regiões com zonas de disponibilidade, deixe **zona redundante** selecionado para garantir que o endereço IP permaneça disponível se uma zona falhar.
 - d. Clique em **Salvar**.



The screenshot shows the 'Add frontend IP configuration' page in the Microsoft Azure portal. The breadcrumb trail is 'Home > Load balancing > azureha1011s3-rg-lb >'. The title is 'Add frontend IP configuration' with a three-dot menu icon. Below the title is the resource name 'azureha1011s3-rg-lb'. The form contains the following fields:

- Name ***: A text input field containing 'ip-for-svm2' with a checkmark icon on the right.
- Virtual network**: A dropdown menu showing 'Default-Networking-vnet'.
- Subnet ***: A dropdown menu showing 'default (172.19.2.0/24)' with a downward arrow icon.
- Assignment**: Two radio buttons, 'Dynamic' (which is selected) and 'Static'.
- Availability zone ***: A dropdown menu showing 'Zone-redundant' with a downward arrow icon and a help icon.

- e. Clique no nome da configuração IP frontend que você acabou de criar, altere **Assignment** para **Static** e clique em **Save**.

É melhor usar um endereço IP estático porque um IP estático garante que o endereço IP não mudará, o que pode ajudar a evitar interrupções desnecessárias para o seu aplicativo.

4. Adicione uma sonda de saúde para cada IP frontend que você acabou de criar.
 - a. Em **Settings** do balanceador de carga, clique em **Health probes**.
 - b. Clique em **Add**.
 - c. Introduza um nome para a sonda de saúde e introduza um número de porta entre 63005 e 65000. Mantenha os valores padrão para os outros campos.

É importante que o número da porta esteja entre 63005 e 65000. Por exemplo, se você estiver criando três sondas de saúde, poderá inserir sondas que usam os números de porta 63005, 63006 e 63007.

Microsoft Azure Search resources, services, and

Home > Load balancers > azureha1011s3-rg-lb >

Add health probe

azureha1011s3-rg-lb

Name *	svm2-health-probe1 ✓
Protocol *	TCP ▼
Port * ⓘ	63005 ✓
Interval * ⓘ	5 seconds
Unhealthy threshold * ⓘ	2 consecutive failures
Used by ⓘ	Not used

5. Crie novas regras de balanceamento de carga para cada IP frontend.

a. Em **Configurações** do balanceador de carga, clique em **regras de balanceamento de carga**.

b. Clique em **Add** e insira as informações necessárias:

- **Nome:** Insira um nome para a regra.
- **Versão IP:** Selecione **IPv4**.
- **Frontend IP address:** Selecione um dos endereços IP frontend que você acabou de criar.
- **Portas HA:** Ative esta opção.
- **Pool de back-end:** Mantenha o pool de back-end padrão que já foi selecionado.
- **Sonda de saúde:** Selecione a sonda de saúde que você criou para o IP frontend selecionado.
- **Persistência da sessão:** Selecione **nenhum**.
- **Floating IP:** Selecione **Enabled**.

Add load balancing rule ⋮

chandanaTcpRst3-rg-lb

i A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name *

IP Version *
 IPv4 IPv6

Frontend IP address * ⓘ

HA Ports ⓘ

Backend pool ⓘ

Health probe ⓘ

Session persistence ⓘ

Floating IP ⓘ

6. Certifique-se de que as regras do grupo de segurança de rede para o Cloud Volumes ONTAP permitem que o balanceador de carga envie sondas TCP para as sondas de integridade criadas na etapa 4 acima. Observe que isso é permitido por padrão.

SMB

Os endereços IP que você usa para dados SMB são alocados no balanceador de carga para que os endereços IP possam migrar para o outro nó caso ocorram eventos de failover.

Você precisará criar os seguintes endereços IP no balanceador de carga:

- Um endereço IP para acesso de LIF de dados nas a partir do nó 1
- Um endereço IP para acesso de LIF de dados nas a partir do nó 2
- Um endereço IP para um iSCSI LIF no nó 1 em cada VM respectivo NIC0
- Um endereço IP para um iSCSI LIF no nó 2

Os iSCSI LIFs são necessários para comunicação DNS e SMB. Um iSCSI LIF é usado para esse fim porque não migra no failover.

- Um endereço IP opcional para um LIF de gerenciamento de VM de storage (SVM)

Esse LIF de gerenciamento fornece uma conexão com ferramentas de gerenciamento como o SnapCenter.

Passos

1. No portal do Azure, abra o serviço **Load Balancers**.
2. Clique no nome do balanceador de carga do par de HA.
3. Crie o número necessário de configurações IP frontend apenas para os dados e LIFs SVM:



Um IP frontend só deve ser criado sob o NIC0 para cada SVM correspondente. Para obter mais informações sobre como adicionar o endereço IP ao SVM NIC0, consulte "Etapa 7 [hiperlink]"

- a. Em **Settings**, clique em **Frontend IP Configuration**.
- b. Clique em **Add**.
- c. Digite um nome para o IP frontend, selecione a sub-rede para o par de HA Cloud Volumes ONTAP, deixe **Dinâmico** selecionado e, em regiões com zonas de disponibilidade, deixe **zona redundante** selecionado para garantir que o endereço IP permaneça disponível se uma zona falhar.
- d. Clique em **Salvar**.

The screenshot shows the 'Add frontend IP configuration' page in the Microsoft Azure portal. The breadcrumb navigation is 'Home > Load balancing > azureha1011s3-rg-lb >'. The title is 'Add frontend IP configuration' with a three-dot menu icon. Below the title is the resource name 'azureha1011s3-rg-lb'. The form contains the following fields:

- Name ***: A text input field containing 'ip-for-svm2' with a checkmark icon on the right.
- Virtual network**: A dropdown menu showing 'Default-Networking-vnet'.
- Subnet ***: A dropdown menu showing 'default (172.19.2.0/24)' with a downward arrow icon.
- Assignment**: Two radio buttons, 'Dynamic' (which is selected) and 'Static'.
- Availability zone ***: A dropdown menu showing 'Zone-redundant' with a downward arrow icon and a help icon.

- e. Clique no nome da configuração IP frontend que você acabou de criar, altere **Assignment** para **Static** e clique em **Save**.

É melhor usar um endereço IP estático porque um IP estático garante que o endereço IP não mudará, o que pode ajudar a evitar interrupções desnecessárias para o seu aplicativo.

4. Adicione uma sonda de saúde para cada IP frontend que você acabou de criar.
 - a. Em **Settings** do balanceador de carga, clique em **Health probes**.
 - b. Clique em **Add**.
 - c. Introduza um nome para a sonda de saúde e introduza um número de porta entre 63005 e 65000. Mantenha os valores padrão para os outros campos.

É importante que o número da porta esteja entre 63005 e 65000. Por exemplo, se você estiver criando três sondas de saúde, poderá inserir sondas que usam os números de porta 63005, 63006 e 63007.

Microsoft Azure Search resources, services, and

Home > Load balancers > azureha1011s3-rg-lb >

Add health probe

azureha1011s3-rg-lb

Name *	<input type="text" value="svm2-health-probe1"/>	✓
Protocol *	<input type="text" value="TCP"/>	▼
Port * ⓘ	<input type="text" value="63005"/>	✓
Interval * ⓘ	<input type="text" value="5"/>	seconds
Unhealthy threshold * ⓘ	<input type="text" value="2"/>	consecutive failures
Used by ⓘ	Not used	

5. Crie novas regras de balanceamento de carga para cada IP frontend.
 - a. Em **Configurações** do balanceador de carga, clique em **regras de balanceamento de carga**.
 - b. Clique em **Add** e insira as informações necessárias:
 - **Nome:** Insira um nome para a regra.
 - **Versão IP:** Selecione **IPv4**.
 - **Frontend IP address:** Selecione um dos endereços IP frontend que você acabou de criar.
 - **Portas HA:** Ative esta opção.
 - **Pool de back-end:** Mantenha o pool de back-end padrão que já foi selecionado.
 - **Sonda de saúde:** Selecione a sonda de saúde que você criou para o IP frontend selecionado.
 - **Persistência da sessão:** Selecione **nenhum**.
 - **Floating IP:** Selecione **Enabled**.

Add load balancing rule

chandanaTcpRst3-rg-lb

i A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name *

jimmy_new_rule

IP Version *

IPv4 IPv6

Frontend IP address * ⓘ

10.1.0.156 (dataAFIP)

HA Ports ⓘ

Backend pool ⓘ

backendPool (2 virtual machines)

Health probe ⓘ

dataProbe (TCP:63002)

Session persistence ⓘ

None

Floating IP ⓘ

Disabled **Enabled**

6. Certifique-se de que as regras do grupo de segurança de rede para o Cloud Volumes ONTAP permitem que o balanceador de carga envie sondas TCP para as sondas de integridade criadas na etapa 4 acima. Observe que isso é permitido por padrão.
7. Para iSCSI LIFs, adicione o endereço IP para NIC0.
 - a. Clique no nome da VM Cloud Volumes ONTAP.
 - b. Clique em **Networking**.
 - c. Clique no nome da interface de rede para nic0.
 - d. Em Configurações, clique em **configurações IP**.
 - e. Clique em **Add**.

connector1-614 | IP configurations

Network interface

Search << **+ Add** Save Discard Refresh

Overview
Activity log
Access control (IAM)
Tags

Settings

IP configurations

DNS servers
Network security group
Properties
Locks

Monitoring
Insights
Alerts
Metrics

IP forwarding settings
IP forwarding: Disabled Enabled
Virtual network: Vnet2
IP configurations
Subnet *: Subnet2

Search IP configurations

Name	IP Version	Type	Private IP address	Public IP address
ipconfig1	IPv4	Primary	10.0.0.1 (Dynamic)	20.100.100.1 (connector1... ***)

f. Introduza um nome para a configuração IP, selecione Dinâmico e, em seguida, clique em **OK**.

connector1-614 | IP configurations

Network interface

Search << + Add Save Discard Refresh

Overview
Activity log
Access control (IAM)
Tags

Settings

IP configurations

DNS servers
Network security group
Properties
Locks

Monitoring
Insights
Alerts
Metrics

IP forwarding settings
IP forwarding: Disabled Enabled
Virtual network: Vnet2
IP configurations
Subnet *: Subnet2

Search IP configurations

Name	IP Version	Type	Private IP
ipconfig1	IPv4	Primary	10.0.0.1

Add IP configuration

connector1-614

Name *

IP version
 IPv4 IPv6

Type
 Primary Secondary

Primary IP configuration already exists

Private IP address settings
Allocation
 Dynamic Static

Public IP address
 Disassociate Associate

OK

g. Clique no nome da configuração IP que você acabou de criar, altere a atribuição para estática e clique em **Salvar**.



É melhor usar um endereço IP estático porque um IP estático garante que o endereço IP não mudará, o que pode ajudar a evitar interrupções desnecessárias para o seu aplicativo.

Depois de terminar

Copie os endereços IP privados que você acabou de criar. Você precisará especificar esses endereços IP ao criar LIFs para a nova VM de armazenamento.

Crie uma VM e LIFs de storage

Depois de alocar endereços IP no Azure, você pode criar uma nova VM de storage em um único sistema de nó ou em um par de HA.

Sistema de nó único

A forma como você cria uma VM de storage e LIFs em um sistema de nó único depende do protocolo de storage que você está usando.

ISCSI

Siga estas etapas para criar uma nova VM de armazenamento, juntamente com os LIFs necessários.

Passos

1. Crie a VM de armazenamento e uma rota para a VM de armazenamento.

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -vserver <svm-name> -destination 0.0.0.0/0  
-gateway <ip-of-gateway-server>
```

2. Criar um LIF de dados:

```
network interface create -vserver <svm-name> -home-port e0a -address  
<iscsi-ip-address> -netmask-length <# of mask bits> -lif <lif-name>  
-home-node <name-of-node1> -data-protocol iscsi
```

3. Opcional: Crie um LIF de gerenciamento de VM de storage.

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy system-defined -firewall-policy mgmt -home-port e0a  
-auto-revert false -failover-group Default
```

4. Atribua um ou mais agregados à VM de storage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Essa etapa é necessária porque a nova VM de storage precisa ter acesso a pelo menos um agregado antes de criar volumes na VM de storage.

NFS

Siga estas etapas para criar uma nova VM de armazenamento, juntamente com os LIFs necessários.

Passos

1. Crie a VM de armazenamento e uma rota para a VM de armazenamento.

```
vserver create -vserver <svm-name> -subtype default -rootvolume <root-volume-name> -rootvolume-security-style unix
```

```
network route create -vserver <svm-name> -destination 0.0.0.0/0 -gateway <ip-of-gateway-server>
```

2. Criar um LIF de dados:

```
network interface create -vserver <svm-name> -lif <lif-name> -service-policy default-data-files -address <nas-ip-address> -netmask-length <length> -home-node <name-of-node1> -status-admin up -failover-policy disabled -firewall-policy data -home-port e0a -auto-revert true -failover-group Default
```

3. Opcional: Crie um LIF de gerenciamento de VM de storage.

```
network interface create -vserver <svm-name> -lif <lif-name> -role data -data-protocol none -address <svm-mgmt-ip-address> -netmask-length <length> -home-node <name-of-node1> -status-admin up -failover-policy system-defined -firewall-policy mgmt -home-port e0a -auto-revert false -failover-group Default
```

4. Atribua um ou mais agregados à VM de storage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Essa etapa é necessária porque a nova VM de storage precisa ter acesso a pelo menos um agregado antes de criar volumes na VM de storage.

SMB

Siga estas etapas para criar uma nova VM de armazenamento, juntamente com os LIFs necessários.

Passos

1. Crie a VM de armazenamento e uma rota para a VM de armazenamento.

```
vserver create -vserver <svm-name> -subtype default -rootvolume <root-volume-name> -rootvolume-security-style unix
```

```
network route create -vserver <svm-name> -destination 0.0.0.0/0
-gateway <ip-of-gateway-server>
```

2. Criar um LIF de dados:

```
network interface create -vserver <svm-name> -lif <lif-name>
-service-policy default-data-files -address <nas-ip-address>
-netmask-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy disabled -firewall-policy data -home-port e0a -auto
-revert true -failover-group Default
```

3. Opcional: Crie um LIF de gerenciamento de VM de storage.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default
```

4. Atribua um ou mais agregados à VM de storage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Essa etapa é necessária porque a nova VM de storage precisa ter acesso a pelo menos um agregado antes de criar volumes na VM de storage.

Par de HA

A forma como você cria uma VM de storage e LIFs em um par de HA depende do protocolo de storage que você está usando.

ISCSI

Siga estas etapas para criar uma nova VM de armazenamento, juntamente com os LIFs necessários.

Passos

1. Crie a VM de armazenamento e uma rota para a VM de armazenamento.

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -vserver <svm-name> -destination 0.0.0.0/0  
-gateway <ip-of-gateway-server>
```

2. Crie LIFs de dados. Nesta etapa, você usa os IPs alocados no ["procedimento anterior"](#) para servir como LIFs de dados.

- a. Use o seguinte comando para criar um iSCSI LIF no nó 1.

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif  
<lif-name> -home-node <name-of-node1> -data-protocol iscsi
```

- b. Use o seguinte comando para criar um iSCSI LIF no nó 2.

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif  
<lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

3. Opcional: Crie um LIF de gerenciamento de VM de storage no nó 1.

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy system-defined -firewall-policy mgmt -home-port e0a  
-auto-revert false -failover-group Default
```

Esse LIF de gerenciamento fornece uma conexão com ferramentas de gerenciamento como o SnapCenter.

4. Atribua um ou mais agregados à VM de storage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Essa etapa é necessária porque a nova VM de storage precisa ter acesso a pelo menos um agregado antes de criar volumes na VM de storage.

5. Se você estiver executando o Cloud Volumes ONTAP 9.11.1 ou posterior, modifique as políticas de serviço de rede para a VM de storage.
 - a. Introduza o seguinte comando para aceder ao modo avançado.

```
::> set adv -con off
```

A modificação dos serviços é necessária porque garante que o Cloud Volumes ONTAP possa usar o iSCSI LIF para conexões de gerenciamento de saída.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client
```

Siga estas etapas para criar uma nova VM de armazenamento, juntamente com os LIFs necessários.

Passos

1. Crie a VM de armazenamento e uma rota para a VM de armazenamento.

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -vserver <svm-name> -destination 0.0.0.0/0  
-gateway <ip-of-gateway-server>
```

2. Crie LIFs de dados. Nesta etapa, você usa os IPs alocados no ["procedimento anterior"](#) para servir como LIFs de dados.

- a. Use o seguinte comando para criar um nas LIF no nó 1.

```
network interface create -vserver <svm-name> -lif <lif-name>  
-service-policy default-data-files -address <nfs-cifs-ip-address>  
-netmask-length <length> -home-node <name-of-node1> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe1>
```

- b. Use o seguinte comando para criar um nas LIF no nó 2.

```
network interface create -vserver <svm-name> -lif <lif-name>  
-service-policy default-data-files -address <nfs-cifs-ip-address>  
-netmask-length <length> -home-node <name-of-node2> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe2>
```

3. Crie iSCSI LIFs para fornecer comunicação DNS. Os iSCSI LIFs são necessários para a comunicação DNS mesmo quando o protocolo iSCSI não é usado.

- a. Use o seguinte comando para criar um iSCSI LIF no nó 1.

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif  
<lif-name> -home-node <name-of-node1> -data-protocol iscsi
```

- b. Use o seguinte comando para criar um iSCSI LIF no nó 2.

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

4. Opcional: Crie um LIF de gerenciamento de VM de storage no nó 1.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

Esse LIF de gerenciamento fornece uma conexão com ferramentas de gerenciamento como o SnapCenter.

5. Opcional: Crie um LIF de gerenciamento de VM de storage no nó 1.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

Esse LIF de gerenciamento fornece uma conexão com ferramentas de gerenciamento como o SnapCenter.

6. Atribua um ou mais agregados à VM de storage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Essa etapa é necessária porque a nova VM de storage precisa ter acesso a pelo menos um agregado antes de criar volumes na VM de storage.

7. Se você estiver executando o Cloud Volumes ONTAP 9.11.1 ou posterior, modifique as políticas de serviço de rede para a VM de storage.

a. Introduza o seguinte comando para aceder ao modo avançado.

```
::> set adv -con off
```

A modificação dos serviços é necessária porque garante que o Cloud Volumes ONTAP possa usar o iSCSI LIF para conexões de gerenciamento de saída.

```

network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client

```

SMB

Siga estas etapas para criar uma nova VM de armazenamento, juntamente com os LIFs necessários.

Passos

1. Crie a VM de armazenamento e uma rota para a VM de armazenamento.

```

vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix

```

```

network route create -vserver <svm-name> -destination 0.0.0.0/0
-gateway <ip-of-gateway-server>

```

2. Criar LIFs de dados nas. Nesta etapa, você usa os IPs alocados no "procedimento anterior" para servir como LIFs de dados.

a. Use o seguinte comando para criar um nas LIF no nó 1.

```
network interface create -vserver <svm-name> -lif <lif-name>
-service-policy default-data-files -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node1> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe1>
```

b. Use o seguinte comando para criar um nas LIF no nó 2.

```
network interface create -vserver <svm-name> -lif <lif-name>
-service-policy default-data-files -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node2> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe2>
```

3. Crie iSCSI LIFs para fornecer comunicação DNS. Os iSCSI LIFs são necessários para a comunicação DNS mesmo quando o protocolo iSCSI não é usado.

a. Use o seguinte comando para criar um iSCSI LIF no nó 1.

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node1> -data-protocol iscsi
```

b. Use o seguinte comando para criar um iSCSI LIF no nó 2.

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

4. Opcional: Crie um LIF de gerenciamento de VM de storage no nó 1.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

Esse LIF de gerenciamento fornece uma conexão com ferramentas de gerenciamento como o SnapCenter.

5. Atribua um ou mais agregados à VM de storage.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Essa etapa é necessária porque a nova VM de storage precisa ter acesso a pelo menos um agregado antes de criar volumes na VM de storage.

6. Se você estiver executando o Cloud Volumes ONTAP 9.11.1 ou posterior, modifique as políticas de serviço de rede para a VM de storage.

a. Introduza o seguinte comando para aceder ao modo avançado.

```
::> set adv -con off
```

A modificação dos serviços é necessária porque garante que o Cloud Volumes ONTAP possa usar o iSCSI LIF para conexões de gerenciamento de saída.

```

network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client

```

O que se segue?

Depois de criar uma VM de storage em um par de HA, é melhor esperar 12 horas antes de provisionar o storage nesse SVM. A partir da versão do Cloud Volumes ONTAP 9.10.1, o BlueXP verifica as configurações do balanceador de carga de um par de HA em um intervalo de 12 horas. Se houver novos SVMs, o BlueXP ativará uma configuração que forneça failover não planejado mais curto.

Crie VMs de storage de fornecimento de dados para o Cloud Volumes ONTAP no Google Cloud

Uma VM de armazenamento é uma máquina virtual em execução no ONTAP que fornece serviços de armazenamento e dados aos seus clientes. Você pode saber isso como um SVM ou um vserver. O Cloud Volumes ONTAP é configurado com uma VM de storage por padrão, mas algumas configurações oferecem suporte a VMs de storage

adicionais.

Número suportado de VMs de storage

Várias VMs de storage são compatíveis com configurações específicas do Cloud Volumes ONTAP no Google Cloud a partir da versão 9.11.1. Vá para ["Notas de versão do Cloud Volumes ONTAP"](#) a para verificar o número suportado de VMs de armazenamento para a sua versão do Cloud Volumes ONTAP.

Todas as outras configurações do Cloud Volumes ONTAP oferecem suporte a uma VM de storage de fornecimento de dados e a uma VM de storage de destino usada para recuperação de desastres. Você pode ativar a VM de storage de destino para acesso aos dados se houver uma interrupção na VM de storage de origem.

Crie uma VM de storage

Se houver suporte da sua licença, você poderá criar várias VMs de storage em um único sistema de nó ou em um par de HA. Observe que você deve usar a API do BlueXP para criar uma VM de storage em um par de HA. Além disso, use o Gerenciador de sistemas do ONTAP ou a CLI do ONTAP para criar uma VM de storage em um único sistema de nós.

Sistema de nó único

Essas etapas criam uma nova VM de storage em um único sistema de nó usando a CLI. Um endereço IP privado é necessário para criar um LIF de dados e outro endereço IP privado opcional é necessário se você quiser criar um LIF de gerenciamento.

Passos

1. No Google Cloud, vá para a instância do Cloud Volumes ONTAP e adicione um endereço IP ao nic0 para cada LIF.

Edit network interface ^

Network *
default ▼ ?

Subnetwork *
default IPv4 (10.138.0.0/20) ▼ ?

i To use IPv6, you need an IPv6 subnet range. [LEARN MORE](#)

IP stack type

IPv4 (single-stack)

IPv4 and IPv6 (dual-stack)

Primary internal IP
gpcvo-vm-ip-nic0-nodemgmt (10.138.0.46) ▼ ?

Alias IP ranges

<p>Subnet range 1 Primary (10.138.0.0/20) ▼</p>	<p>Alias IP range 1 * 10.138.0.25/32 ?</p>
<p>Subnet range 2 Primary (10.138.0.0/20) ▼</p>	<p>Alias IP range 2 * 10.138.0.23/32 ?</p>
<p>Subnet range 3 Primary (10.138.0.0/20) ▼</p>	<p>Alias IP range 3 * 10.138.0.21/32 ?</p>
<p>Subnet range 4 Primary (10.138.0.0/20) ▼</p>	<p>Alias IP range 4 * 10.138.0.31/32 ?</p>

+ ADD IP RANGE

External IPv4 address
None ▼ ?

Você precisa de um endereço IP para um LIF de dados e outro endereço IP opcional se quiser criar um LIF de gerenciamento na VM de armazenamento.

["Documentação do Google Cloud: Adicionando intervalos de IP de alias a uma instância existente"](#)

2. Crie a VM de armazenamento e uma rota para a VM de armazenamento.

```
vserver create -vserver <svm-name> -subtype default -rootvolume <root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name> -gateway <ip-of-gateway-server>
```

3. Crie um LIF de dados especificando o endereço IP que você adicionou no Google Cloud.

ISCSI

```
network interface create -vserver <svm-name> -home-port e0a -address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-nodel> -data -protocol iscsi
```

NFS ou SMB

```
network interface create -vserver <svm-name> -lif <lif-name> -role data -data-protocol cifs,nfs -address <nfs-ip-address> -netmask -length <length> -home-node <name-of-nodel> -status-admin up -failover-policy disabled -firewall-policy data -home-port e0a -auto -revert true -failover-group Default
```

4. Opcional: Crie um LIF de gerenciamento de VM de armazenamento especificando o endereço IP adicionado ao Google Cloud.

```
network interface create -vserver <svm-name> -lif <lif-name> -role data -data-protocol none -address <svm-mgmt-ip-address> -netmask-length <length> -home-node <name-of-nodel> -status-admin up -failover-policy system-defined -firewall-policy mgmt -home-port e0a -auto-revert false -failover-group Default
```

5. Atribua um ou mais agregados à VM de storage.

```
vserver add-aggregates -vserver <svm-name> -aggregates <aggr1,aggr2>
```

Essa etapa é necessária porque a nova VM de storage precisa ter acesso a pelo menos um agregado antes de criar volumes na VM de storage.

Par de HA

Você deve usar a API do BlueXP para criar uma VM de storage em um sistema Cloud Volumes ONTAP no Google Cloud. O uso da API (e não do Gerenciador de sistemas ONTAP ou da CLI ONTAP) é necessário porque o BlueXP configura a VM de storage com os serviços de LIF necessários, bem como um LIF iSCSI necessário para a comunicação SMB/CIFS de saída.

Observe que o BlueXP aloca os endereços IP necessários no Google Cloud e cria a VM de storage com um LIF de dados para acesso SMB/NFS e um LIF iSCSI para comunicação SMB de saída.

O BlueXP também modifica as `default-data-files` políticas nas VMs de armazenamento de dados removendo os seguintes serviços de LIFs de dados nas e adicionando-os a LIFs de dados iSCSI:

- data-fpolicy-client
- management-ad-client
- management-dns-client
- management-ldap-client
- management-nis-client

A modificação dos serviços é necessária porque garante que o Cloud Volumes ONTAP possa usar o iSCSI LIF para conexões de gerenciamento de saída.

Permissões do Google Cloud necessárias

O conector requer permissões específicas para criar e gerenciar VMs de storage para pares de HA do Cloud Volumes ONTAP. As permissões necessárias estão incluídas no ["As políticas fornecidas pela NetApp"](#).

Passos

1. Use a seguinte chamada de API para criar uma VM de armazenamento:

```
POST /occm/api/gcp/ha/working-environments/{WE_ID}/svm/
```

O organismo de solicitação deve incluir o seguinte:

```
{ "svmName": "myNewSvm1" }
```

Gerenciar VMs de storage em pares de HA

A API do BlueXP também é compatível com a renomeação e exclusão de VMs de storage em pares de HA.

Renomeie uma VM de armazenamento

Se necessário, você pode alterar o nome de uma VM de storage a qualquer momento.

Passos

1. Use a seguinte chamada de API para renomear uma VM de armazenamento:

```
PUT /occm/api/gcp/ha/working-environments/{WE_ID}/svm
```

O organismo de solicitação deve incluir o seguinte:

```
{
  "svmNewName": "newSvmName",
  "svmName": "oldSvmName"
}
```

Exclua uma VM de armazenamento

Se você não precisar mais de uma VM de storage, poderá excluí-la do Cloud Volumes ONTAP.

Passos

1. Use a seguinte chamada de API para excluir uma VM de armazenamento:

```
DELETE /occm/api/gcp/ha/working-environments/{WE_ID}/svm/{SVM_NAME}
```

Configurar a recuperação de desastres do SVM

O BlueXP não oferece qualquer configuração ou suporte de orquestração para recuperação de desastres de VM de storage (SVM). Use o Gerenciador de sistemas do ONTAP ou a CLI do ONTAP.

Se você configurar a replicação do SnapMirror SVM entre dois sistemas Cloud Volumes ONTAP, a replicação deve estar entre dois sistemas de par de HA ou dois sistemas de nó único. Não é possível configurar a replicação do SnapMirror SVM entre um par de HA e um sistema de nó único.

Consulte os seguintes documentos para obter as instruções da CLI do ONTAP.

- ["Guia expresso de preparação para recuperação de desastres da SVM"](#)
- ["Guia do SVM Disaster Recovery Express"](#)

Segurança e criptografia de dados

Criptografando volumes com soluções de criptografia NetApp

O Cloud Volumes ONTAP é compatível com criptografia de volume NetApp (NVE) e criptografia agregada NetApp (NAE). NVE e NAE são soluções baseadas em software que permitem a criptografia de volumes em repouso compatível com FIPS 140-2. ["Saiba mais sobre essas soluções de criptografia"](#).

Tanto o NVE quanto o NAE são compatíveis com um gerenciador de chaves externo.

```
] endif::aws[] ifdef::azure[] endif::azure[] ifdef::gcp[] endif::gcp[] ifdef::aws[] endif::aws[] ifdef::azure[]  
endif::azure[:gcp[
```

Gerencie chaves com o AWS Key Management Service

Você pode usar ["Serviço de gerenciamento de chaves \(KMS\) da AWS"](#) para proteger suas chaves de criptografia ONTAP em um aplicativo implantado pela AWS.

O gerenciamento de chaves com o AWS KMS pode ser habilitado com a CLI ou a API REST do ONTAP.

Ao usar o KMS, esteja ciente de que, por padrão, o LIF de um SVM de dados é usado para se comunicar com o endpoint de gerenciamento de chaves na nuvem. Uma rede de gerenciamento de nós é usada para se comunicar com os serviços de autenticação da AWS. Se a rede do cluster não estiver configurada corretamente, o cluster não utilizará adequadamente o serviço de gerenciamento de chaves.

Antes de começar

- O Cloud Volumes ONTAP deve estar executando a versão 9.12.0 ou posterior
- Tem de ter instalado a licença de encriptação de volume (VE) e.

- Você deve ter instalado a licença MTEKM (Multi-tenant Encryption Key Management) instalada.
- Você precisa ser um administrador de cluster ou SVM
- Você precisa ter uma assinatura da AWS ativa



Você só pode configurar chaves para um SVM de dados.

Configuração

AWS

1. Você deve criar uma **"concessão"** chave para o AWS KMS que será usada pela função de gerenciamento de criptografia do IAM. A função IAM deve incluir uma política que permita as seguintes operações:
 - DescribeKey
 - Encrypt
 - Decrypt Para criar uma subvenção, **"Documentação do AWS"** consulte .
2. **"Adicione uma política à função IAM apropriada."** A política deve suportar as DescribeKey operações , Encrypt, e Decrypt .

Cloud Volumes ONTAP

1. Mude para o seu ambiente Cloud Volumes ONTAP.
2. Mude para o nível de privilégio avançado:


```
set -privilege advanced
```
3. Habilite o gerenciador de chaves da AWS:


```
security key-manager external aws enable -vserver data_svm_name -region AWS_region -key-id key_ID -encryption-context encryption_context
```
4. Quando solicitado, insira a chave secreta.
5. Confirme se o AWS KMS foi configurado corretamente:


```
security key-manager external aws show -vserver svm_name
```

Gerencie chaves com o Azure Key Vault

Você pode usar **"Azure Key Vault (AKV)"** para proteger suas chaves de criptografia ONTAP em um aplicativo implantado no Azure.

O AKV pode ser usado para proteger **"Chaves de criptografia de volume NetApp (NVE)"** somente para SVMs de dados.

O gerenciamento de chaves com AKV pode ser habilitado com a CLI ou a API REST do ONTAP.

Ao usar o AKV, esteja ciente de que, por padrão, um data SVM LIF é usado para se comunicar com o endpoint de gerenciamento de chaves na nuvem. Uma rede de gerenciamento de nós é usada para se comunicar com os serviços de autenticação do provedor de nuvem (login.microsoftonline.com). Se a rede do cluster não estiver configurada corretamente, o cluster não utilizará adequadamente o serviço de gerenciamento de chaves.

Antes de começar

- O Cloud Volumes ONTAP deve estar executando a versão 9.10.1 ou posterior

- Licença de encriptação de volume (VE) instalada (a licença de encriptação de volume NetApp é instalada automaticamente em cada sistema Cloud Volumes ONTAP registado com o suporte NetApp)
- Você deve ter uma licença de gerenciamento de chave de criptografia de vários locatários (MT_EK_MGMT)
- Você precisa ser um administrador de cluster ou SVM
- Uma subscrição do ative Azure

Limitações

- O AKV só pode ser configurado em um SVM de dados
- Não pode ser usado usando AKV. O NAE requer um servidor KMIP com suporte externo.
- Os nós do Cloud Volumes ONTAP pesquisam o AKV a cada 15 minutos para confirmar a acessibilidade e a disponibilidade das chaves. Este período de polling não é configurável e, após quatro falhas consecutivas na tentativa de polling (totalizando 1 hora), os volumes são colocados offline.

Processo de configuração

As etapas descritas capturam como Registrar sua configuração do Cloud Volumes ONTAP com o Azure e como criar um Cofre e chaves do Azure. Se você já tiver concluído estas etapas, verifique se tem as configurações corretas, especialmente em [Crie um cofre de chave do Azure](#), em seguida, prossiga para [Configuração do Cloud Volumes ONTAP](#).

- [Registro de aplicativos do Azure](#)
- [Criar segredo de cliente Azure](#)
- [Crie um cofre de chave do Azure](#)
- [Criar chave de criptografia](#)
- [Criar um endpoint do Azure ative Directory \(somente HA\)](#)
- [Configuração do Cloud Volumes ONTAP](#)

Registro de aplicativos do Azure

1. Primeiro, você deve Registrar seu aplicativo na assinatura do Azure que deseja que o Cloud Volumes ONTAP use para acessar o Cofre de chaves do Azure. No portal do Azure, selecione **inscrições de aplicativos**.
2. Selecione **novo registro**.
3. Forneça um nome para o aplicativo e selecione um tipo de aplicativo compatível. O locatário único padrão é suficiente para o uso do Azure Key Vault. Selecione **Registrar**.
4. Na janela Visão geral do Azure, selecione o aplicativo que você registrou. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)** para um local seguro. Eles serão necessários mais tarde no processo de Registro.

Criar segredo de cliente Azure

1. No portal do Azure para o Registro do aplicativo Azure Key Vault, selecione o painel **certificados e segredos**.
2. Selecione **segredo de novo cliente**. Introduza um nome significativo para o segredo do cliente. A NetApp recomenda um período de expiração de 24 meses. No entanto, suas políticas específicas de governança de nuvem podem exigir uma configuração diferente.
3. Clique em **Adicionar** para criar o segredo do cliente. Copie a cadeia de caracteres secreta listada na coluna **value** e armazene-a em um local seguro para uso posterior no [Configuração do Cloud Volumes](#)

ONTAP. O valor secreto não será exibido novamente depois que você navegar para fora da página.

Crie um cofre de chave do Azure

1. Se você tiver um cofre de chaves do Azure existente, poderá conectá-lo à configuração do Cloud Volumes ONTAP; no entanto, você deve adaptar as políticas de acesso às configurações desse processo.
2. No portal do Azure, navegue até a seção **Key Vaults**.
3. Clique em **criar** e insira as informações necessárias, incluindo grupo de recursos, região e nível de preços. Além disso, insira o número de dias para manter os cofres excluídos e selecione **Ativar proteção de purga** no cofre de chaves.
4. Selecione **Avançar** para escolher uma política de acesso.
5. Selecione as seguintes opções:
 - a. Em **Configuração de acesso**, selecione a **Política de Acesso ao Vault**.
 - b. Em **Acesso a recursos**, selecione **criptografia de disco do Azure para criptografia de volume**.
6. Selecione **criar** para adicionar uma política de acesso.
7. Em **Configurar a partir de um modelo**, clique no menu suspenso e selecione o modelo **Key, Secret e Certificate Management**.
8. Escolha cada um dos menus suspensos de permissões (chave, segredo, certificado) e, em seguida, **Selecionar tudo** no topo da lista de menus para selecionar todas as permissões disponíveis. Você deve ter:
 - **Permissões de chave**: 20 selecionado
 - **Permissões secretas**: 8 selecionadas
 - **Permissões de certificado**: 16 selecionado

Create an access policy



- 1 Permissions
- 2 Principal
- 3 Application (optional)
- 4 Review + create

Configure from a template

Key, Secret, & Certificate Management

Key permissions

Key Management Operations

- Select all
- Get
- List
- Update
- Create
- Import
- Delete
- Recover
- Backup
- Restore

Cryptographic Operations

- Select all
- Decrypt
- Encrypt
- Unwrap Key
- Wrap Key
- Verify
- Sign

Privileged Key Operations

- Select all
- Purge
- Release

Rotation Policy Operations

- Select all
- Rotate
- Get Rotation Policy
- Set Rotation Policy

Secret permissions

Secret Management Operations

- Select all
- Get
- List
- Set
- Delete
- Recover
- Backup
- Restore

Privileged Secret Operations

- Select all
- Purge

Certificate permissions

Certificate Management Operations

- Select all
- Get
- List
- Update
- Create
- Import
- Delete
- Recover
- Backup
- Restore
- Manage Contacts
- Manage Certificate Authorities
- Get Certificate Authorities
- List Certificate Authorities
- Set Certificate Authorities
- Delete Certificate Authorities

Privileged Certificate Operations

- Select all
- Purge

Previous

Next

9. Clique em **Next** (seguinte) para selecionar o aplicativo registrado **principal** do Azure que você criou no [Registro de aplicativos do Azure](#). Selecione **seguinte**.



Apenas um principal pode ser atribuído por política.

Create an access policy

1 Permissions **2 Principal** 3 Application (optional) 4 Review + create

Only 1 principal can be assigned per access policy.
Use the new embedded experience to select a principal. The previous popup experience can be accessed here. [Select a principal](#)

Selected item

No item selected

Previous **Next**

10. Clique em **seguinte** duas vezes até chegar a **Revisão e criar**. Em seguida, clique em **criar**.
11. Selecione **Next** (seguinte) para avançar para as opções **Networking**.
12. Escolha o método de acesso à rede apropriado ou selecione **todas as redes** e **Revisão e criação** para criar o cofre de chaves. (O método de acesso à rede pode ser prescrito por uma política de governança ou pela equipe de segurança da nuvem corporativa.)
13. Gravar o URI do Key Vault: No cofre de chaves que você criou, navegue até o menu Visão geral e copie o URI ** do Vault da coluna direita. Você precisa disso para uma etapa posterior.

Criar chave de criptografia

1. No menu do cofre de chaves que você criou para o Cloud Volumes ONTAP, navegue até a opção **Keys**.
2. Selecione **Generate/import** (gerar/importar) para criar uma nova chave.
3. Deixe a opção padrão definida como **Generate**.
4. Forneça as seguintes informações:
 - Nome da chave de criptografia

- Tipo de chave: RSA
 - Tamanho da chave RSA: 2048
 - Ativado: Sim
5. Selecione **criar** para criar a chave de criptografia.
 6. Retorne ao menu **Keys** e selecione a tecla que você acabou de criar.
 7. Selecione o ID da chave em **versão atual** para ver as propriedades da chave.
 8. Localize o campo **Key Identifier**. Copie o URI até, mas não incluindo a cadeia hexadecimal.

Criar um endpoint do Azure active Directory (somente HA)

1. Esse processo só é necessário se você estiver configurando o Azure Key Vault para um ambiente de trabalho do HA Cloud Volumes ONTAP.
2. No portal do Azure, navegue até **redes virtuais**.
3. Selecione a rede virtual onde você implantou o ambiente de trabalho do Cloud Volumes ONTAP e selecione o menu **sub-redes** no lado esquerdo da página.
4. Selecione o nome da sub-rede para a implementação do Cloud Volumes ONTAP na lista.
5. Navegue até o título **Service Endpoints**. No menu pendente, selecione o seguinte:
 - **Microsoft.AzureActiveDirectory**
 - **Microsoft.KeyVault**
 - **Microsoft.Storage** (opcional)

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

3 selected

Service	Status	
Microsoft.Storage	Succeeded	
Microsoft.AzureActiveDirectory	Succeeded	
Microsoft.KeyVault	Succeeded	

Service endpoint policies

0 selected

SUBNET DELEGATION

Delegate subnet to a service ⓘ

None

NETWORK POLICY FOR PRIVATE ENDPOINTS

The network policy affects all private endpoints in this subnet. To use network security groups, application security groups, or user defined routes to control traffic going to a private endpoint, set the private endpoint network policy to enabled. [Learn more](#)

Private endpoint network policy

Disabled

Save **Cancel**

6. Selecione **Guardar** para captar as suas definições.

Configuração do Cloud Volumes ONTAP

1. Conecte-se ao LIF de gerenciamento de cluster com seu cliente SSH preferido.
2. Entre no modo de privilégio avançado no ONTAP:

```
set advanced -con off
```

3. Identifique os dados SVM desejados e verifique sua configuração de DNS:

```
vserver services name-service dns show
```

- a. Se existir uma entrada DNS para os dados desejados SVM e contiver uma entrada para o DNS do Azure, nenhuma ação será necessária. Caso contrário, adicione uma entrada de servidor DNS para o SVM de dados que aponte para o DNS do Azure, DNS privado ou servidor local. Isso deve corresponder à entrada do cluster admin SVM:

```
vserver services name-service dns create -vserver SVM_name -domains domain  
-name-servers IP_address
```

- b. Verifique se o serviço DNS foi criado para os dados SVM:

```
vserver services name-service dns show
```

4. Ative o Azure Key Vault usando o ID do cliente e o ID do locatário salvos após o Registro do aplicativo:

```
security key-manager external azure enable -vserver SVM_name -client-id  
Azure_client_ID -tenant-id Azure_tenant_ID -name key_vault_URI -key-id  
full_key_URI
```



O `_full_key_URI` valor deve utilizar o `<https:// <key vault host name>/keys/<key label>` formato.

5. Após a ativação bem-sucedida do Azure Key Vault, insira o `client secret value` quando solicitado.

6. Verifique o status do gerenciador de chaves:

```
security key-manager external azure check
```

A saída será semelhante a:

```
::*> security key-manager external azure check  
  
Vserver: data_svm_name  
Node: akvlab01-01  
  
Category: service_reachability  
Status: OK  
  
Category: ekvip_server  
Status: OK  
  
Category: kms_wrapped_key_status  
Status: UNKNOWN  
Details: No volumes created yet for the vserver. Wrapped KEK status  
will be available after creating encrypted volumes.  
  
3 entries were displayed.
```

Se o `service_reachability` status não for `OK`, o SVM não poderá alcançar o serviço Azure Key Vault com toda a conectividade e permissões necessárias. Certifique-se de que as políticas de rede e o roteamento do Azure não bloqueiem o vNet privado de alcançar o endpoint público do Azure KeyVault. Se o fizerem, considere usar um endpoint privado do Azure para acessar o Vault de chaves a partir do vNet. Você também pode precisar adicionar uma entrada de hosts estáticos no SVM para resolver o endereço

IP privado do endpoint.

O `kms_wrapped_key_status` irá comunicar UNKNOWN na configuração inicial. Seu status mudará para OK depois que o primeiro volume for criptografado.

7. Opcional: Crie um volume de teste para verificar a funcionalidade do NVE.

```
vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size  
-state online -policy default
```

Se configurado corretamente, o Cloud Volumes ONTAP criará automaticamente o volume e ativará a criptografia de volume.

8. Confirme se o volume foi criado e criptografado corretamente. Se for, o `-is-encrypted` parâmetro será exibido como `true`.

```
vol show -vserver SVM_name -fields is-encrypted
```

Gerencie chaves com o Cloud Key Management Service do Google

Você pode usar "[Serviço de gerenciamento de chaves do Google Cloud Platform \(Cloud KMS\)](#)" para proteger suas chaves de criptografia do ONTAP em um aplicativo implantado no Google Cloud Platform.

O gerenciamento de chaves com o Cloud KMS pode ser habilitado com a CLI da ONTAP ou a API REST do ONTAP.

Ao usar o Cloud KMS, esteja ciente de que, por padrão, o LIF de um SVM de dados é usado para se comunicar com o endpoint de gerenciamento de chaves na nuvem. Uma rede de gerenciamento de nós é usada para se comunicar com os serviços de autenticação do provedor de nuvem (`oauth2.googleapis.com`). Se a rede do cluster não estiver configurada corretamente, o cluster não utilizará adequadamente o serviço de gerenciamento de chaves.

Antes de começar

- O Cloud Volumes ONTAP deve estar executando a versão 9.10.1 ou posterior
- Licença de encriptação de volume (VE) instalada
- Licença MTEKM (gerenciamento de chave de criptografia multi-tenente) instalada, começando com o Cloud Volumes ONTAP 9.12.1 GA.
- Você precisa ser um administrador de cluster ou SVM
- Uma assinatura ativa do Google Cloud Platform

Limitações

- O Cloud KMS só pode ser configurado em um data SVM

Configuração

Google Cloud

1. No ambiente do Google Cloud "[Crie um anel e chave simétricos do GCP](#)", .
2. Crie uma função personalizada para sua conta de serviço do Cloud Volumes ONTAP.

```

gcloud iam roles create kmsCustomRole
  --project=<project_id>
  --title=<kms_custom_role_name>
  --description=<custom_role_description>

--permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersions.
list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.
useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.loca
tions.get,cloudkms.locations.list,resourceManager.projects.get
  --stage=GA

```

3. Atribua a função personalizada à chave KMS da nuvem e à conta de serviço Cloud Volumes ONTAP:

```

gcloud kms keys add-iam-policy-binding key_name --keyring key_ring_name
--location key_location --member serviceAccount:_service_account_Name_ --role
projects/customer_project_id/roles/kmsCustomRole

```

4. Transferir a chave JSON da conta de serviço:

```

gcloud iam service-accounts keys create key-file --iam-account=sa-name
@project-id.iam.gserviceaccount.com

```

Cloud Volumes ONTAP

1. Conecte-se ao LIF de gerenciamento de cluster com seu cliente SSH preferido.

2. Mude para o nível de privilégio avançado:

```
set -privilege advanced
```

3. Criar um DNS para o SVM de dados.

```
dns create -domains c.<project>.internal -name-servers server_address -vserver
SVM_name
```

4. Criar entrada CMEK:

```
security key-manager external gcp enable -vserver SVM_name -project-id project
-key-ring-name key_ring_name -key-ring-location key_ring_location -key-name
key_name
```

5. Quando solicitado, insira a chave JSON da conta de serviço na sua conta do GCP.

6. Confirme se o processo ativado foi bem-sucedido:

```
security key-manager external gcp check -vserver svm_name
```

7. OPCIONAL: Crie um volume para testar a criptografia `vol create volume_name -aggregate aggregate -vserver vserver_name -size 10G`

Solucionar problemas

Se você precisar solucionar problemas, você pode desativar os logs da API REST em bruto nas duas etapas finais acima:

1. `set d`

2. `systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2_client.log`

Aumento da proteção contra ransomware

Os ataques de ransomware podem custar tempo, recursos e reputação aos negócios. O BlueXP permite que você implemente duas soluções NetApp para ransomware: Proteção contra extensões comuns de arquivos de ransomware e proteção Autônoma contra ransomware (ARP). Essas soluções fornecem ferramentas eficazes para visibilidade, detecção e correção.

Proteção contra extensões comuns de arquivos ransomware

Disponível através do BlueXP, a configuração proteção contra ransomware permite que você utilize a funcionalidade ONTAP FPolicy para proteger contra tipos comuns de extensão de arquivo ransomware.

Passos

1. Na página Canvas, clique duas vezes no nome do sistema que você configura para proteção contra ransomware.
2. Na guia Visão geral, clique no painel recursos e, em seguida, clique no ícone de lápis ao lado de **proteção contra ransomware**.

Information	Features
Working Environment Tags	Tags 
Scheduled Downtime	Off 
S3 Storage Classes	Standard-Infrequent Access 
Instance Type	m5.xlarge 
Write Speed	Normal 
Ransomware Protection	Off 
Support Registration	Not Registered 
CIFs Setup	

3. Implemente a solução NetApp para ransomware:

- a. Clique em **Ativar política de instantâneo**, se tiver volumes que não tenham uma política de

instantâneo ativada.

A tecnologia NetApp Snapshot oferece a melhor solução do setor para correção de ransomware. A chave para uma recuperação bem-sucedida é restaurar a partir de backups não infectados. As cópias snapshot são somente leitura, o que impede a corrupção de ransomware. Eles também podem fornecer a granularidade para criar imagens de uma única cópia de arquivo ou uma solução completa de recuperação de desastres.

- b. Clique em **Ativar FPolicy** para ativar a solução FPolicy do ONTAP, que pode bloquear operações de arquivo com base na extensão de um arquivo.

Essa solução preventiva melhora a proteção contra ataques de ransomware bloqueando tipos comuns de arquivos de ransomware.

O escopo padrão do FPolicy bloqueia arquivos que têm as seguintes extensões:

Micro, criptografado, bloqueado, cripto, cripta, crinf, r5a, XRNT, XTBL, R16M01D05, pzdc, bom, LOL!, OMG!, RDM, RRK, cryptedRS, crjoker, EnCiPhErEd, LeChiffre



O BlueXP cria esse escopo quando você ativa o FPolicy no Cloud Volumes ONTAP. A lista é baseada em tipos de arquivos de ransomware comuns. Você pode personalizar as extensões de arquivo bloqueadas usando os comandos `vserver fpolicy scope` da CLI do Cloud Volumes ONTAP.

Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

- 1 Enable Snapshot Copy Protection**
50 % Protection
1 Volumes without a Snapshot Policy
To protect your data, activate the default Snapshot policy for these volumes
[Activate Snapshot Policy](#)
- 2 Block Ransomware File Extensions**
ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.
[View Denied File Names](#)
[Activate FPolicy](#)

Proteção autônoma contra ransomware

O Cloud Volumes ONTAP oferece suporte ao recurso de proteção Autônoma contra ransomware (ARP), que executa análises de workloads para detectar e avisar proativamente sobre atividades anormais que podem indicar um ataque de ransomware.

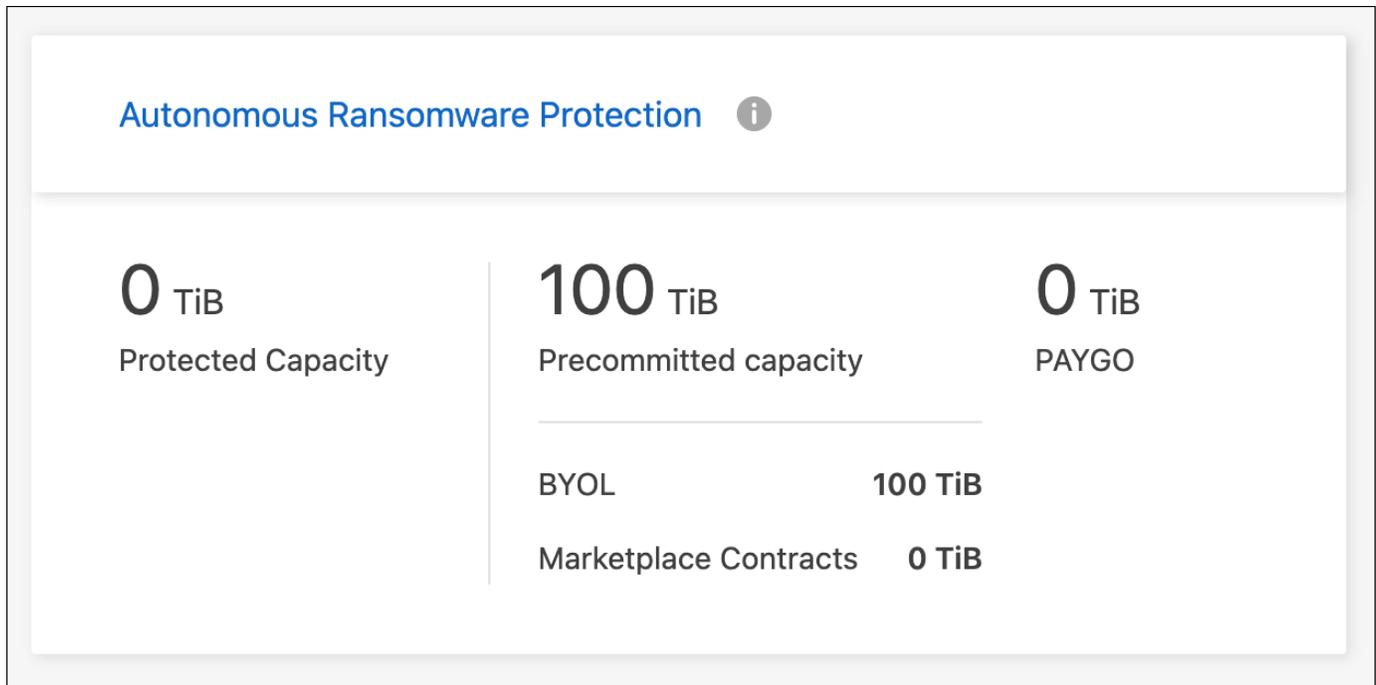
Separado das proteções de extensão de arquivo fornecidas pelo "configuração de proteção contra ransomware", o recurso ARP usa análise de carga de trabalho para alertar o usuário sobre possíveis ataques com base na "atividade anormal" detetada. Tanto a configuração de proteção contra ransomware quanto o recurso ARP podem ser usados em conjunto para uma proteção abrangente contra ransomware.

O recurso ARP está disponível para uso com as assinaturas bring Your own license (BYOL) e marketplace para suas licenças sem custo adicional.

Os volumes habilitados para ARP têm um estado designado de "modo de aprendizagem" ou "Ativo".

A configuração do ARP para volumes é realizada por meio do Gerenciador do sistema ONTAP e da CLI do ONTAP.

Para obter mais informações sobre como ativar o ARP com o Gerenciador de sistemas ONTAP e a CLI do ONTAP, "[Ative a proteção Autonomous ransomware](#)" consulte .



Crie cópias de Snapshot à prova de violações para storage WORM

Você pode criar cópias Snapshot à prova de violações de arquivos WORM (uma gravação, muitas leituras) em um sistema Cloud Volumes ONTAP e reter os snapshots em forma não modificada por um período de retenção específico. Esse recurso é baseado na tecnologia SnapLock e fornece uma camada adicional de proteção e conformidade de dados.

Antes de começar

Certifique-se de que o volume usado para criar cópias Snapshot seja um volume SnapLock. Para obter informações sobre como ativar a proteção SnapLock em volumes, "[Configurar o SnapLock](#)" consulte .

Passos

1. Criar cópias Snapshot a partir do volume SnapLock. Para obter informações sobre como criar cópias Snapshot usando a CLI ou o System Manager, "[Visão geral do gerenciamento de cópias Snapshot locais](#)" consulte .

As cópias Snapshot herdam as propriedades WORM do volume, o que as torna à prova de violações. A tecnologia SnapLock subjacente garante que um snapshot permaneça protegido de edição e exclusão até que o período de retenção especificado tenha decorrido.

2. Você pode modificar o período de retenção se houver a necessidade de editar esses snapshots. Para obter informações, "[Defina o tempo de retenção](#)" consulte .



Embora uma cópia Snapshot seja protegida por um período de retenção específico, o volume de origem pode ser excluído por um administrador de cluster, já que o storage WORM no Cloud Volumes ONTAP opera em um modelo de "administrador de storage confiável". Além disso, um administrador de nuvem confiável pode excluir os dados WORM operando nos recursos de storage de nuvem.

Administração do sistema

Atualize o software Cloud Volumes ONTAP

Atualize o Cloud Volumes ONTAP do BlueXP para ter acesso aos novos recursos e aprimoramentos mais recentes. Você deve preparar os sistemas Cloud Volumes ONTAP antes de atualizar o software.

Visão geral da atualização

Você deve estar ciente do seguinte antes de iniciar o processo de atualização do Cloud Volumes ONTAP.

Atualizar apenas a partir do BlueXP

As atualizações do Cloud Volumes ONTAP devem ser concluídas a partir do BlueXP. Você não deve atualizar o Cloud Volumes ONTAP usando o Gerenciador de sistema do ONTAP ou a CLI do ONTAP. Isso pode afetar a estabilidade do sistema.

Como atualizar

O BlueXP oferece duas maneiras de atualizar o Cloud Volumes ONTAP:

- Seguindo as notificações de atualização que aparecem no ambiente de trabalho
- Colocando a imagem de atualização em um local HTTPS e, em seguida, fornecendo ao BlueXP o URL

Caminhos de atualização suportados

A versão do Cloud Volumes ONTAP para a qual você pode atualizar depende da versão do Cloud Volumes ONTAP que você está executando atualmente.

Versão atual	Versões para as quais você pode atualizar diretamente
9.15.0	9.15.1
9.14.1	9.15.1
	9.15.0
9.14.0	9.14.1
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1

Versão atual	Versões para as quais você pode atualizar diretamente
9.12.1	9.13.1
	9.13.0
9.12.0	9.12.1
9.11.1	9.12.1
	9.12.0
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9,8	9.9.1
9,7	9,8
9,6	9,7
9,5	9,6
9,4	9,5
9,3	9,4
9,2	9,3
9,1	9,2
9,0	9,1
8,3	9,0

Observe o seguinte:

- Os caminhos de atualização compatíveis para o Cloud Volumes ONTAP são diferentes dos de um cluster ONTAP no local.
- Se você atualizar seguindo as notificações de atualização que aparecem em um ambiente de trabalho, o BlueXP solicitará que você atualize para uma versão que siga esses caminhos de atualização suportados.
- Se você atualizar colocando uma imagem de atualização em um local HTTPS, siga estes caminhos de atualização suportados.
- Em alguns casos, você pode precisar atualizar algumas vezes para alcançar seu lançamento alvo.

Por exemplo, se você estiver executando a versão 9,8 e quiser atualizar para a versão 9.10.1, primeiro você precisa atualizar para a versão 9.9.1 e depois para a versão 9.10.1.

Lançamentos de patches

A partir de janeiro de 2024, as atualizações de patch só estão disponíveis no BlueXP se forem uma versão de patch para as três versões mais recentes do Cloud Volumes ONTAP. Usamos a versão mais recente do GA para determinar as três versões mais recentes a serem exibidas no BlueXP. Por exemplo, se a versão atual do GA for 9.13.1, os patches para 9.11.1-9.13.1 aparecem no BlueXP. Se você quiser atualizar para uma versão de patch para as versões 9.11.1 ou abaixo, você precisará usar o procedimento de atualização manual pelo [Transferir a imagem ONTAP](#).

Como regra geral para versões de patch (P), você pode atualizar de uma versão para qualquer versão P da versão atual ou da próxima versão.

Aqui estão alguns exemplos:

- 9.13.0 > 9.13.1P15
- 9.12.1 > 9.13.1P2

Revertendo ou downgrade

Reverter ou baixar Cloud Volumes ONTAP para uma versão anterior não é suportado.

Registro de suporte

O Cloud Volumes ONTAP deve ser registrado no suporte da NetApp para atualizar o software usando qualquer um dos métodos descritos nesta página. Isso se aplica tanto ao pagamento conforme o uso (PAYGO) quanto ao uso (BYOL). Você precisará "[Registrar manualmente os sistemas PAYGO](#)", enquanto os sistemas BYOL são registrados por padrão.



Um sistema que não está registrado para suporte ainda receberá as notificações de atualização de software que aparecem no BlueXP quando uma nova versão estiver disponível. Mas você precisará Registrar o sistema antes que você possa atualizar o software.

Atualizações do mediador de HA

O BlueXP também atualiza a instância do mediador conforme necessário durante o processo de atualização do Cloud Volumes ONTAP.

Atualizações na AWS com tipos de instância C4, M4 e R4 EC2

O Cloud Volumes ONTAP não suporta mais os tipos de instância C4, M4 e R4 EC2. Você pode atualizar implantações existentes para o Cloud Volumes ONTAP versões 9,8-9.12.1 com esses tipos de instância. Antes de atualizar, recomendamos que você [altere o tipo de instância](#). Se você não puder alterar o tipo de instância, você precisará [ativar rede melhorada](#) antes de atualizar. Leia as seções a seguir para saber mais sobre como alterar o tipo de instância e ativar redes aprimoradas.

No Cloud Volumes ONTAP executando as versões 9.13.0 e superiores, você não pode atualizar com os tipos de instância C4, M4 e R4 EC2. Nesse caso, você precisa reduzir o número de discos e, em seguida [altere o tipo de instância](#), implantar uma nova configuração de par de HA com os tipos de instância C5, M5 e R5 EC2 e migrar os dados.

Altere o tipo de instância

Os tipos de instância C4, M4 e R4 EC2 permitem mais discos por nó do que os tipos de instância C5, M5 e R5 EC2. Se a contagem de disco por nó para a instância C4, M4 ou R4 EC2 que você está executando estiver

abaixo da permissão máxima de disco por nó para instâncias C5, M5 e R5, você poderá alterar o tipo de instância EC2 para C5, M5 ou R5.

["Verifique os limites de disco e disposição em camadas pela instância do EC2" "Altere o tipo de instância EC2 para Cloud Volumes ONTAP"](#)

Se não for possível alterar o tipo de instância, siga as etapas em [Ativar rede melhorada](#).

Ativar rede melhorada

Para atualizar para o Cloud Volumes ONTAP versões 9,8 e posteriores, você deve ativar *Enhanced Networking* no cluster que executa o tipo de instância C4, M4 ou R4. Para ativar o ENA, consulte o artigo da base de dados de Conhecimento ["Como habilitar redes avançadas como SR-IOV ou ENA em instâncias do AWS Cloud Volumes ONTAP"](#).

Prepare-se para atualizar

Antes de realizar uma atualização, você deve verificar se seus sistemas estão prontos e fazer as alterações necessárias na configuração.

- [Planeje o tempo de inatividade](#)
- [Verifique se a giveback automática ainda está ativada](#)
- [Suspender transferências SnapMirror](#)
- [Verifique se os agregados estão online](#)
- [Verifique se todos os LIFs estão em portas residenciais](#)

Planeje o tempo de inatividade

Quando você atualiza um sistema de nó único, o processo de atualização leva o sistema off-line por até 25 minutos, durante os quais a e/S é interrompida.

Em muitos casos, a atualização de um par de HA não causa interrupções e e/S é ininterrupta. Durante esse processo de atualização sem interrupções, cada nó é atualizado em conjunto para continuar fornecendo e/S aos clientes.

Protocolos orientados para sessões podem causar efeitos adversos em clientes e aplicações em determinadas áreas durante as atualizações. Para mais detalhes, ["Consulte a documentação do ONTAP"](#)

Verifique se a giveback automática ainda está ativada

A giveback automática deve estar ativada num par de HA Cloud Volumes ONTAP (esta é a predefinição). Se não for, então a operação falhará.

["Documentação do ONTAP 9: Comandos para configurar o giveback automático"](#)

Suspender transferências SnapMirror

Se um sistema Cloud Volumes ONTAP tiver relações SnapMirror ativas, é melhor suspender transferências antes de atualizar o software Cloud Volumes ONTAP. Suspender as transferências impede falhas no SnapMirror. Tem de suspender as transferências a partir do sistema de destino.



Embora o backup e a recuperação do BlueXP usem uma implementação do SnapMirror para criar arquivos de backup (chamados de nuvem SnapMirror), os backups não precisam ser suspensos quando um sistema é atualizado.

Sobre esta tarefa

Estas etapas descrevem como usar o Gerenciador de sistema do ONTAP para a versão 9,3 e posterior.

Passos

1. Inicie sessão no System Manager a partir do sistema de destino.

Você pode fazer login no System Manager apontando seu navegador da Web para o endereço IP do LIF de gerenciamento de cluster. Você pode encontrar o endereço IP no ambiente de trabalho do Cloud Volumes ONTAP.



O computador a partir do qual você está acessando o BlueXP deve ter uma conexão de rede com o Cloud Volumes ONTAP. Por exemplo, talvez seja necessário fazer login no BlueXP a partir de um host de salto que esteja na rede do provedor de nuvem.

2. Clique em **proteção > relacionamentos**.
3. Selecione a relação e clique em **operações > quiesce**.

Verifique se os agregados estão online

Os agregados para Cloud Volumes ONTAP devem estar online antes de atualizar o software. Os agregados devem estar online na maioria das configurações, mas se não estiverem, você deve colocá-los online.

Sobre esta tarefa

Estas etapas descrevem como usar o Gerenciador de sistema do ONTAP para a versão 9,3 e posterior.

Passos

1. No ambiente de trabalho, clique na guia **agregados**.
2. No título agregado, clique no botão elipses e selecione **Exibir detalhes do agregado**.

Aggregate Details	
aggr1	
Overview	Capacity Allocation
Provider Properties	
State	online
Home Node	[redacted]
Encryption Type	cloudEncrypted
Volumes	2 ▼

3. Se o agregado estiver offline, use o System Manager para colocar o agregado on-line:
 - a. Clique em **armazenamento > agregados e discos > agregados**.
 - b. Selecione o agregado e clique em **mais ações > Status > Online**.

Verifique se todos os LIFs estão em portas residenciais

Antes de atualizar, todos os LIFs devem estar em portas domésticas. Consulte a documentação do ONTAP para "[Verifique se todos os LIFs estão em portas residenciais](#)".

Se ocorrer um erro de falha de atualização, consulte o "[artigo da base de dados de conhecimento "Falha na atualização do Cloud Volumes ONTAP"](#)".

Atualize o Cloud Volumes ONTAP

O BlueXP notifica você quando uma nova versão está disponível para atualização. Você pode iniciar o processo de atualização a partir desta notificação. Para obter mais informações, [Atualize a partir de notificações BlueXP](#) consulte .

Outra maneira de realizar atualizações de software usando uma imagem em um URL externo. Esta opção é útil se o BlueXP não puder acessar o bucket do S3 para atualizar o software ou se você tiver fornecido um patch. Para obter mais informações, [Atualize a partir de uma imagem disponível em um URL](#) consulte .

Atualize a partir de notificações BlueXP

O BlueXP exibe uma notificação em ambientes de trabalho do Cloud Volumes ONTAP quando uma nova versão do Cloud Volumes ONTAP está disponível:



Antes de poder atualizar o Cloud Volumes ONTAP através da notificação do BlueXP , tem de ter uma conta no site de suporte da NetApp.

Você pode iniciar o processo de atualização a partir desta notificação, que automatiza o processo, obtendo a imagem de software de um bucket do S3, instalando a imagem e reiniciando o sistema.

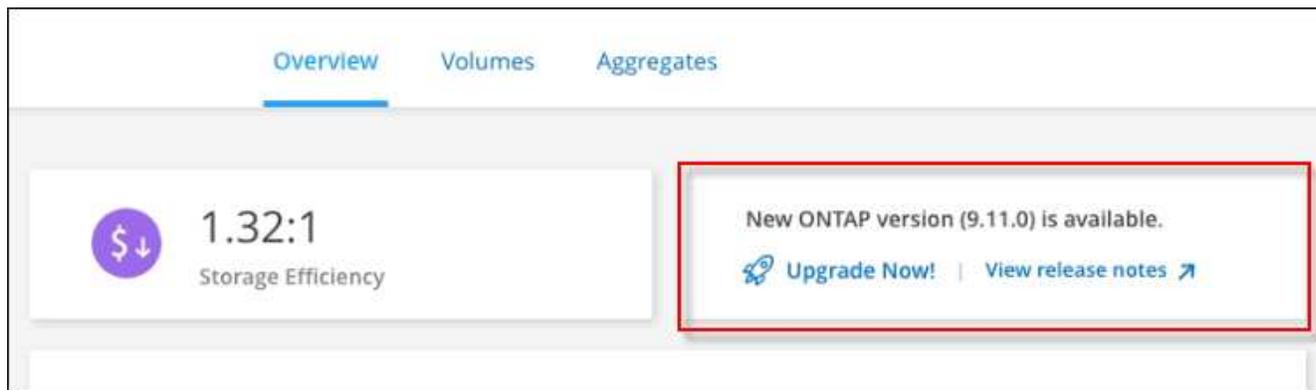
Antes de começar

Operações do BlueXP , como criação de volume ou agregado, não devem estar em andamento no sistema Cloud Volumes ONTAP.

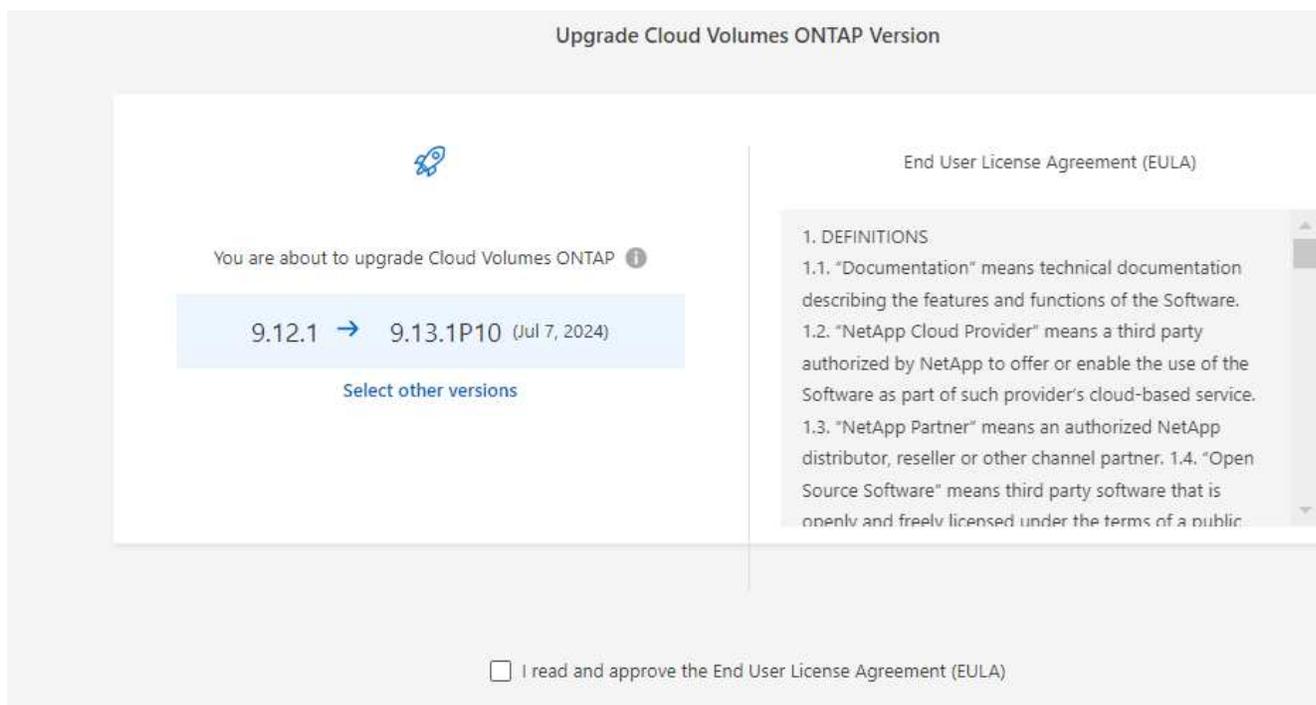
Passos

1. No menu de navegação à esquerda, selecione **Storage > Canvas**.
2. Selecione um ambiente de trabalho.

Uma notificação será exibida na guia Visão geral se uma nova versão estiver disponível:



3. Se você quiser atualizar a versão instalada do Cloud Volumes ONTAP, clique em **Atualizar agora!** Por padrão, você vê a versão mais recente e compatível para atualização.



Se quiser atualizar para outra versão, clique em **Selecionar outras versões**. Você vê as versões mais recentes do Cloud Volumes ONTAP listadas que também são compatíveis com a versão instalada em seu sistema. Por exemplo, a versão instalada no seu sistema é 9.12.1P3 e as seguintes versões compatíveis estão disponíveis:

- 9.12.1P4 a 9.12.1P14
- 9.13.1 e 9.13.1P1 você vê 9.13.1P1 como a versão padrão para atualização, e 9.12.1P13, 9.13.1P14, 9.13.1 e 9.13.1P1 como as outras versões disponíveis.

4. Opcionalmente, você pode clicar em **todas as versões** para inserir outra versão para a qual deseja atualizar (digamos, o próximo patch da versão instalada). Para obter um caminho de atualização compatível da versão atual do Cloud Volumes ONTAP, "[Caminhos de atualização suportados](#)" consulte .

5. Clique em **Salvar** e, em seguida, em **aplicar**.

Select the ONTAP version you want to upgrade to:

Version	Date
<input type="radio"/> 9.12.1P14	Aug 22, 2024
<input type="radio"/> 9.12.1P13	Jul 7, 2024
<input type="radio"/> 9.13.1P10	Jul 7, 2024
<input type="radio"/> 9.13.1P9	May 9, 2024

All versions ^

Write the version you want to upgrade to:

Save Cancel

Apply Cancel

6. Na página Atualizar Cloud Volumes ONTAP, leia o EULA e, em seguida, selecione **Eu li e aprovo o EULA**.
7. Clique em **Upgrade**.
8. Para verificar o status da atualização, clique no ícone Configurações e selecione **linha do tempo**.

Resultado

O BlueXP inicia a atualização de software. Pode executar ações no ambiente de trabalho quando a atualização de software estiver concluída.

Depois de terminar

Se você suspendeu as transferências do SnapMirror, use o Gerenciador do sistema para retomar as transferências.

Atualize a partir de uma imagem disponível em um URL

Você pode colocar a imagem do software Cloud Volumes ONTAP no conector ou em um servidor HTTP e, em seguida, iniciar a atualização do software a partir do BlueXP. Você pode usar essa opção se o BlueXP não puder acessar o bucket do S3 para atualizar o software.

Antes de começar

- Operações do BlueXP , como criação de volume ou agregado, não devem estar em andamento no sistema Cloud Volumes ONTAP.
- Se você usar HTTPS para hospedar imagens do ONTAP, a atualização pode falhar devido a problemas de autenticação SSL, causados por certificados ausentes. A solução alternativa é gerar e instalar um certificado assinado pela CA para ser usado para autenticação entre o ONTAP e o BlueXP .

Vá para a base de dados de Conhecimento da NetApp para ver instruções passo a passo:

["KB do NetApp: Como configurar o BlueXP como um servidor HTTPS para hospedar imagens de atualização"](#)

Passos

1. Opcional: Configure um servidor HTTP que possa hospedar a imagem do software Cloud Volumes ONTAP.

Se você tiver uma conexão VPN com a rede virtual, poderá colocar a imagem do software Cloud Volumes ONTAP em um servidor HTTP em sua própria rede. Caso contrário, você deve colocar o arquivo em um servidor HTTP na nuvem.

2. Se você usar seu próprio grupo de segurança para o Cloud Volumes ONTAP, verifique se as regras de saída permitem conexões HTTP para que o Cloud Volumes ONTAP possa acessar a imagem do software.



O grupo de segurança Cloud Volumes ONTAP predefinido permite ligações HTTP de saída por predefinição.

3. Obtenha a imagem do software em "[O site de suporte da NetApp](#)".
4. Copie a imagem do software para um diretório no conetor ou em um servidor HTTP do qual o arquivo será servido.

Dois caminhos estão disponíveis. O caminho correto depende da versão do conetor.

- `/opt/application/netapp/cloudmanager/docker_occm/data/ontap/images/`
- `/opt/application/netapp/cloudmanager/ontap/images/`

5. A partir do ambiente de trabalho no BlueXP , clique no botão ... (**Ícone de elipses**) e, em seguida, clique em **Atualizar Cloud Volumes ONTAP**.
6. Na página Atualizar versão do Cloud Volumes ONTAP, digite o URL e clique em **alterar imagem**.

Se você copiou a imagem do software para o conetor no caminho mostrado acima, digite o seguinte URL:

`Http://<Connector-private-IP-address>/ONTAP/Images/<image-file-name>`



No URL, **image-file-name** deve seguir o formato "COT.image.9.13.1P2.tgz".

7. Clique em **Proceed** para confirmar.

Resultado

O BlueXP inicia a atualização de software. Você pode executar ações no ambiente de trabalho assim que a atualização de software estiver concluída.

Depois de terminar

Se você suspendeu as transferências do SnapMirror, use o Gerenciador do sistema para retomar as transferências.

Corrigir falhas de download ao usar um gateway NAT do Google Cloud

O conector transfere automaticamente atualizações de software para o Cloud Volumes ONTAP. O download pode falhar se a configuração usar um gateway NAT do Google Cloud. Você pode corrigir esse problema limitando o número de partes nas quais a imagem do software está dividida. Esta etapa deve ser concluída usando a API do BlueXP .

Passo

1. Envie uma SOLICITAÇÃO PUT para `/occm/config` com o seguinte JSON como corpo:

```
{
  "maxDownloadSessions": 32
}
```

O valor para `maxDownloadSessions` pode ser 1 ou qualquer número inteiro maior que 1. Se o valor for 1, a imagem transferida não será dividida.

Note que 32 é um valor de exemplo. O valor que você deve usar depende da configuração NAT e do número de sessões que você pode ter simultaneamente.

["Saiba mais sobre a chamada API /occm/config"](#).

Registrar sistemas de pagamento conforme o uso

O suporte da NetApp está incluído nos sistemas Cloud Volumes ONTAP pay-as-you-go (PAYGO), mas você deve primeiro ativar o suporte registrando os sistemas no NetApp.

O Registro de um sistema PAYGO com o NetApp é necessário para atualizar o software ONTAP usando qualquer um dos métodos ["descrito nesta página"](#).



Um sistema que não está registrado para suporte ainda receberá as notificações de atualização de software que aparecem no BlueXP quando uma nova versão estiver disponível. Mas você precisará Registrar o sistema antes que você possa atualizar o software.

Passos

1. Se você ainda não adicionou sua conta do site de suporte da NetApp ao BlueXP , acesse **Configurações da conta** e adicione-a agora.

["Saiba como adicionar contas do site de suporte da NetApp"](#).

2. Na página Canvas, clique duas vezes no nome do sistema que você deseja Registrar.
3. Na guia Visão geral, clique no painel recursos e, em seguida, clique no ícone de lápis ao lado de **Registro de suporte**.

Information	Features
Working Environment Tags	Tags 
Scheduled Downtime	Off 
S3 Storage Classes	Standard-Infrequent Access 
Instance Type	m5.xlarge 
Write Speed	Normal 
Ransomware Protection	Off 
Support Registration	Not Registered 
CIFs Setup	

4. Selecione uma conta do site de suporte da NetApp e clique em **Register**.

Resultado

O BlueXP Registra o sistema com o NetApp.

Converta licenças baseadas em nós em capacidade

Após o fim da disponibilidade (EOA) de suas licenças baseadas em nós, você deve fazer a transição para o licenciamento baseado em capacidade usando a ferramenta de conversão de licenças do BlueXP .

Para compromissos anuais ou de longo prazo, a NetApp recomenda que você entre em Contato com seu representante da NetApp antes da data da EOA (11 de novembro de 2024) ou da data de expiração da licença para garantir que os pré-requisitos para a transição estejam em vigor. Se você não tiver um contrato de longo prazo para um nó Cloud Volumes ONTAP e executar seu sistema com uma assinatura paga conforme o uso (PAYGO) sob demanda, é importante Planejar sua conversão antes do final do suporte (EOS) em 31 de dezembro de 2024. Em ambos os casos, você deve garantir que seu sistema atenda aos requisitos antes de usar a ferramenta de conversão de licenças do BlueXP para uma transição perfeita.

Para obter informações sobre a EOA e a EOS, ["Término da disponibilidade de licenças baseadas em nós"](#) consulte .

Sobre esta tarefa

- Quando você usa a ferramenta de conversão de licença, a transição do modelo de licenciamento baseado em nó para o modelo de licenciamento baseado em capacidade é executada on-line e isso elimina a necessidade de qualquer migração de dados ou provisionamento de recursos de nuvem adicionais.
- Ele é uma operação sem interrupções, e não ocorre interrupção do serviço ou tempo de inatividade do aplicativo.
- Os dados da conta e da aplicação no sistema Cloud Volumes ONTAP permanecem intactos.
- Os recursos de nuvem subjacentes não são afetados após a conversão.
- A ferramenta de conversão de licenças oferece suporte a todos os tipos de implantação, como nó único, alta disponibilidade (HA) em zona de disponibilidade única (AZ), HA em várias AZ, traga sua própria licença (BYOL) e PAYGO.
- A ferramenta suporta todas as licenças baseadas em nós como origem e todas as licenças baseadas em capacidade como destino. Por exemplo, se você tiver uma licença baseada em nó PAYGO Standard, poderá convertê-la em uma licença baseada em capacidade BYOL.
- A conversão é compatível com todos os fornecedores de nuvem, AWS, Azure e Google Cloud.
- Após a conversão, o número de série da licença baseada em nó será substituído por um formato baseado em capacidade. Isso é feito como parte da conversão e é refletido em sua conta do site de suporte da NetApp (NSS).
- Quando você faz a transição para o modelo baseado em capacidade, seus dados continuam sendo mantidos no mesmo local do licenciamento baseado em nó. Essa abordagem garante a ausência de interrupções no posicionamento dos dados e mantém os princípios de soberania de dados durante a transição.

Antes de começar

- Você deve ter uma conta NSS com acesso ao cliente ou acesso de administrador.
- Sua conta NSS deve ser registrada com as credenciais de usuário do BlueXP .
- O ambiente de trabalho deve estar associado à conta NSS com acesso ao cliente ou acesso de administrador.
- Você deve ter uma licença baseada em capacidade válida, seja uma licença BYOL ou uma assinatura do mercado.
- Uma licença baseada em capacidade deve estar disponível na conta BlueXP . Essa licença pode ser uma

assinatura de mercado ou um pacote de oferta BYOL/private na carteira digital BlueXP .

- Compreenda os seguintes critérios antes de selecionar um pacote de destino:
 - Se a conta tiver uma licença BYOL baseada em capacidade, o pacote de destino selecionado deverá estar alinhado com as licenças baseadas em capacidade BYOL da conta:
 - Quando `Professional` for selecionado como o pacote de destino, a conta deve ter uma licença BYOL com um pacote `Professional`:
 - Quando `Essentials` for selecionado como o pacote de destino, a conta deve ter uma licença BYOL com o pacote `Essentials`.
 - Quando `Optimized` é selecionado como o pacote de destino, a conta deve ter uma licença BYOL com o pacote `otimizado`.
 - Se o pacote de destino não se alinhar com a disponibilidade de licença BYOL da conta, isso implica que a licença baseada em capacidade pode não incluir o pacote selecionado. Nesse caso, você será cobrado por meio de sua assinatura do marketplace.
 - Se não houver licença BYOL baseada em capacidade, mas apenas uma assinatura do mercado, você deve garantir que o pacote selecionado esteja incluído na sua assinatura do mercado baseada em capacidade.
 - Se não houver capacidade suficiente na sua licença baseada em capacidade existente e se você tiver uma assinatura do mercado para cobrar pelo uso adicional de capacidade, você será cobrado pela capacidade adicional por meio da sua assinatura do mercado.
 - Se não houver capacidade suficiente em sua licença baseada em capacidade existente e você não tiver uma assinatura do mercado para cobrar pelo uso de capacidade adicional, a conversão não poderá ocorrer. Você deve adicionar uma assinatura de mercado para cobrar a capacidade adicional ou estender a capacidade disponível à sua licença atual.
 - Se o pacote de destino não se alinhar com a disponibilidade de licença BYOL da conta e também se não houver capacidade suficiente em sua licença baseada em capacidade existente, você será cobrado por meio de sua assinatura do marketplace.



Se algum desses requisitos não for cumprido, a conversão de licença não acontece. Em casos específicos, a licença pode ser convertida, mas não pode ser usada. Clique no ícone de informações para identificar os problemas e tomar medidas corretivas.

Passos

1. Na página `Canvas`, clique duas vezes no nome do ambiente de trabalho para o qual você deseja modificar o tipo de licença.
2. Na guia `Visão geral`, clique no painel `recursos`.
3. Verifique o ícone do lápis ao lado de **método de carregamento**. Se o método de carregamento para o seu sistema for `Node Based`, pode convertê-lo em carregamento por capacidade.



O ícone é desativado se o sistema `Cloud Volumes ONTAP` já tiver sido cobrado por capacidade ou se algum dos requisitos não for cumprido.

4. Na tela **Converter licenças baseadas em nó para capacidade**, verifique o nome do ambiente de trabalho e os detalhes da licença de origem.
5. Selecione o pacote de destino para converter a licença existente:
 - `Essenciais`. O valor padrão é `Essentials`.
 - `Professional`

- Otimizado (para Azure)
 - Otimizado (para Google Cloud)
6. Se você tiver uma licença BYOL, marque a caixa de seleção para excluir a licença baseada em nó da conversão pós-carteira digital da BlueXP . Se a conversão não estiver concluída, mesmo ao selecionar esta caixa de seleção, a licença não será excluída da carteira digital. Se você tiver uma assinatura do marketplace, essa opção não estará disponível.
 7. Selecione a caixa de verificação para confirmar que compreende as implicações da alteração e, em seguida, clique em **Proceed**.

Depois de terminar

Veja o novo número de série da licença e verifique as alterações na carteira digital BlueXP .

Gerenciando o estado do Cloud Volumes ONTAP

Você pode parar e iniciar o Cloud Volumes ONTAP da BlueXP para gerenciar seus custos de computação em nuvem.

Agendamento de paradas automáticas do Cloud Volumes ONTAP

Você pode querer desligar o Cloud Volumes ONTAP durante intervalos de tempo específicos para reduzir seus custos de computação. Em vez de fazer isso manualmente, você pode configurar o BlueXP para desligar automaticamente e, em seguida, reiniciar os sistemas em momentos específicos.

Sobre esta tarefa

- Quando você agendar um desligamento automático do seu sistema Cloud Volumes ONTAP, o BlueXP adia o desligamento se uma transferência de dados ativa estiver em andamento.

O BlueXP desliga o sistema após a conclusão da transferência.

- Essa tarefa agenda paradas automáticas de ambos os nós em um par de HA.
- Snapshots de discos de inicialização e raiz não são criados ao desativar o Cloud Volumes ONTAP por meio de paradas programadas.

Os instantâneos são criados automaticamente apenas quando se executa um encerramento manual, conforme descrito na seção seguinte.

Passos

1. Na página Canvas, clique duas vezes no ambiente de trabalho desejado.
2. Na guia Visão geral, clique no painel recursos e, em seguida, clique no ícone de lápis ao lado de **tempo de inatividade programado**.

Information	Features
Working Environment Tags	Tags 
Scheduled Downtime	Off 
S3 Storage Classes	Standard-Infrequent Access 
Instance Type	m5.xlarge 
Write Speed	Normal 
Ransomware Protection	Off 
Support Registration	Not Registered 
CIFs Setup	

3. Especifique o agendamento de encerramento:

- Escolha se deseja desligar o sistema todos os dias, todos os dias da semana, todos os fins de semana ou qualquer combinação das três opções.

- b. Especifique quando pretende desligar o sistema e durante quanto tempo pretende que este seja desligado.

Exemplo

A imagem a seguir mostra uma programação que instrui o BlueXP a desligar o sistema todos os sábados às 20:00 HORAS (8:00 horas) por 12 horas. O BlueXP reinicia o sistema todas as segundas-feiras às 12:00 da manhã

Schedule Downtime
Cloud Manager Time Zone: 17:58 UTC

Select when to turn off your Working Environment:

Turn off every day at 20 : 00 for 12 hours (1-24)
Sun, Mon, Tue, Wed, Thu, Fri, Sat

Turn off every weekdays at 20 : 00 for 12 hours (1-24)
Mon, Tue, Wed, Thu, Fri

Turn off every weekend at 20 : 00 for 12 hours (1-48)
Sat

4. Clique em **Salvar**.

Resultado

O BlueXP salva a programação. O item de linha de tempo de inatividade programado correspondente no painel recursos exibe 'On'.

Parar o Cloud Volumes ONTAP

Parar o Cloud Volumes ONTAP evita que você acumule custos de computação e cria snapshots dos discos raiz e de inicialização, o que pode ser útil para a solução de problemas.



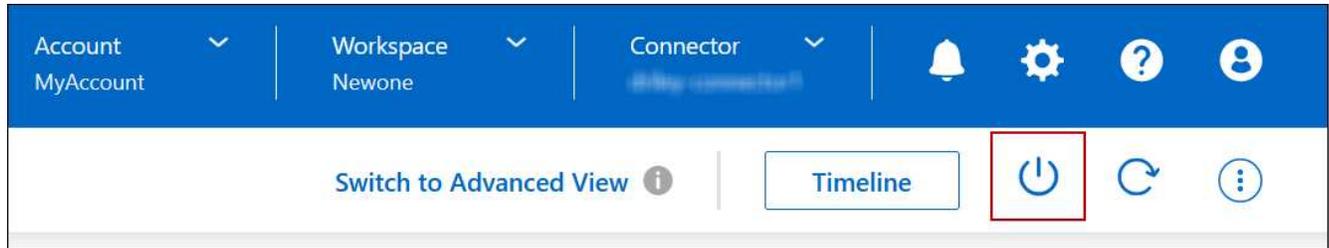
Para reduzir custos, o BlueXP exclui periodicamente snapshots mais antigos dos discos raiz e de inicialização. Apenas os dois snapshots mais recentes são retidos para os discos raiz e de inicialização.

Sobre esta tarefa

Quando você interrompe um par de HA, o BlueXP encerra ambos os nós.

Passos

1. No ambiente de trabalho, clique no ícone **Desligar**.



2. Mantenha a opção de criar instantâneos ativada porque os instantâneos podem ativar a recuperação do sistema.
3. Clique em **Desligar**.

Pode demorar alguns minutos para parar o sistema. Pode reiniciar os sistemas posteriormente a partir da página ambiente de trabalho.



Os instantâneos são criados automaticamente após a reinicialização.

Sincronize a hora do sistema usando NTP

Especificar um servidor NTP sincroniza o tempo entre os sistemas da rede, o que pode ajudar a evitar problemas devido a diferenças de tempo.

Especifique um servidor NTP usando "API BlueXP " ou a partir da interface do usuário quando "Crie um servidor CIFS" você .

Modifique a velocidade de gravação do sistema

O BlueXP permite que você escolha uma velocidade de gravação normal ou alta para Cloud Volumes ONTAP. A velocidade de gravação padrão é normal. Você pode mudar para alta velocidade de gravação se a performance de gravação rápida for necessária para seu workload.

A alta velocidade de gravação é compatível com todos os tipos de sistemas de nó único e algumas configurações de par de HA. Veja as configurações suportadas no "[Notas de versão do Cloud Volumes ONTAP](#)"

Antes de alterar a velocidade de gravação, você deve "[entenda as diferenças entre as configurações normal e alta](#)".

Sobre esta tarefa

- Certifique-se de que operações como criação de volume ou agregado não estejam em andamento.
- Esteja ciente de que essa alteração reinicia o sistema Cloud Volumes ONTAP. Este é um processo disruptivo que requer tempo de inatividade para todo o sistema.

Passos

1. Na página Canvas, clique duas vezes no nome do sistema configurado para a velocidade de gravação.

2. Na guia Visão geral, clique no painel recursos e, em seguida, clique no ícone de lápis ao lado de **velocidade de gravação**.

Information	Features
Working Environment Tags	Tags 
Scheduled Downtime	Off 
S3 Storage Classes	Standard-Infrequent Access 
Instance Type	m5.xlarge 
Write Speed	Normal 
Ransomware Protection	Off 
Support Registration	Not Registered 
CIFs Setup	

3. Selecione **normal** ou **High**.

Se você escolher Alto, então você precisará ler a declaração "Eu entendo..." e confirmar marcando a caixa.



A opção **alta** velocidade de gravação é compatível com pares de HA do Cloud Volumes ONTAP no Google Cloud a partir da versão 9.13.0.

4. Clique em **Salvar**, revise a mensagem de confirmação e clique em **aprovar**.

Altere a senha do Cloud Volumes ONTAP

O Cloud Volumes ONTAP inclui uma conta de administrador do cluster. Você pode alterar a senha dessa conta no BlueXP , se necessário.



Você não deve alterar a senha da conta de administrador por meio do Gerenciador de sistema do ONTAP ou da CLI do ONTAP. A senha não será refletida no BlueXP . Como resultado, o BlueXP não pode monitorar a instância corretamente.

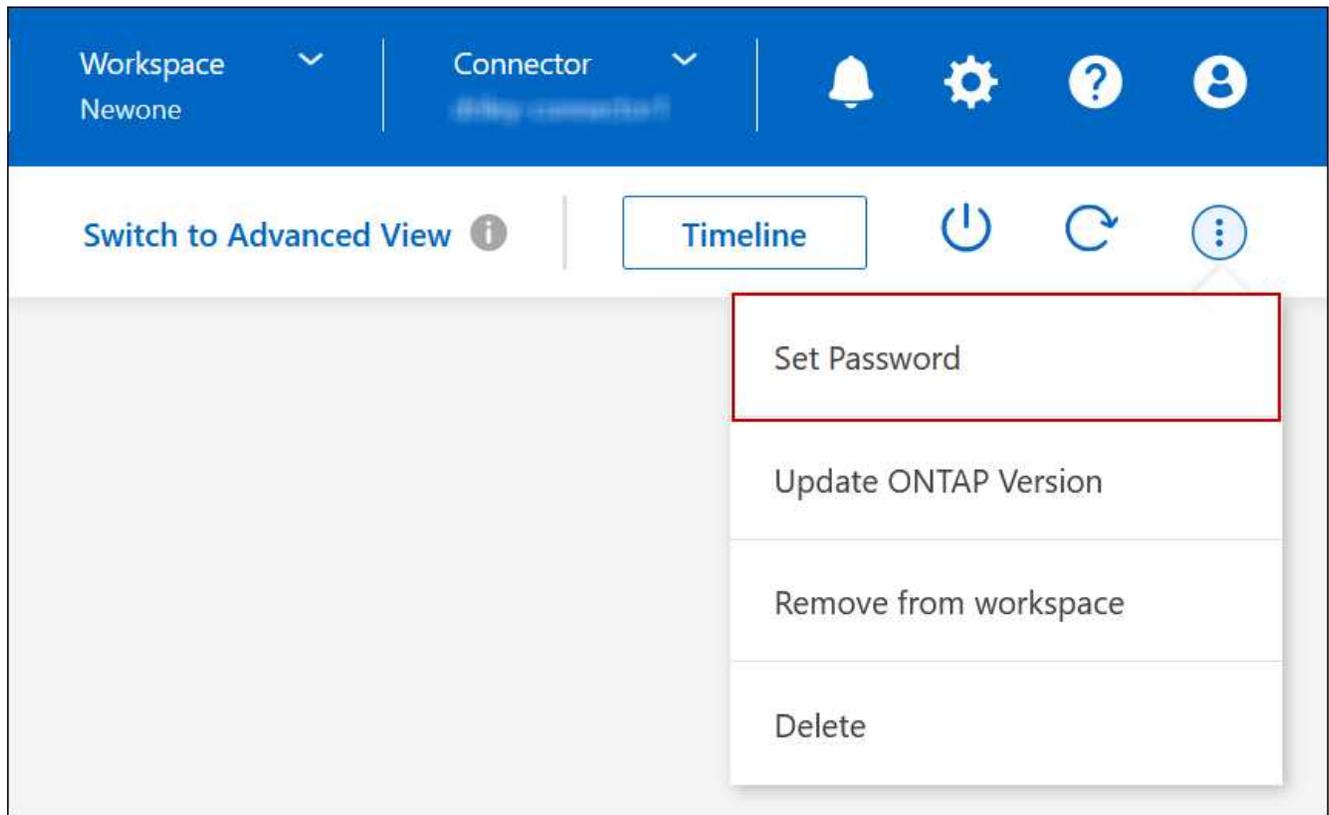
Sobre esta tarefa

A nova palavra-passe deve respeitar as seguintes regras:

- Não pode conter o nome de utilizador
- Deve ter pelo menos oito caracteres
- Deve conter pelo menos uma letra e um número
- Não pode ser o mesmo que as últimas seis senhas

Passos

1. Na página tela, clique duas vezes no nome do ambiente de trabalho do Cloud Volumes ONTAP.
2. No canto superior direito do console BlueXP , clique no ícone de elipses e selecione **Definir senha**.



Adicione, remova ou exclua sistemas

Adição de sistemas Cloud Volumes ONTAP existentes ao BlueXP

Você pode descobrir e adicionar sistemas Cloud Volumes ONTAP existentes ao BlueXP . Você pode fazer isso se você implantou um novo sistema BlueXP .

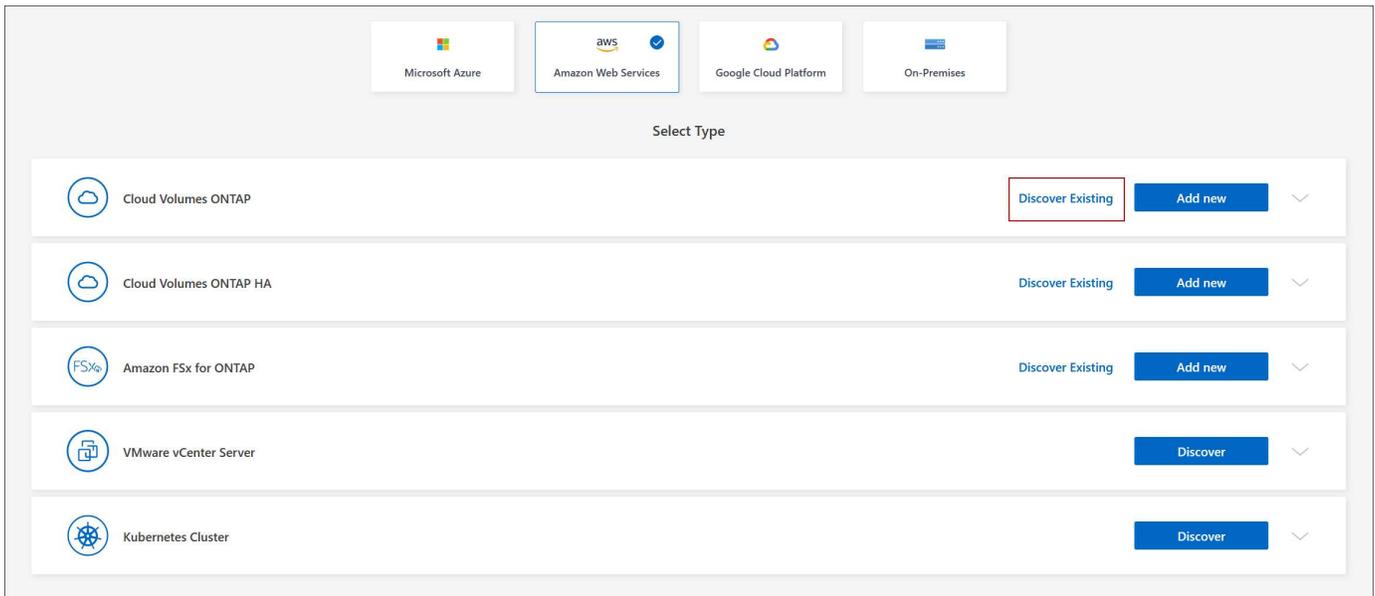
Antes de começar

Você deve saber a senha da conta de usuário admin do Cloud Volumes ONTAP.

Passos

1. No menu de navegação à esquerda, selecione **Storage > Canvas**.
2. Na página Canvas, clique em **Adicionar ambiente de trabalho**.
3. Selecione o provedor de nuvem no qual o sistema reside.
4. Escolha o tipo de sistema Cloud Volumes ONTAP.
5. Clique no link para descobrir um sistema existente.

E



1. Na página região, escolha a região em que as instâncias estão sendo executadas e selecione as instâncias.
2. Na página credenciais, digite a senha do usuário admin do Cloud Volumes ONTAP e clique em **Go**.

Resultado

O BlueXP adiciona as instâncias do Cloud Volumes ONTAP ao projeto ou à área de trabalho.

Remoção de ambientes de trabalho do Cloud Volumes ONTAP

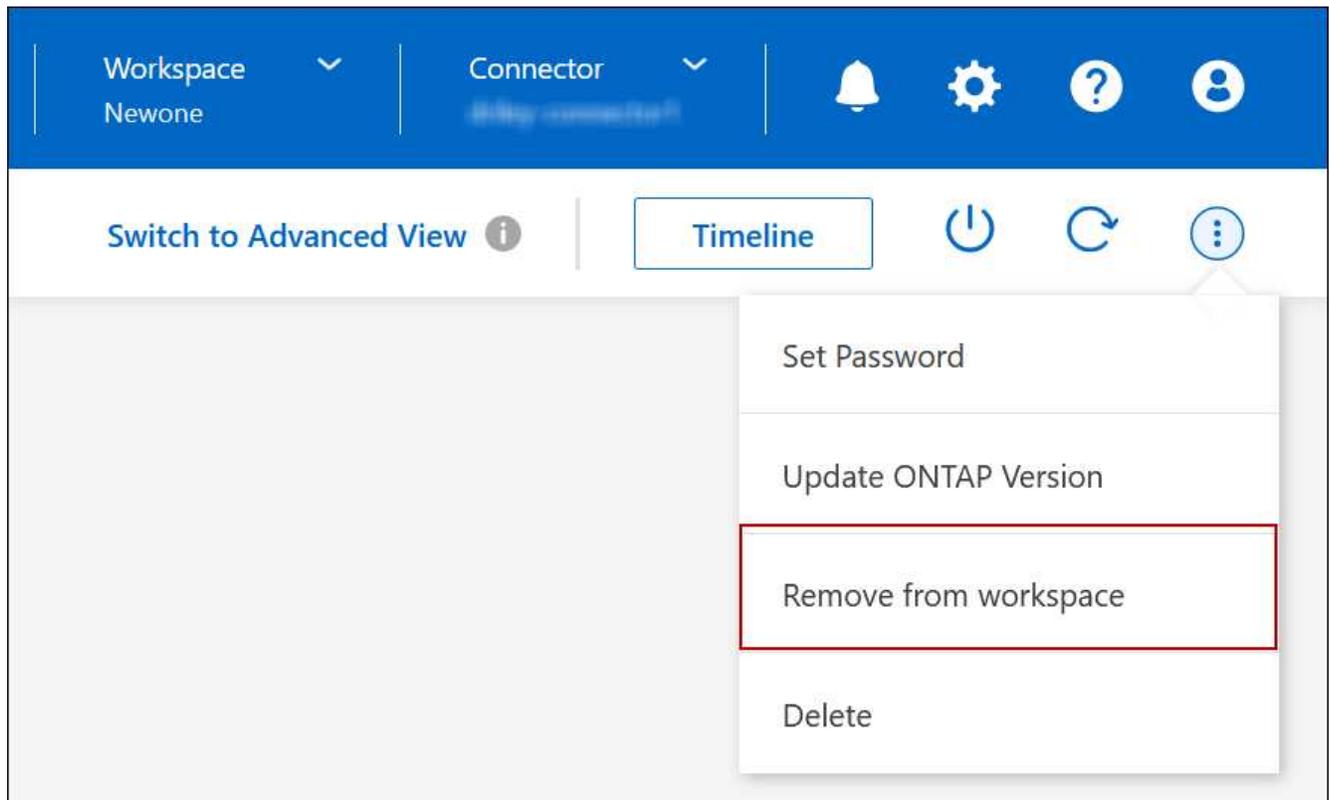
Você pode remover um ambiente de trabalho do Cloud Volumes ONTAP para movê-lo para outro sistema ou para solucionar problemas de descoberta.

Sobre esta tarefa

Remover um ambiente de trabalho do Cloud Volumes ONTAP remove-o do BlueXP . Ele não exclui o sistema Cloud Volumes ONTAP. Você pode mais tarde redescobrir o ambiente de trabalho - por exemplo, se você teve problemas durante a descoberta inicial.

Passos

1. Na página Canvas, clique duas vezes no ambiente de trabalho que deseja remover.
2. No canto superior direito do console do BlueXP , clique no ícone de elipses e selecione **Remover da área de trabalho**.



3. Na janela Revisão do espaço de trabalho, clique em **Remover**.

Resultado

O BlueXP remove o ambiente de trabalho. Os usuários podem redescobrir esse ambiente de trabalho a partir da página do Canvas a qualquer momento.

Eliminar um sistema Cloud Volumes ONTAP

Você deve sempre excluir sistemas Cloud Volumes ONTAP do BlueXP, em vez de do console do seu provedor de nuvem. Por exemplo, se você encerrar uma instância do Cloud Volumes ONTAP licenciada do seu provedor de nuvem, não poderá usar a chave de licença para outra instância. Você deve excluir o ambiente de trabalho do BlueXP para liberar a licença.

Quando você exclui um ambiente de trabalho, o BlueXP encerra instâncias do Cloud Volumes ONTAP e exclui discos e snapshots.

Os recursos gerenciados por outros serviços, como backups para backup e recuperação do BlueXP e instâncias para classificação do BlueXP, não são excluídos quando você exclui um ambiente de trabalho. Você precisará excluí-los manualmente. Se você não fizer isso, continuará a receber cobranças por esses recursos.



Quando o BlueXP implanta o Cloud Volumes ONTAP em seu provedor de nuvem, ele habilita a proteção de encerramento nas instâncias. Esta opção ajuda a evitar a cessação acidental.

Passos

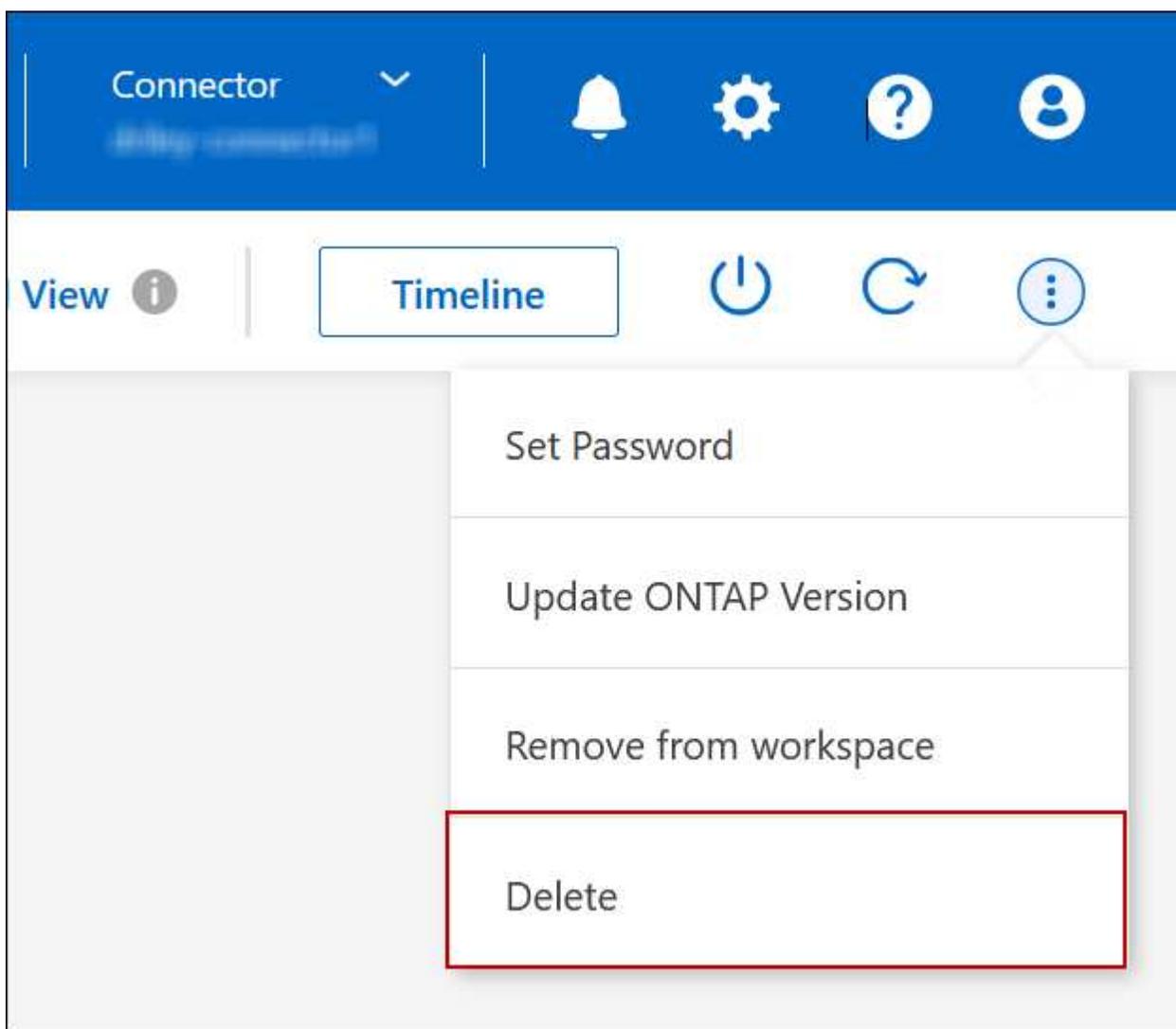
1. Se você ativou o backup e a recuperação do BlueXP no ambiente de trabalho, determine se os dados de backup ainda são necessários e, em seguida ["exclua os backups, se necessário"](#), .

O backup e a recuperação do BlueXP são independentes do Cloud Volumes ONTAP por design. O backup e a recuperação do BlueXP não excluem automaticamente os backups quando você exclui um sistema Cloud Volumes ONTAP e não há suporte atual na IU para excluir os backups depois que o sistema for excluído.

2. Se você ativou a classificação do BlueXP neste ambiente de trabalho e nenhum outro ambiente de trabalho usa esse serviço, então você precisará excluir a instância do serviço.

["Saiba mais sobre a instância de classificação do BlueXP"](#).

3. Exclua o ambiente de trabalho do Cloud Volumes ONTAP.
 - a. Na página tela, clique duas vezes no nome do ambiente de trabalho do Cloud Volumes ONTAP que você deseja excluir.
 - b. No canto superior direito do console BlueXP, clique no ícone de elipses e selecione **Excluir**.



- c. Na janela Excluir ambiente de trabalho, digite o nome do ambiente de trabalho e clique em **Excluir**.
Pode demorar até 5 minutos para eliminar o ambiente de trabalho.

Administração da AWS

Altere o tipo de instância EC2 para Cloud Volumes ONTAP

Você pode escolher entre várias instâncias ou tipos ao iniciar o Cloud Volumes ONTAP na AWS. Você pode alterar o tipo de instância a qualquer momento se você determinar que ele é subdimensionado ou superdimensionado para suas necessidades.

Sobre esta tarefa

- A giveback automática deve estar ativada num par de HA Cloud Volumes ONTAP (esta é a predefinição). Se não for, então a operação falhará.

["Documentação do ONTAP 9: Comandos para configurar o giveback automático"](#)

- Alterar o tipo de instância pode afetar as cobranças de serviço da AWS.
- A operação reinicia o Cloud Volumes ONTAP.

Para sistemas de nó único, a e/S é interrompida.

Para pares de HA, a alteração não causa interrupções. Os pares DE HA continuam fornecendo dados.



O BlueXP muda um nó de cada vez, iniciando a aquisição e aguardando a devolução. A equipe de Garantia de qualidade da NetApp testou tanto a escrita quanto a leitura de arquivos durante esse processo e não viu nenhum problema no lado do cliente. À medida que as conexões mudaram, algumas tentativas foram observadas no nível de e/S, mas a camada de aplicação superou a redefinição das conexões NFS/CIFS.

Referência

Para obter uma lista dos tipos de instâncias compatíveis na AWS, ["Instâncias EC2 suportadas"](#) consulte .

Se você não puder alterar o tipo de instância de instâncias C4, M4 ou R4, consulte o artigo da KB ["Convertendo uma instância do AWS Xen CVO para Nitro \(KVM\)"](#).

Passos

1. Na página Canvas, selecione o ambiente de trabalho.
2. Na guia Visão geral, clique no painel recursos e, em seguida, clique no ícone de lápis ao lado de **tipo de instância**.

Information	Features
Working Environment Tags	Tags 
Scheduled Downtime	Off 
S3 Storage Classes	Standard-Infrequent Access 
Instance Type	m5.xlarge 
Write Speed	Normal 
Ransomware Protection	Off 
Support Registration	Not Registered 
CIFs Setup	

Se você estiver usando uma licença de pagamento conforme o uso (PAYGO) baseada em nó, você pode escolher uma licença e tipo de instância diferentes clicando no ícone de lápis ao lado de **tipo de licença**.

1. Escolha um tipo de instância, marque a caixa de seleção para confirmar que você entende as implicações da alteração e clique em **alterar**.

Resultado

O Cloud Volumes ONTAP reinicializa com a nova configuração.

Alterar tabelas de rota para pares HA em vários AZs

Você pode modificar as tabelas de rota da AWS que incluem rotas para os endereços IP flutuantes de um par de HA implantado em várias zonas de disponibilidade da AWS (AZs). Você pode fazer isso se novos clientes NFS ou CIFS precisarem acessar um par de HA na AWS.

Passos

1. Na página Canvas, selecione o ambiente de trabalho.
2. Na guia Visão geral, clique no painel recursos e, em seguida, clique no ícone de lápis ao lado de **tabelas de rota**.



3. Modifique a lista de tabelas de rota selecionadas e clique em **Salvar**.

Resultado

O BlueXP envia uma solicitação da AWS para modificar as tabelas de rota.

Administração do Azure

Altere o tipo de VM do Azure para o Cloud Volumes ONTAP

Você pode escolher entre vários tipos de VM ao iniciar o Cloud Volumes ONTAP no Microsoft Azure. Você pode alterar o tipo de VM a qualquer momento se determinar que ele é subdimensionado ou superdimensionado para suas necessidades.

Sobre esta tarefa

- A giveback automática deve estar ativada num par de HA Cloud Volumes ONTAP (esta é a predefinição). Se não for, então a operação falhará.

["Documentação do ONTAP 9: Comandos para configurar o giveback automático"](#)

- Alterar o tipo de VM pode afetar as taxas de serviço do Microsoft Azure.
- A operação reinicia o Cloud Volumes ONTAP.

Para sistemas de nó único, a e/S é interrompida.

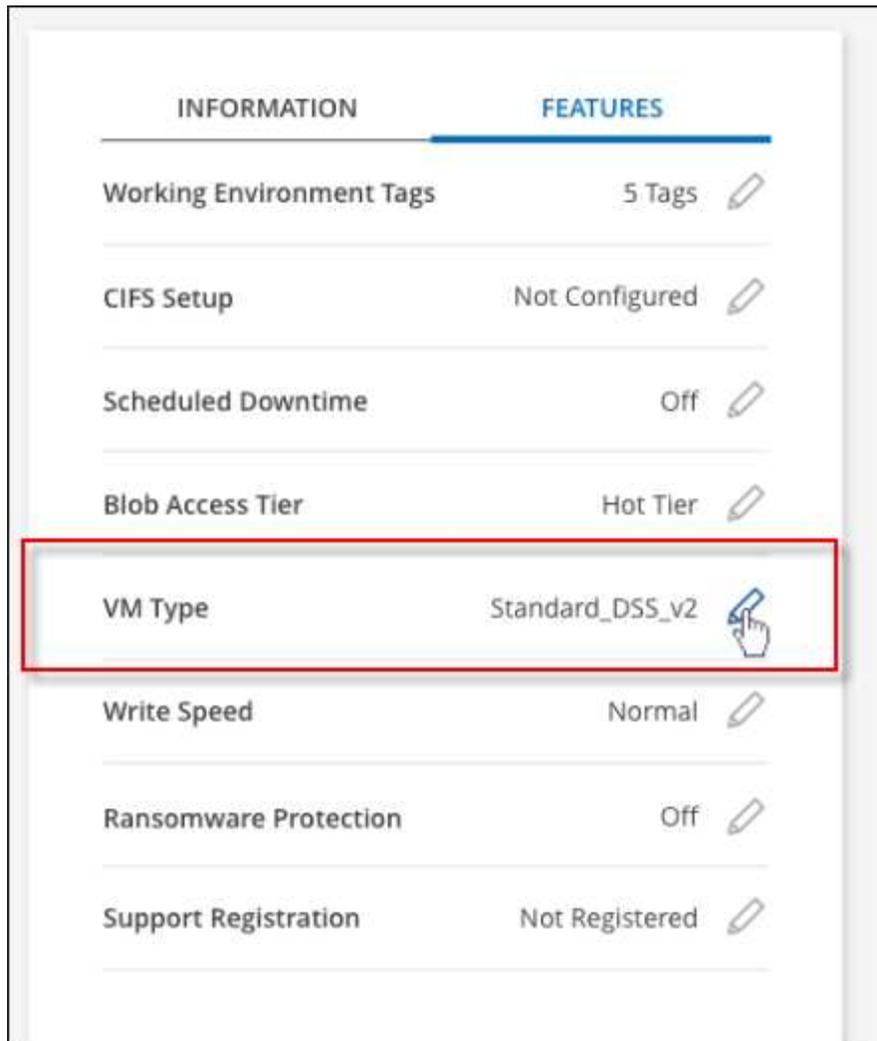
Para pares de HA, a alteração não causa interrupções. Os pares DE HA continuam fornecendo dados.



O BlueXP muda um nó de cada vez, iniciando a aquisição e aguardando a devolução. A equipe de Garantia de qualidade da NetApp testou tanto a escrita quanto a leitura de arquivos durante esse processo e não viu nenhum problema no lado do cliente. À medida que as conexões mudaram, algumas tentativas foram observadas no nível de e/S, mas a camada de aplicação superou a refiação das conexões NFS/CIFS.

Passos

1. Na página Canvas, selecione o ambiente de trabalho.
2. Na guia Visão geral, clique no painel recursos e, em seguida, clique no ícone de lápis ao lado de **tipo de VM**.



Se você estiver usando uma licença de pagamento conforme o uso baseada em nó (PAYGO), você pode escolher uma licença diferente e um tipo de VM clicando no ícone de lápis ao lado de **tipo de licença**.

1. Selecione um tipo de VM, marque a caixa de seleção para confirmar que você entende as implicações da alteração e clique em **alterar**.

Resultado

O Cloud Volumes ONTAP reinicializa com a nova configuração.

Substituindo bloqueios CIFS para pares de HA do Cloud Volumes ONTAP no Azure

A organização ou o administrador da conta do BlueXP pode habilitar uma configuração no BlueXP que impede problemas com o armazenamento Cloud Volumes ONTAP giveback durante eventos de manutenção do Azure. Quando você ativa essa configuração, o Cloud Volumes ONTAP veta o CIFS bloqueia e redefine as sessões ativas do CIFS.

Sobre esta tarefa

O Microsoft Azure agenda eventos de manutenção periódica em suas máquinas virtuais. Quando ocorre um evento de manutenção em um par de HA do Cloud Volumes ONTAP, o par de HA inicia o takeover do storage. Se houver sessões CIFS ativas durante este evento de manutenção, os bloqueios nos arquivos CIFS podem

impedir o armazenamento de giveback.

Se ativar esta definição, o Cloud Volumes ONTAP vetará os bloqueios e redefinirá as sessões CIFS ativas. Como resultado, o par de HA pode concluir a giveback de storage durante esses eventos de manutenção.



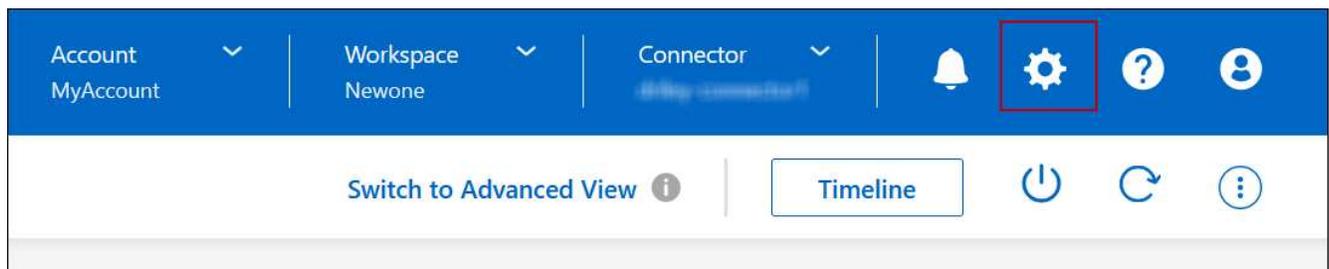
Esse processo pode ser disruptivo para clientes CIFS. Os dados que não forem comprometidos com clientes CIFS podem ser perdidos.

O que você vai precisar

Você precisa criar um conector antes de poder alterar as configurações do BlueXP . ["Saiba como"](#).

Passos

1. No canto superior direito do console BlueXP , clique no ícone Configurações e selecione **Configurações do Cloud Volumes ONTAP**.



2. Em **Azure**, clique em **bloqueios CIFS do Azure para ambientes de trabalho do Azure HA**.
3. Clique na caixa de verificação para ativar a funcionalidade e, em seguida, clique em **Guardar**.

Use um link privado do Azure ou endpoints de serviço

O Cloud Volumes ONTAP usa um link privado do Azure para conexões com suas contas de armazenamento associadas. Se necessário, você pode desativar os links privados do Azure e usar endpoints de serviço em vez disso.

Visão geral

Por padrão, o BlueXP habilita um link privado do Azure para conexões entre o Cloud Volumes ONTAP e suas contas de armazenamento associadas. Um link privado do Azure protege conexões entre endpoints no Azure e fornece benefícios de desempenho.

Se necessário, você pode configurar o Cloud Volumes ONTAP para usar endpoints de serviço em vez de um link privado do Azure.

Em qualquer uma das configurações, o BlueXP sempre limita o acesso à rede para conexões entre Cloud Volumes ONTAP e contas de armazenamento. O acesso à rede é limitado ao VNet onde o Cloud Volumes ONTAP é implantado e ao VNet onde o conector é implantado.

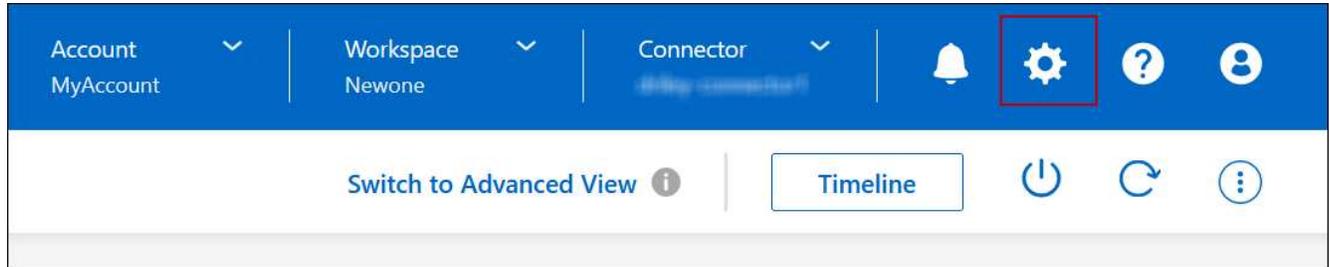
Desative os links privados do Azure e use endpoints de serviço em vez disso

Se exigido pela sua empresa, você pode alterar uma configuração no BlueXP para que ele configure o Cloud Volumes ONTAP para usar endpoints de serviço em vez de um link privado do Azure. A alteração desta definição aplica-se aos novos sistemas Cloud Volumes ONTAP criados por si. Os pontos de extremidade de serviço são suportados apenas ["Pares de regiões do Azure"](#) entre o conector e os VNets Cloud Volumes ONTAP.

O conetor deve ser implantado na mesma região do Azure que os sistemas Cloud Volumes ONTAP que gerencia, ou no "[Par de regiões do Azure](#)" para os sistemas Cloud Volumes ONTAP.

Passos

1. No canto superior direito do console BlueXP , clique no ícone Configurações e selecione **Configurações do Cloud Volumes ONTAP**.



2. Em **Azure**, clique em **usar o Azure Private Link**.
3. Desmarque **ligação privada entre o Cloud Volumes ONTAP e contas de armazenamento**.
4. Clique em **Salvar**.

Depois de terminar

Se você desativou os Links privados do Azure e o conetor usa um servidor proxy, você deve habilitar o tráfego direto da API.

["Saiba como ativar o tráfego direto da API no conetor"](#)

Trabalhe com o Azure Private Links

Na maioria dos casos, não há nada que você precise fazer para configurar os links privados do Azure com o Cloud Volumes ONTAP. O BlueXP gerencia links privados do Azure para você. Mas se você usar uma zona DNS privada do Azure existente, precisará editar um arquivo de configuração.

Requisito para DNS personalizado

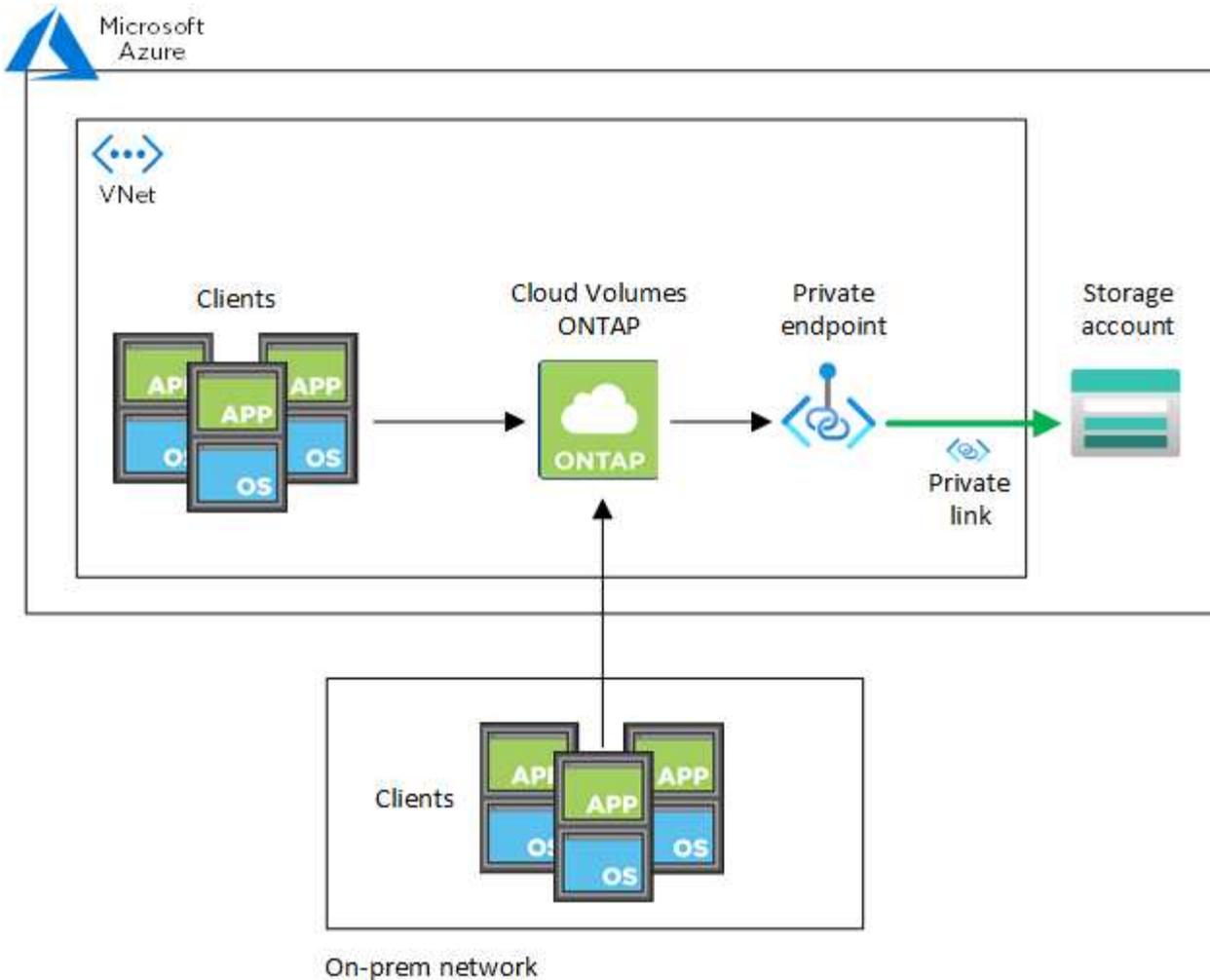
Opcionalmente, se você trabalha com DNS personalizado, você precisa criar um encaminhador condicional para a zona DNS privada do Azure a partir de seus servidores DNS personalizados. Para saber mais, ["Documentação do Azure sobre o uso de um encaminhador DNS"](#) consulte .

Como as conexões de link privado funcionam

Quando o BlueXP implanta o Cloud Volumes ONTAP no Azure, ele cria um endpoint privado no grupo de recursos. O endpoint privado está associado às contas de armazenamento do Cloud Volumes ONTAP. Como resultado, o acesso ao storage Cloud Volumes ONTAP viaja pela rede backbone da Microsoft.

O acesso ao cliente passa pelo link privado quando os clientes estão dentro do mesmo VNet que o Cloud Volumes ONTAP, dentro de VNets peered ou em sua rede local ao usar uma conexão VPN privada ou ExpressRoute ao VNet.

Aqui está um exemplo que mostra o acesso do cliente através de um link privado dentro do mesmo VNet e de uma rede local que tem uma conexão VPN privada ou ExpressRoute.



Se o conector e os sistemas Cloud Volumes ONTAP forem implantados em VNets diferentes, você deverá configurar o peering VNet entre o VNet onde o conector é implantado e o VNet onde os sistemas Cloud Volumes ONTAP são implantados.

Forneça ao BlueXP detalhes sobre o DNS Privado do Azure

Se utilizar "[DNS privado do Azure](#)", terá de modificar um ficheiro de configuração em cada conector. Caso contrário, o BlueXP não pode ativar a conexão do Azure Private Link entre o Cloud Volumes ONTAP e suas contas de armazenamento associadas.

Observe que o nome DNS deve corresponder aos requisitos de nomenclatura do DNS do Azure "[Como mostrado na documentação do Azure](#)".

Passos

1. SSH para o host do conector e faça login.
2. Navegue para o seguinte diretório: `/Opt/application/NetApp/cloudmanager/docker_occm/data`
3. Edite o `app.conf` adicionando o parâmetro "user-private-dns-zone-settings" com os seguintes pares de palavras-chave-valor:

```
"user-private-dns-zone-settings" : {
  "resource-group" : "<resource group name of the DNS zone>",
  "subscription" : "<subscription ID>",
  "use-existing" : true,
  "create-private-dns-zone-link" : true
}
```

O parâmetro deve ser inserido no mesmo nível que "System-id", como mostrado abaixo:

```
"system-id" : "<system ID>",
"user-private-dns-zone-settings" : {
```

Observe que a palavra-chave de assinatura é necessária somente se a zona DNS Privada existir em uma assinatura diferente do conetor.

4. Guarde o ficheiro e termine a sessão no conetor.

Não é necessário reiniciar.

Ativar reversão em falhas

Se o BlueXP não criar um link privado do Azure como parte de ações específicas, ele conclui a ação sem a conexão do link privado do Azure. Isso pode acontecer ao criar um novo ambiente de trabalho (nó único ou par de HA), ou quando as seguintes ações ocorrem em um par de HA: Criar um novo agregado, adicionar discos a um agregado existente ou criar uma nova conta de storage quando estiver acima de 32 TIB.

Você pode alterar esse comportamento padrão habilitando rollback se o BlueXP não conseguir criar o link privado do Azure. Isso pode ajudar a garantir que você esteja totalmente em conformidade com os regulamentos de segurança da sua empresa.

Se você ativar a reversão, o BlueXP interromperá a ação e reverterá todos os recursos criados como parte da ação.

Você pode ativar a reversão através da API ou atualizando o arquivo app.conf.

Ativar rollback através da API

Passo

1. Use a PUT `/occm/config` chamada API com o seguinte corpo de solicitação:

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

Ativar reversão atualizando o app.conf

Passos

1. SSH para o host do conetor e faça login.

2. Navegue para o seguinte diretório: /Opt/application/NetApp/cloudmanager/docker_occm/data
3. Edite o app.conf adicionando o seguinte parâmetro e valor:

```
"rollback-on-private-link-failure": true
. Guarde o ficheiro e termine a sessão no conetor.
```

Não é necessário reiniciar.

Movendo grupos de recursos

O Cloud Volumes ONTAP oferece suporte a movimentos de grupos de recursos do Azure, mas o fluxo de trabalho acontece somente no console do Azure.

Você pode mover um ambiente de trabalho de um grupo de recursos para um grupo de recursos diferente no Azure na mesma assinatura do Azure. A movimentação de grupos de recursos entre diferentes assinaturas do Azure não é suportada.

Passos

1. Remova o ambiente de trabalho do **Canvas**.

Para saber como remover um ambiente de trabalho, ["Remoção de ambientes de trabalho do Cloud Volumes ONTAP"](#) consulte .

2. Execute a movimentação do grupo de recursos no console do Azure.

Para concluir a deslocação, ["Mova recursos para um novo grupo de recursos ou assinatura na documentação do Microsoft Azure"](#) consulte a .

3. Em **Canvas**, descubra o ambiente de trabalho.
4. Procure o novo grupo de recursos nas informações do ambiente de trabalho.

Resultado

O ambiente de trabalho e seus recursos (VMs, discos, contas de storage, interfaces de rede, snapshots) estão no novo grupo de recursos.

Segregar o tráfego SnapMirror no Azure

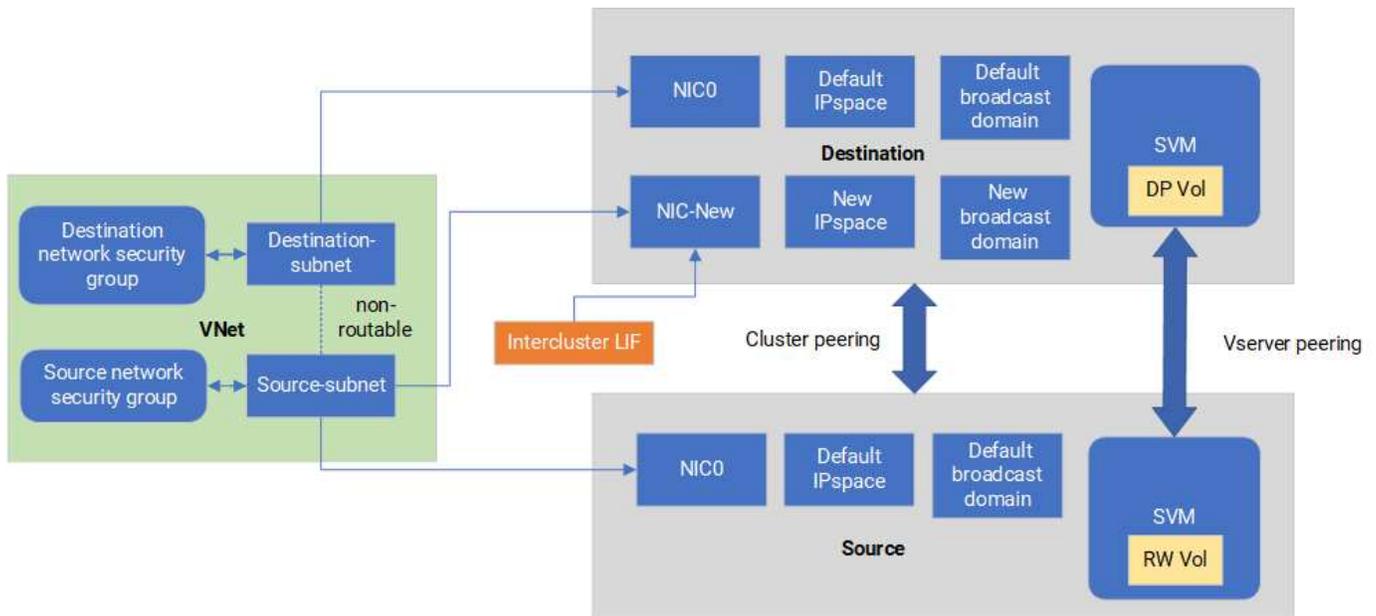
Com o Cloud Volumes ONTAP no Azure, você pode segregar o tráfego de replicação do SnapMirror a partir de dados e tráfego de gerenciamento. Para segregar o tráfego de replicação do SnapMirror do tráfego de dados, você adicionará uma nova placa de interface de rede (NIC), um LIF entre clusters associado e uma sub-rede não roteável.

Sobre a segregação de tráfego do SnapMirror no Azure

Por padrão, o BlueXP configura todas as NICs e LIFs em uma implantação do Cloud Volumes ONTAP na mesma sub-rede. Nessas configurações, o tráfego de replicação e os dados do SnapMirror e o tráfego de gerenciamento usam a mesma sub-rede. O tráfego segregante do SnapMirror aproveita uma sub-rede adicional que não é roteável para a sub-rede existente usada para dados e tráfego de gerenciamento.

Figura 1

Os diagramas a seguir mostram a segregação do tráfego de replicação do SnapMirror com uma NIC adicional, um LIF entre clusters associado e uma sub-rede não roteável em uma implantação de nó único. A implantação de um par de HA difere ligeiramente.



Antes de começar

Reveja as seguintes considerações:

- Você só pode adicionar uma única NIC a um nó único do Cloud Volumes ONTAP ou implantação de par de HA (instância de VM) para segregação de tráfego do SnapMirror.
- Para adicionar uma nova NIC, o tipo de instância da VM que você implantar deve ter uma NIC não utilizada.
- Os clusters de origem e destino devem ter acesso à mesma rede virtual (VNet). O cluster de destino é um sistema Cloud Volumes ONTAP no Azure. O cluster de origem pode ser um sistema Cloud Volumes ONTAP no Azure ou um sistema ONTAP.

Etapa 1: Crie uma NIC adicional e anexe à VM de destino

Esta seção fornece instruções sobre como criar uma NIC adicional e anexá-la à VM de destino. A VM de destino é o nó único ou sistema de par de HA no Cloud Volumes ONTAP no Azure, onde você deseja configurar sua NIC adicional.

Passos

1. Na CLI do ONTAP, pare o nó.

```
dest::> halt -node <dest_node-vm>
```

2. No portal do Azure, verifique se o status da VM (nó) está parado.

```
az vm get-instance-view --resource-group <dest-rg> --name <dest-vm>
--query instanceView.statuses[1].displayStatus
```

3. Use o ambiente Bash no Azure Cloud Shell para parar o nó.

a. Pare o nó.

```
az vm stop --resource-group <dest_node-rg> --name <dest_node-vm>
```

b. Desalocar o nó.

```
az vm deallocate --resource-group <dest_node-rg> --name <dest_node-vm>
```

4. Configure as regras do grupo de segurança de rede para tornar as duas sub-redes (sub-rede do cluster de origem e sub-rede do cluster de destino) não roteáveis entre si.

a. Crie a nova NIC na VM de destino.

b. Procure a ID da sub-rede para a sub-rede do cluster de origem.

```
az network vnet subnet show -g <src_vnet-rg> -n <src_subnet> --vnet -name <vnet> --query id
```

c. Crie a nova NIC na VM de destino com o ID da sub-rede para a sub-rede do cluster de origem. Aqui você insere o nome da nova NIC.

```
az network nic create -g <dest_node-rg> -n <dest_node-vm-nic-new> --subnet <id_from_prev_command> --accelerated-networking true
```

d. Salve o privateIPAddress. Este endereço IP, <new_added_nic_primary_addr>, é usado para criar um LIF entre clusters [Domínio de broadcast](#), [LIF entre clusters para a nova NIC](#)no .

5. Anexe a nova NIC à VM.

```
az vm nic add -g <dest_node-rg> --vm-name <dest_node-vm> --nics <dest_node-vm-nic-new>
```

6. Inicie a VM (nó).

```
az vm start --resource-group <dest_node-rg> --name <dest_node-vm>
```

7. No portal do Azure, vá para **rede** e confirme se a nova NIC, por exemplo, nic-novo, existe e a rede acelerada está ativada.

```
az network nic list --resource-group azure-59806175-60147103-azure-rg
--query "[].{NIC: name, VM: virtualMachine.id}"
```

Para implantações de par de HA, repita as etapas para o nó do parceiro.

Etapa 2: Crie um novo IPspace, domínio de broadcast e LIF entre clusters para a nova NIC

Um espaço IPspace separado para LIFs entre clusters fornece separação lógica entre a funcionalidade de rede para replicação entre clusters.

Use a CLI do ONTAP para as etapas a seguir.

Passos

1. Crie o novo IPspace (`new_ipspace`).

```
dest::> network ipspace create -ipspace <new_ipspace>
```

2. Crie um domínio de broadcast no novo IPspace (`new_ipspace`) e adicione a nova porta nic.

```
dest::> network port show
```

3. Para sistemas de nó único, a porta recém-adicionada é `e0b`. Para implantações de par de HA com discos gerenciados, a porta recém-adicionada é `e0d`. Para implantações de par de HA com blobs de página, a porta recém-adicionada é `e0e`. Use o nome do nó e não o nome da VM. Localize o nome do nó executando ``node show``.

```
dest::> broadcast-domain create -broadcast-domain <new_bd> -mtu 1500
-ipspace <new_ipspace> -ports <dest_node-cot-vm:e0b>
```

4. Crie um LIF entre clusters no novo domínio broadcast (`new_bd`) e na nova NIC (`nic-novo`).

```
dest::> net int create -vserver <new_ipspace> -lif <new_dest_node-ic-
lif> -service-policy default-intercluster -address
<new_added_nic_primary_addr> -home-port <e0b> -home-node <node> -netmask
<new_netmask_ip> -broadcast-domain <new_bd>
```

5. Verificar a criação do novo LIF entre clusters.

```
dest::> net int show
```

Para implantações de par de HA, repita as etapas para o nó do parceiro.

Etapa 3: Verifique o peering de cluster entre os sistemas de origem e destino

Esta seção fornece instruções sobre como verificar peering entre os sistemas de origem e destino.

Use a CLI do ONTAP para as etapas a seguir.

Passos

1. Verifique se o LIF entre clusters do cluster de destino pode fazer ping no LIF entre clusters do cluster de origem. Como o cluster de destino executa esse comando, o endereço IP de destino é o endereço IP de LIF entre clusters na origem.

```
dest::> ping -lif <new_dest_node-ic-lif> -vserver <new_ipspace>
-destination <10.161.189.6>
```

2. Verifique se o LIF entre clusters do cluster de origem pode fazer ping no LIF entre clusters do cluster de destino. O destino é o endereço IP da nova NIC criada no destino.

```
src::> ping -lif <src_node-ic-lif> -vserver <src_svm> -destination
<10.161.189.18>
```

Para implantações de par de HA, repita as etapas para o nó do parceiro.

Etapa 4: Criar peering SVM entre o sistema de origem e destino

Esta seção fornece instruções sobre como criar peering SVM entre o sistema de origem e destino.

Use a CLI do ONTAP para as etapas a seguir.

Passos

1. Crie peering de cluster no destino usando o endereço IP de clusters de LIF de origem como o `-peer-addr`s. Para pares de HA, liste o endereço IP de LIF entre clusters de origem para ambos os nós como o `-peer-addr`s.

```
dest::> cluster peer create -peer-addr <10.161.189.6> -ipspace
<new_ipspace>
```

2. Introduza e confirme a frase-passe.
3. Crie peering de cluster na origem usando o endereço IP de LIF do cluster de destino como `peer-addr`s. Para pares de HA, liste o endereço IP de LIF entre clusters de destino para ambos os nós como o `-peer-addr`s.

```
src::> cluster peer create -peer-addr <10.161.189.18>
```

4. Introduza e confirme a frase-passe.
5. Verifique se o grupo de instrumentos esteve em contacto.

```
src::> cluster peer show
```

Peering bem-sucedido mostra **disponível** no campo disponibilidade.

6. Crie peering SVM no destino. As SVMs de origem e de destino devem ser SVMs de dados.

```
dest::> vserver peer create -vserver <dest_svm> -peer-vserver <src_svm>  
-peer-cluster <src_cluster> -applications snapmirror``
```

7. Aceitar peering SVM.

```
src::> vserver peer accept -vserver <src_svm> -peer-vserver <dest_svm>
```

8. Verifique se o SVM entrou em Contato.

```
dest::> vserver peer show
```

O estado peer mostra **peered** e os aplicativos de peering mostram **snapmirror**.

Etapas 5: Crie uma relação de replicação do SnapMirror entre o sistema de origem e destino

Esta seção fornece instruções sobre como criar uma relação de replicação do SnapMirror entre o sistema de origem e destino.

Para mover uma relação de replicação existente do SnapMirror, primeiro você deve quebrar a relação de replicação existente do SnapMirror antes de criar uma nova relação de replicação do SnapMirror.

Use a CLI do ONTAP para as etapas a seguir.

Passos

1. Criar um volume protegido de dados no SVM de destino.

```
dest::> vol create -volume <new_dest_vol> -vserver <dest_svm> -type DP  
-size <10GB> -aggregate <aggr1>
```

2. Crie a relação de replicação do SnapMirror no destino, que inclui a política e a programação do SnapMirror para a replicação.

```
dest::> snapmirror create -source-path src_svm:src_vol -destination  
-path dest_svm:new_dest_vol -vserver dest_svm -policy  
MirrorAllSnapshots -schedule 5min
```

3. Inicialize a relação de replicação do SnapMirror no destino.

```
dest::> snapmirror initialize -destination-path <dest_svm:new_dest_vol>
```

4. Na CLI do ONTAP, valide o status do relacionamento do SnapMirror executando o seguinte comando:

```
dest::> snapmirror show
```

O status da relação é `Snapmirrored` e a saúde da relação é `true`.

5. Opcional: Na CLI do ONTAP, execute o seguinte comando para visualizar o histórico de ações para a relação do SnapMirror.

```
dest::> snapmirror show-history
```

Opcionalmente, você pode montar os volumes de origem e destino, gravar um arquivo na origem e verificar se o volume está replicando no destino.

Administração do Google Cloud

Altere o tipo de máquina Google Cloud para Cloud Volumes ONTAP

Você pode escolher entre vários tipos de máquina ao iniciar o Cloud Volumes ONTAP no Google Cloud. Você pode alterar a instância ou o tipo de máquina a qualquer momento se você determinar que ela é subdimensionada ou superdimensionada para suas necessidades.

Sobre esta tarefa

- A giveback automática deve estar ativada num par de HA Cloud Volumes ONTAP (esta é a predefinição). Se não for, então a operação falhará.

["Documentação do ONTAP 9: Comandos para configurar o giveback automático"](#)

- Alterar o tipo de máquina pode afetar as taxas de serviço do Google Cloud.
- A operação reinicia o Cloud Volumes ONTAP.

Para sistemas de nó único, a e/S é interrompida.

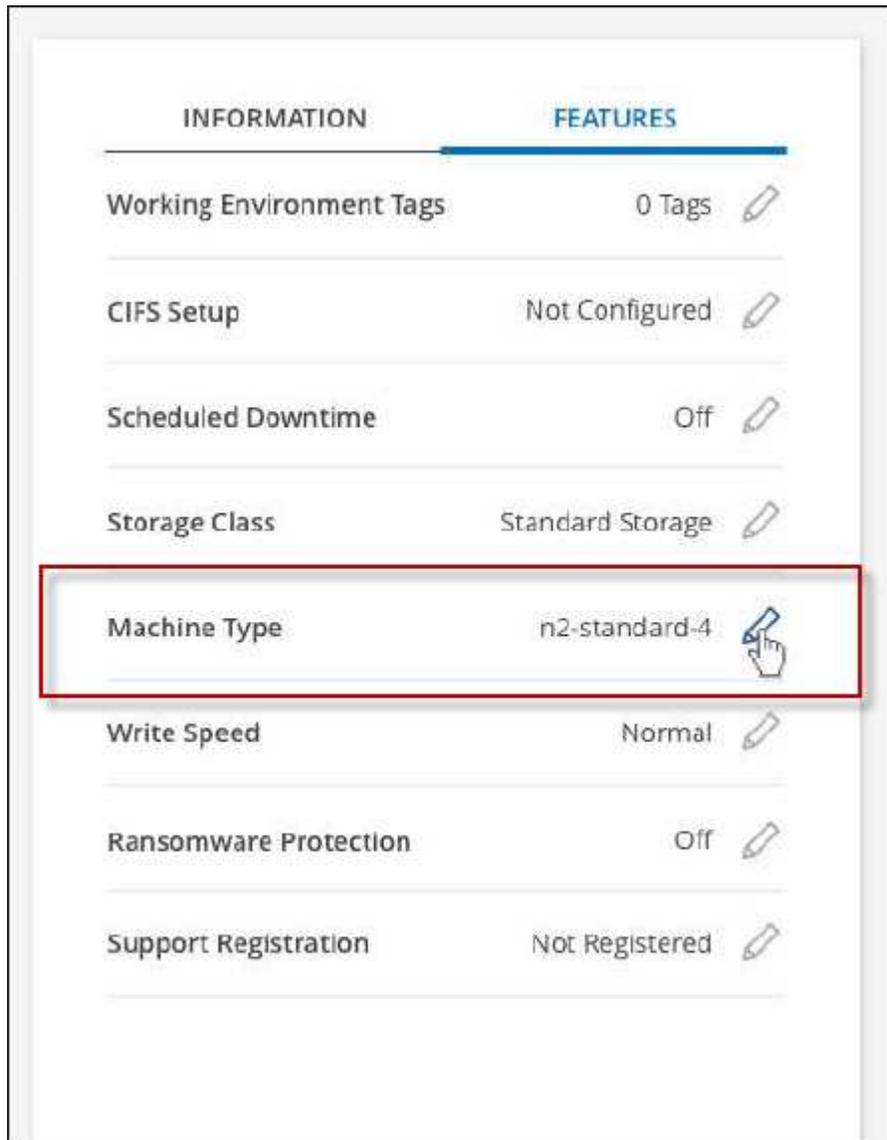
Para pares de HA, a alteração não causa interrupções. Os pares DE HA continuam fornecendo dados.



O BlueXP muda um nó de cada vez, iniciando a aquisição e aguardando a devolução. A equipe de Garantia de qualidade da NetApp testou tanto a escrita quanto a leitura de arquivos durante esse processo e não viu nenhum problema no lado do cliente. À medida que as conexões mudaram, algumas tentativas foram observadas no nível de e/S, mas a camada de aplicação superou a redefinição das conexões NFS/CIFS.

Passos

1. Na página Canvas, selecione o ambiente de trabalho.
2. Na guia Visão geral, clique no painel recursos e, em seguida, clique no ícone de lápis ao lado de **tipo de máquina**.



Se você estiver usando uma licença de pagamento conforme o uso baseada em nó (PAYGO), você pode escolher uma licença e tipo de máquina diferente clicando no ícone de lápis ao lado de **tipo de licença**.

1. Escolha um tipo de máquina, marque a caixa de seleção para confirmar que você entende as implicações da alteração e clique em **alterar**.

Resultado

O Cloud Volumes ONTAP reinicializa com a nova configuração.

Administrar o Cloud Volumes ONTAP usando a visualização avançada

Se você precisar executar o gerenciamento avançado do Cloud Volumes ONTAP, poderá fazê-lo usando o Gerenciador de sistemas do ONTAP, que é uma interface de

gerenciamento fornecida com um sistema ONTAP. Incluímos a interface do Gerenciador de sistema diretamente no BlueXP para que você não precise sair do BlueXP para gerenciamento avançado.

Caraterísticas

A visualização Avançada no BlueXP oferece acesso a recursos de gerenciamento adicionais:

- Gerenciamento avançado de storage

Gerencie grupos de consistência, compartilhamentos, qtrees, cotas e VMs de armazenamento.

- Gerenciamento de rede

Gerencie IPspaces, interfaces de rede, portsets e portas ethernet.

- Eventos e empregos

Ver registros de eventos, alertas do sistema, trabalhos e registros de auditoria.

- Proteção de dados avançada

Proteja VMs de storage, LUNs e grupos de consistência.

- Gerenciamento de host

Configurar grupos de iniciadores SAN e clientes NFS.

Configurações compatíveis

O gerenciamento avançado por meio do ONTAP System Manager é compatível com o Cloud Volumes ONTAP 9.10.0 e posterior em regiões de nuvem padrão.

A integração do System Manager não é suportada nas regiões GovCloud ou em regiões que não têm acesso de saída à Internet.

Limitações

Alguns recursos que aparecem na interface do Gerenciador de sistema não são suportados com o Cloud Volumes ONTAP:

- Disposição em camadas do BlueXP

O serviço de disposição em camadas do BlueXP não é compatível com o Cloud Volumes ONTAP. Ao criar volumes, é necessário configurar a disposição em camadas dos dados para o storage de objetos diretamente da visualização padrão do BlueXP .

- Camadas

O gerenciamento de agregados (incluindo camadas locais e camadas de nuvem) não é compatível com o System Manager. Você precisa gerenciar agregados diretamente da visualização padrão do BlueXP .

- Atualizações de firmware

As atualizações automáticas de firmware a partir da página **Cluster > Settings** não são suportadas com o

Cloud Volumes ONTAP.

Além disso, o controle de acesso baseado em função do System Manager não é suportado.

Como começar

Abra um ambiente de trabalho do Cloud Volumes ONTAP e clique na opção visualização avançada.

Passos

1. No menu de navegação à esquerda, selecione **Storage > Canvas**.
2. Na página tela, selecione um sistema Cloud Volumes ONTAP.
3. No painel direito, em **Serviços**, localize **System Manager** e selecione **Open**.
4. Se a mensagem de confirmação aparecer, leia-a e clique em **Fechar**.
5. Use o Gerenciador do sistema para gerenciar o Cloud Volumes ONTAP.
6. Se necessário, clique em **mudar para a visualização padrão** para retornar ao gerenciamento padrão por meio do BlueXP .

Ajuda com o uso do System Manager

Se precisar de ajuda para usar o Gerenciador de sistema com o Cloud Volumes ONTAP, "[Documentação do ONTAP](#)" consulte para obter instruções passo a passo. Aqui estão alguns links que podem ajudar:

- "[Gerenciamento de volume e LUN](#)"
- "[Gerenciamento de rede](#)"
- "[Proteção de dados](#)"

Administrar o Cloud Volumes ONTAP a partir da CLI

A CLI do Cloud Volumes ONTAP permite executar todos os comandos administrativos e é uma boa escolha para tarefas avançadas ou se você estiver mais confortável usando a CLI. Você pode se conectar à CLI usando o Secure Shell (SSH).

Antes de começar

O host a partir do qual você usa SSH para se conectar ao Cloud Volumes ONTAP deve ter uma conexão de rede com o Cloud Volumes ONTAP. Por exemplo, você pode precisar de SSH de um host jump que esteja na rede do seu provedor de nuvem.



Quando implantadas em vários AZs, as configurações do Cloud Volumes ONTAP HA usam um endereço IP flutuante para a interface de gerenciamento de cluster, o que significa que o roteamento externo não está disponível. Você deve se conectar a partir de um host que faça parte do mesmo domínio de roteamento.

Passos

1. No BlueXP , identifique o endereço IP da interface de gerenciamento de cluster:
 - a. No menu de navegação à esquerda, selecione **Storage > Canvas**.
 - b. Na página tela, selecione o sistema Cloud Volumes ONTAP.
 - c. Copie o endereço IP de gerenciamento de cluster que aparece no painel direito.

- Use SSH para se conectar ao endereço IP da interface de gerenciamento de cluster usando a conta de administrador.

Exemplo

A imagem a seguir mostra um exemplo usando PuTTY:



- No prompt de login, insira a senha da conta de administrador.

Exemplo

```
Password: *****  
COT2::>
```

Saúde do sistema e eventos

Verifique a configuração do AutoSupport

O AutoSupport monitora proativamente a integridade do sistema e envia mensagens para o suporte técnico da NetApp. Por padrão, o AutoSupport está habilitado em cada nó para enviar mensagens para suporte técnico usando o protocolo de transporte HTTPS. É melhor verificar se o AutoSupport pode enviar essas mensagens.

A única etapa de configuração necessária é garantir que o Cloud Volumes ONTAP tenha conectividade de saída à Internet. Para obter detalhes, consulte os requisitos de rede do seu provedor de nuvem.

Requisitos da AutoSupport

Os nós do Cloud Volumes ONTAP exigem acesso de saída à Internet para NetApp AutoSupport, que monitora proativamente a integridade do sistema e envia mensagens para o suporte técnico da NetApp.

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

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

Se uma conexão de saída à Internet não estiver disponível para enviar mensagens AutoSupport, o BlueXP configura automaticamente seus sistemas Cloud Volumes ONTAP para usar o conector como um servidor proxy. O único requisito é garantir que o grupo de segurança do conector permita conexões *inbound* pela porta 3128. Você precisará abrir essa porta depois de implantar o conector.

Se você definiu regras de saída rígidas para o Cloud Volumes ONTAP, também precisará garantir que o grupo de segurança do Cloud Volumes ONTAP permita conexões *de saída* pela porta 3128.

Depois de verificar que o acesso de saída à Internet está disponível, você pode testar o AutoSupport para garantir que ele possa enviar mensagens. Para obter instruções, "[ONTAP docs: Configurar o AutoSupport](#)" consulte .

Solucionar problemas da configuração do AutoSupport

Se uma conexão de saída não estiver disponível e o BlueXP não puder configurar seu sistema Cloud Volumes ONTAP para usar o conector como um servidor proxy, você receberá uma notificação do BlueXP intitulada " Nome do ambiente de trabalho> não consegue enviar mensagens AutoSupport."

Você provavelmente está recebendo essa mensagem por causa de problemas de rede.

Siga estes passos para resolver este problema.

Passos

1. SSH para o sistema Cloud Volumes ONTAP para que você possa administrar o sistema a partir da CLI do ONTAP.

["Saiba como fazer SSH para Cloud Volumes ONTAP"](#).

2. Apresentar o estado detalhado do subsistema AutoSupport:

```
autosupport check show-details
```

A resposta deve ser semelhante à seguinte:

```
Category: smtp
  Component: mail-server
  Status: failed
  Detail: SMTP connectivity check failed for destination:
        mailhost. Error: Could not resolve host -
'mailhost'
  Corrective Action: Check the hostname of the SMTP server

Category: http-https
  Component: http-put-destination
  Status: ok
  Detail: Successfully connected to:
        <https://support.netapp.com/put/AsupPut/>.

  Component: http-post-destination
  Status: ok
  Detail: Successfully connected to:

https://support.netapp.com/asupprod/post/1.0/postAsup.

Category: on-demand
  Component: ondemand-server
  Status: ok
  Detail: Successfully connected to:
        https://support.netapp.com/aods/asupmessage.

Category: configuration
  Component: configuration
  Status: ok
  Detail: No configuration issues found.

5 entries were displayed.
```

Se o status da categoria http-https for "ok", significa que o AutoSupport está configurado corretamente e as mensagens podem ser enviadas.

3. Se o status não estiver ok, verifique o URL do proxy para cada nó do Cloud Volumes ONTAP:

```
autosupport show -fields proxy-url
```

4. Se o parâmetro URL do proxy estiver vazio, configure o Cloud Volumes ONTAP para usar o conector como um proxy:

```
autosupport modify -proxy-url http://<connector private ip>:3128
```

5. Verifique novamente o status do AutoSupport:

```
autosupport check show-details
```

6. Se o status continuar com falha, valide que há conectividade entre o Cloud Volumes ONTAP e o conetor pela porta 3128.
7. Se o ID de status ainda falhar após verificar se há conectividade, SSH para o conetor.

["Saiba mais sobre como conetar-se à VM Linux para o conetor"](#)

8. Vá para `/opt/application/netapp/cloudmanager/docker_occm/data/`
9. Abra o arquivo de configuração do proxy `squid.conf`

A estrutura básica do arquivo é a seguinte:

```
http_port 3128
acl localnet src 172.31.0.0/16
acl azure_aws_metadata dst 169.254.169.254

http_access allow localnet
http_access deny azure_aws_metadata
http_access allow localhost
http_access deny all
```

O valor `src localnet` é o CIDR do sistema Cloud Volumes ONTAP.

10. Se o bloco CIDR do sistema Cloud Volumes ONTAP não estiver no intervalo especificado no arquivo, atualize o valor ou adicione uma nova entrada da seguinte forma:

```
acl cvonet src <cidr>
```

Se você adicionar esta nova entrada, não se esqueça de adicionar também uma entrada permitir:

```
http_access allow cvonet
```

Aqui está um exemplo:

```
http_port 3128
acl localnet src 172.31.0.0/16
acl cvonet src 172.33.0.0/16
acl azure_aws_metadata dst 169.254.169.254

http_access allow localnet
http_access allow cvonet
http_access deny azure_aws_metadata
http_access allow localhost
http_access deny all
```

11. Depois de editar o arquivo de configuração, reinicie o contentor proxy como `sudo`:

```
docker restart squid
```

12. Volte para a CLI do Cloud Volumes ONTAP e verifique se o Cloud Volumes ONTAP pode enviar mensagens do AutoSupport:

```
autosupport check show-details
```

Configurar o EMS

O sistema de Gestão de Eventos (EMS) recolhe e apresenta informações sobre eventos que ocorrem em sistemas ONTAP. Para receber notificações de eventos, você pode definir destinos de eventos (endereços de e-mail, hosts de intercetação SNMP ou servidores syslog) e rotas de eventos para uma determinada gravidade de evento.

Você pode configurar o EMS usando a CLI. Para obter instruções, ["ONTAP docs: Visão geral da configuração do EMS"](#) consulte .

Conceitos

Licenciamento

Licenciamento 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.

Visão geral do licenciamento

As opções de licenciamento a seguir estão disponíveis para novos clientes.

Licenciamento baseado em capacidade

Pague por vários sistemas Cloud Volumes ONTAP na sua conta do NetApp por capacidade provisionada. Inclui a capacidade de adquirir serviços de dados de nuvem complementares.

Inscrição no Keystone

Um serviço baseado em subscrição com pagamento conforme o uso que proporciona uma experiência otimizada de nuvem híbrida para pares de alta disponibilidade (HA).

As seções a seguir fornecem mais detalhes sobre cada uma dessas opções.



O suporte não está disponível para o uso de recursos licenciados sem uma licença.

Licenciamento baseado em capacidade

Os pacotes de licenciamento baseados em capacidade permitem que você pague por Cloud Volumes ONTAP por TIB de capacidade. A licença está associada à sua conta NetApp e permite que você carregue vários sistemas contra a licença, contanto que a capacidade suficiente esteja disponível através da licença.

Por exemplo, você pode comprar uma única licença TIB de 20 TB, implantar quatro sistemas Cloud Volumes ONTAP e alocar um volume de TIB de 5 TB para cada sistema, totalizando 20 TIB. A capacidade está disponível para os volumes em cada sistema Cloud Volumes ONTAP implantado nessa conta.

O licenciamento baseado em capacidade está disponível na forma de um *pacote*. Ao implantar um sistema Cloud Volumes ONTAP, você pode escolher entre vários pacotes de licenciamento com base nas necessidades da sua empresa.



Embora o uso real e a medição dos produtos e serviços gerenciados no BlueXP sejam sempre calculados em GiB e TIB, os termos GB/GiB e TB/TIB são usados de forma intercambiável. Isso é refletido nas listagens do Cloud Marketplace, cotações de preços, descrições de listagem e em outra documentação de suporte.

Pacotes

Os seguintes pacotes baseados em capacidade estão disponíveis para o Cloud Volumes ONTAP.

Para obter uma lista de tipos de VM suportados com os seguintes pacotes baseados em capacidade, consulte:

- ["Configurações compatíveis no Azure"](#)
- ["Configurações compatíveis no Google Cloud"](#)

Freemium

Fornecer todos os recursos do Cloud Volumes ONTAP gratuitamente da NetApp (taxas de provedor de nuvem ainda se aplicam).

- Nenhuma licença ou contrato é necessário.
- O suporte do NetApp não está incluído.
- Você está limitado a 500 GiB de capacidade provisionada por sistema Cloud Volumes ONTAP.
- Você pode usar até 10 sistemas Cloud Volumes ONTAP com a oferta Freemium por conta NetApp, em qualquer provedor de nuvem.
- Se a capacidade provisionada para um sistema Cloud Volumes ONTAP exceder 500 GiB, o BlueXP converte o sistema no pacote Essentials.

Assim que um sistema é convertido para o pacote Essentials, o [carga mínima](#) aplica-se.

Quaisquer outros sistemas que tenham menos de 500 GiB de capacidade provisionada permanecem no Freemium (desde que sejam implantados usando a oferta do Freemium).

Essenciais

Você pode pagar por capacidade em várias configurações diferentes:

- Escolha sua configuração do Cloud Volumes ONTAP:
 - Um único nó ou sistema de HA
 - Storage de arquivos e blocos ou dados secundários para recuperação de desastres (DR)
- Adicione qualquer um dos serviços de dados de nuvem da NetApp a um custo extra

Para obter mais informações, ["Mais sobre licenças baseadas em capacidade"](#) consulte .

Otimizado

Pague por operações de e/S e capacidade provisionadas separadamente.

- Nó único ou HA da Cloud Volumes ONTAP
- O carregamento baseia-se em dois componentes de custo: Armazenamento e utilização (e/S).

Você não será cobrado por e/S relacionadas à replicação de dados (SnapMirror), backups (SnapVault) ou NDMP.

- Disponível no Azure Marketplace como uma oferta de pagamento conforme o uso ou como um contrato anual
- Disponível no Google Cloud Marketplace como uma oferta de pagamento conforme o uso ou como um contrato anual
- Adicione qualquer um dos serviços de dados de nuvem da NetApp a um custo extra

Profissional

Pague por capacidade por qualquer tipo de configuração Cloud Volumes ONTAP com backups ilimitados.

- Fornece licenciamento para qualquer configuração do Cloud Volumes ONTAP

Nó único ou HA com carregamento de capacidade para volumes primários e secundários à mesma taxa

- Inclui backups de volume ilimitados usando backup e recuperação do BlueXP , mas apenas para sistemas Cloud Volumes ONTAP que usam o pacote profissional.



É necessária uma subscrição de pagamento conforme o uso (PAYGO) para a recuperação e o backup do BlueXP , no entanto, não haverá cobrança pelo uso deste serviço. Para obter mais informações sobre como configurar o licenciamento para backup e recuperação do BlueXP , ["Configure o licenciamento para backup e recuperação do BlueXP "](#) consulte .

- Adicione qualquer um dos serviços de dados de nuvem da NetApp a um custo extra

Como começar

Saiba como começar a usar o licenciamento baseado em capacidade:

- ["Configure o licenciamento para o Cloud Volumes ONTAP na AWS"](#)
- ["Configure o licenciamento para o Cloud Volumes ONTAP no Azure"](#)
- ["Configure o licenciamento para o Cloud Volumes ONTAP no Google Cloud"](#)

Inscrição no Keystone

Um serviço baseado em subscrição com pagamento conforme o uso que oferece uma experiência de nuvem híbrida otimizada para quem prefere modelos de consumo de despesas operacionais para CapEx adiantado ou aluguel.

O carregamento é baseado no tamanho da sua capacidade comprometida com um ou mais pares de HA da Cloud Volumes ONTAP na assinatura do Keystone.

A capacidade provisionada para cada volume é agregada e comparada com a capacidade comprometida periodicamente na sua assinatura do Keystone, e quaisquer excedentes são cobrados como o pico da sua assinatura do Keystone.

["Saiba mais sobre o NetApp Keystone"](#).

Configurações compatíveis

As assinaturas do Keystone são compatíveis com pares de HA. Esta opção de licenciamento não é suportada com sistemas de nó único no momento.

Limite de capacidade

Cada sistema Cloud Volumes ONTAP individual dá suporte a até 2 PIB de capacidade por meio de discos e disposição em camadas no storage de objetos.

Como começar

Saiba como começar a usar uma assinatura do Keystone:

- ["Configure o licenciamento para o Cloud Volumes ONTAP na AWS"](#)
- ["Configure o licenciamento para o Cloud Volumes ONTAP no Azure"](#)
- ["Configure o licenciamento para o Cloud Volumes ONTAP no Google Cloud"](#)

Licenciamento baseado em nó

O licenciamento baseado em nó é o modelo de licenciamento da geração anterior que permitiu licenciar o Cloud Volumes ONTAP por nó. Este modelo de licenciamento não está disponível para novos clientes. O carregamento por nó foi substituído pelos métodos de carregamento por capacidade adicional descritos acima.

A NetApp planejou o fim da disponibilidade (EOA) e o suporte (EOS) do licenciamento baseado em nós. Após a EOA e a EOS, as licenças baseadas em nós precisarão ser convertidas em licenças baseadas em capacidade.

Para obter informações, ["Comunicado do cliente: CPC-00589"](#) consulte .

Término da disponibilidade de licenças baseadas em nós

A partir de 11 de novembro de 2024, a disponibilidade limitada de licenças baseadas em nós foi encerrada. O suporte para licenciamento baseado em nós termina em 31 de dezembro de 2024.

Se você tiver um contrato válido baseado em nós que se estende além da data EOA, você pode continuar a usar a licença até que o contrato expire. Uma vez que o contrato expirar, será necessário fazer a transição para o modelo de licenciamento baseado em capacidade. Se não tiver um contrato de longo prazo para um nó Cloud Volumes ONTAP, é importante planejar a sua conversão antes da data EOS.

Saiba mais sobre cada tipo de licença e o impactos da EOA sobre ele a partir desta tabela:

Tipo de licença	Impacto após EOA
Licença válida baseada em nó adquirida por meio do bring Your own license (BYOL)	A licença permanece válida até a expiração. As licenças não utilizadas existentes baseadas em nós podem ser usadas para implantar novos sistemas Cloud Volumes ONTAP.
Licença baseada em nó expirada adquirida por meio do BYOL	Você não terá o direito de implantar novos sistemas Cloud Volumes ONTAP usando esta licença. Os sistemas existentes podem continuar a funcionar, mas não receberá qualquer suporte ou atualizações para os seus sistemas após a data EOS.
Licença válida baseada em nó com assinatura PAYGO	Deixará de receber o suporte NetApp após a data EOS, até que faça a transição para uma licença baseada em capacidade.

Exclusões

A NetApp reconhece que certas situações exigem consideração especial, e a EOA e EOS de licenciamento baseado em nós não se aplicarão aos seguintes casos:

- Clientes do setor público dos EUA

- Implantações em modo privado
- Implementações da região da China do Cloud Volumes ONTAP na AWS

Para esses cenários específicos, a NetApp oferecerá suporte para atender aos requisitos exclusivos de licenciamento em conformidade com as obrigações contratuais e as necessidades operacionais.



Mesmo nesses cenários, novas licenças baseadas em nós e renovações de licença são válidas por um máximo de um ano a partir da data de aprovação.

Conversão de licença

O BlueXP permite uma conversão contínua de licenças baseadas em nós para capacidade com base na ferramenta de conversão de licenças. Para obter informações sobre a EOA do licenciamento baseado em nós, "[Término da disponibilidade de licenças baseadas em nós](#)" consulte .

Antes da transição, é bom se familiarizar com a diferença entre os dois modelos de licenciamento. O licenciamento baseado em nó inclui capacidade fixa para cada instância do ONTAP, o que pode restringir a flexibilidade. O licenciamento baseado em capacidade, por outro lado, permite um pool compartilhado de storage em várias instâncias, oferecendo maior flexibilidade, otimizando a utilização de recursos e reduzindo o potencial de penalidades financeiras ao redistribuir cargas de trabalho. O carregamento baseado em capacidade ajusta-se perfeitamente às mudanças nos requisitos de armazenamento.

Para saber como pode efetuar esta conversão, "[Converta licenças baseadas em nós em capacidade](#)" consulte .



A conversão de um sistema de licenças baseadas em capacidade para licenças baseadas em nós não é suportada.

Saiba mais sobre licenças baseadas em capacidade

Você deve estar familiarizado com o carregamento e uso de capacidade para licenças baseadas em capacidade

Modelos de consumo

Pacotes de licenciamento baseados em capacidade estão disponíveis com os seguintes modelos de consumo:

- **BYOL:** Traga sua própria licença (BYOL). Uma licença adquirida na NetApp que pode ser usada para implantar o Cloud Volumes ONTAP em qualquer provedor de nuvem.

Observe que o pacote otimizado não está disponível com o BYOL.

- **PAYGO:** Uma assinatura paga conforme o uso (PAYGO) é uma assinatura por hora do mercado do seu provedor de nuvem.
- **Anual:** Um contrato anual do mercado do seu provedor de nuvem.

Observe o seguinte:

- Se você adquirir uma licença da NetApp (BYOL), também precisará assinar a oferta PAYGO no mercado do seu provedor de nuvem.

Sua licença sempre será cobrada primeiro, mas você será cobrado pela taxa por hora no mercado nestes casos:

- Se você exceder sua capacidade licenciada
- Se o prazo da sua licença expirar
- Se você tiver um contrato anual de um mercado, *All Cloud Volumes ONTAP* sistemas que você implantar serão cobrados contra esse contrato. Você não pode misturar e combinar um contrato de mercado anual com o BYOL.
- Somente sistemas de nó único com BYOL são compatíveis nas regiões da China.

Mudando pacotes

Após a implantação, você pode alterar o pacote de um sistema Cloud Volumes ONTAP que usa licenciamento baseado em capacidade. Por exemplo, se você implantou um sistema Cloud Volumes ONTAP com o pacote Essentials, poderá alterá-lo para o pacote Professional se a sua empresa precisar ser alterada.

["Saiba como alterar os métodos de carregamento"](#).

Para obter informações sobre como converter licenças baseadas em nós para baseadas em capacidade, consulte

Preços e configurações compatíveis

Para obter detalhes sobre preços, ["Site da NetApp BlueXP"](#) visite .

Pacotes de licenciamento baseados em capacidade estão disponíveis com o Cloud Volumes ONTAP 9,7 e versões posteriores.

VMs de storage

- Não há custos adicionais de licenciamento para VMs de storage de fornecimento de dados (SVMs) adicionais, mas há uma cobrança de capacidade mínima de 4 TIB por SVM de fornecimento de dados.
- As SVMs de recuperação de desastres são cobradas de acordo com a capacidade provisionada.

Pares HA

Para pares de HA, você só será cobrado pela capacidade provisionada em um nó. Você não será cobrado pelos dados espelhados de forma síncrona para o nó do parceiro.

FlexClone e FlexCache volumes

- Não será cobrado pela capacidade usada pelo FlexClone volumes.
- Os volumes FlexCache de origem e destino são considerados dados primários e cobrados de acordo com o espaço provisionado.

Limite de capacidade

Com esse modelo de licenciamento, cada sistema Cloud Volumes ONTAP individual dá suporte a até 2 PIB de capacidade por meio de discos e disposição em camadas no storage de objetos.

Não há limite máximo de capacidade quando se trata da própria licença.

Número máximo de sistemas

Com o licenciamento baseado em capacidade, o número máximo de sistemas Cloud Volumes ONTAP é limitado a 20 por conta do NetApp. Um *System* é um par de HA do Cloud Volumes ONTAP, um sistema de nó único do Cloud Volumes ONTAP ou quaisquer VMs de storage adicionais que você criar. A VM de armazenamento padrão não conta com o limite. Este limite aplica-se a todos os modelos de licenciamento.

Por exemplo, digamos que você tenha três ambientes de trabalho:

- Um sistema Cloud Volumes ONTAP de nó único com uma VM de storage (essa é a VM de storage padrão criada quando você implanta o Cloud Volumes ONTAP)

Este ambiente de trabalho conta como um sistema.

- Um sistema Cloud Volumes ONTAP de nó único com duas VMs de storage (a VM de storage padrão e uma VM de storage adicional criada por você)

Esse ambiente de trabalho conta como dois sistemas: Um para o sistema de nó único e outro para a VM de storage adicional.

- Um par de HA do Cloud Volumes ONTAP com três VMs de storage (a VM de storage padrão e duas VMs de storage adicionais criadas por você)

Esse ambiente de trabalho conta como três sistemas: Um para o par de HA e dois para as VMs de storage adicionais.

São seis sistemas no total. Você teria então espaço para um sistema 14 adicional em sua conta.

Se você tiver uma implantação grande que exija mais de 20 sistemas, entre em Contato com o representante de sua conta ou com a equipe de vendas.

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

Notas sobre o carregamento

Os detalhes a seguir podem ajudá-lo a entender como o carregamento funciona com licenciamento baseado em capacidade.

Carga mínima

Há uma cobrança mínima de 4 TIB para cada VM de storage de fornecimento de dados que tenha pelo menos um volume primário (leitura-gravação). Se a soma dos volumes primários for inferior a 4 TIB, o BlueXP aplicará a carga mínima de 4 TIB a essa VM de armazenamento.

Se você ainda não provisionou nenhum volume, a cobrança mínima não se aplica.

Para o pacote Essentials, a taxa de capacidade mínima de 4 TIB não se aplica a VMs de armazenamento que contêm apenas volumes secundários (proteção de dados). Por exemplo, se você tiver uma VM de storage com 1 TIB de dados secundários, então você será cobrado apenas por 1 TIB de dados. Com todos os outros tipos de pacotes não essenciais (otimizado e profissional), a capacidade mínima de carregamento de 4 TIB aplica-se independentemente do tipo de volume.

Excesso de idade

Se você exceder sua capacidade BYOL ou se sua licença expirar, será cobrado por excesso de idade à taxa

por hora com base na assinatura do marketplace.

Pacote Essentials

Com o pacote Essentials, você é cobrado pelo tipo de implantação (HA ou nó único) e pelo tipo de volume (primário ou secundário). Os preços de alta para baixa estão na seguinte ordem: *Essentials Primary HA*, *Essentials Primary Single Node*, *Essentials Secondary HA* e *Essentials Secondary Single Node*. Como alternativa, quando você compra um contrato de mercado ou aceita uma oferta privada, as taxas de capacidade são as mesmas para qualquer tipo de implantação ou volume.

O licenciamento é baseado inteiramente no tipo de volume criado nos sistemas Cloud Volumes ONTAP:

- Nó único Essentials: Volumes de leitura/gravação criados em um sistema Cloud Volumes ONTAP usando apenas um nó ONTAP.
- Essentials HA: Volumes de leitura/gravação usando dois nós de ONTAP que podem fazer failover uns para os outros para acesso a dados sem interrupções.
- Nó único secundário do Essentials: Volumes do tipo de proteção de dados (normalmente volumes de destino SnapMirror ou SnapVault que são somente leitura) criados em um sistema Cloud Volumes ONTAP usando apenas um nó ONTAP.



Se um volume somente leitura/DP se tornar um volume primário, o BlueXP o considera como dados primários e os custos de carregamento são calculados com base no tempo em que o volume estava no modo de leitura/gravação. Quando o volume é novamente feito somente leitura/DP, a BlueXP considera-o como dados secundários novamente e cobra de acordo com a licença mais adequada na carteira digital.

- Essentials secundário HA: Volumes do tipo de proteção de dados (DP) (normalmente volumes de destino SnapMirror ou SnapVault somente leitura) criados em um sistema Cloud Volumes ONTAP usando dois nós de ONTAP que podem fazer failover entre si para acesso a dados sem interrupções.

Observe estes pontos:

- Cobrança mínima: Há uma cobrança mínima de 4 TIB para cada VM de storage de fornecimento de dados que tenha pelo menos um volume primário (leitura-gravação). Para o pacote Essentials, essa cobrança mínima não se aplica às VMs de storage somente com volumes secundários (proteção de dados).
- Excedentes: Se a capacidade licenciada for excedida, os excedentes são cobrados pelas taxas de mercado, com preferência pela utilização da capacidade disponível de outras licenças em primeiro lugar.
- FlexClone e FlexCache volumes: O FlexClone volumes não é cobrado. Os volumes FlexCache de origem e destino são considerados dados primários e são cobrados de acordo com o espaço provisionado.
- Carregamento de pares HA: Para pares de HA, somente a capacidade provisionada em um nó é cobrada. Os dados espelhados de forma síncrona para o nó do parceiro não são cobrados.

BYOL

Se você comprou uma licença Essentials da NetApp (BYOL) e exceder a capacidade licenciada para esse tipo de implantação e volume, a carteira digital da BlueXP cobra sobretaxas a uma licença Essentials de preço mais alto (se você tiver uma e houver capacidade disponível). Isso acontece porque primeiro usamos a capacidade disponível que você já comprou como capacidade pré-paga antes de cobrar no mercado. Se não houver capacidade disponível com sua licença BYOL, a capacidade excedida será cobrada nas taxas horárias sob demanda do mercado (PAYGO) e adicionará custos à sua fatura mensal.

Aqui está um exemplo. Digamos que você tenha as seguintes licenças para o pacote Essentials:

- Uma licença 500 TIB *Essentials Secondary HA* que tem 500 TIB de capacidade comprometida
- Uma licença de nó único TIB *_Essentials* de 500 TIB que tenha apenas 100 TIB de capacidade comprometida

Outro 50 TIB é provisionado em um par de HA com volumes secundários. Em vez de cobrar esse 50 TIB ao PAYGO, a carteira digital BlueXP cobra o excesso de TIB de 50 TIB contra a licença *Essentials Single Node*. Essa licença tem um preço superior ao *Essentials Secondary HA*, mas está fazendo uso de uma licença que você já comprou, e não adicionará custos à sua conta mensal.

Na carteira digital BlueXP, esse 50 TIB será mostrado como cobrado com a licença *Essentials Single Node*.

Aqui está outro exemplo. Digamos que você tenha as seguintes licenças para o pacote Essentials:

- Uma licença 500 TIB *Essentials Secondary HA* que tem 500 TIB de capacidade comprometida
- Uma licença de nó único TIB *_Essentials* de 500 TIB que tenha apenas 100 TIB de capacidade comprometida

Outro 100 TIB é provisionado em um par de HA com volumes primários. A licença que você comprou não tem a capacidade comprometida *Essentials Primary HA*. A licença *Essentials Primary HA* tem um preço superior às licenças *Essentials Primary Single Node* e *Essentials Secondary HA*.

Neste exemplo, a carteira digital BlueXP cobra sobretaxas à taxa de mercado para os 100 TIB adicionais. As taxas de excesso de idade aparecerão na sua conta mensal.

Contratos de mercado ou ofertas privadas

Se você comprou uma licença Essentials como parte de um contrato de mercado ou uma oferta privada, a lógica BYOL não se aplica e você deve ter o tipo de licença exato para o uso. O tipo de licença inclui o tipo de volume (primário ou secundário) e o tipo de implantação (HA ou nó único).

Por exemplo, digamos que você implante uma instância do Cloud Volumes ONTAP com a licença Essentials. Depois, você provisiona volumes de leitura e gravação (nó único primário) e volumes somente leitura (nó único secundário). Seu contrato de mercado ou oferta privada deve incluir capacidade para *Essentials Single Node* e *Essentials Secondary Single Node* para cobrir a capacidade provisionada. Qualquer capacidade provisionada que não faça parte do seu contrato de mercado ou oferta privada será cobrada de acordo com as taxas por hora sob demanda (PAYGO) e adicionará custos à sua fatura mensal.

Armazenamento

Protocolos do cliente

O Cloud Volumes ONTAP dá suporte aos protocolos de clientes iSCSI, NFS, SMB, NVMe-TCP e S3.

iSCSI

iSCSI é um protocolo de bloco que pode ser executado em redes Ethernet padrão. A maioria dos sistemas operacionais cliente oferece um iniciador de software que é executado em uma porta Ethernet padrão.

NFS

NFS é o protocolo de acesso a arquivos tradicional para sistemas UNIX e LINUX. Os clientes podem acessar arquivos em volumes ONTAP usando os protocolos NFSv3, NFSv4 e NFSv4.1. Você pode controlar o acesso

a arquivos usando permissões de estilo UNIX, permissões de estilo NTFS ou uma combinação de ambos.

Os clientes podem acessar os mesmos arquivos usando os protocolos NFS e SMB.

SMB

SMB é o protocolo tradicional de acesso a arquivos para sistemas Windows. Os clientes podem acessar arquivos em volumes ONTAP usando os protocolos SMB 2,0, SMB 2,1, SMB 3,0 e SMB 3.1.1. Assim como no NFS, uma combinação de estilos de permissão é compatível.

S3

O Cloud Volumes ONTAP é compatível com o S3 como opção para storage com escalabilidade horizontal. O suporte ao protocolo S3 permite configurar o acesso de cliente S3 a objetos contidos em um bucket em uma VM de storage (SVM).

["Saiba como o multiprotocolo S3 funciona"](#). ["Saiba como configurar e gerenciar serviços de armazenamento de objetos S3 no ONTAP"](#).

NVMe-TCP

A partir da versão 9.12.1 do ONTAP, o NVMe-TCP é compatível com provedores de nuvem. O BlueXP não oferece recursos de gerenciamento para NVMe-TCP.

Para obter mais informações sobre como configurar o NVMe por meio do ONTAP, ["Configurar uma VM de storage para NVMe"](#) consulte .

Discos e agregados

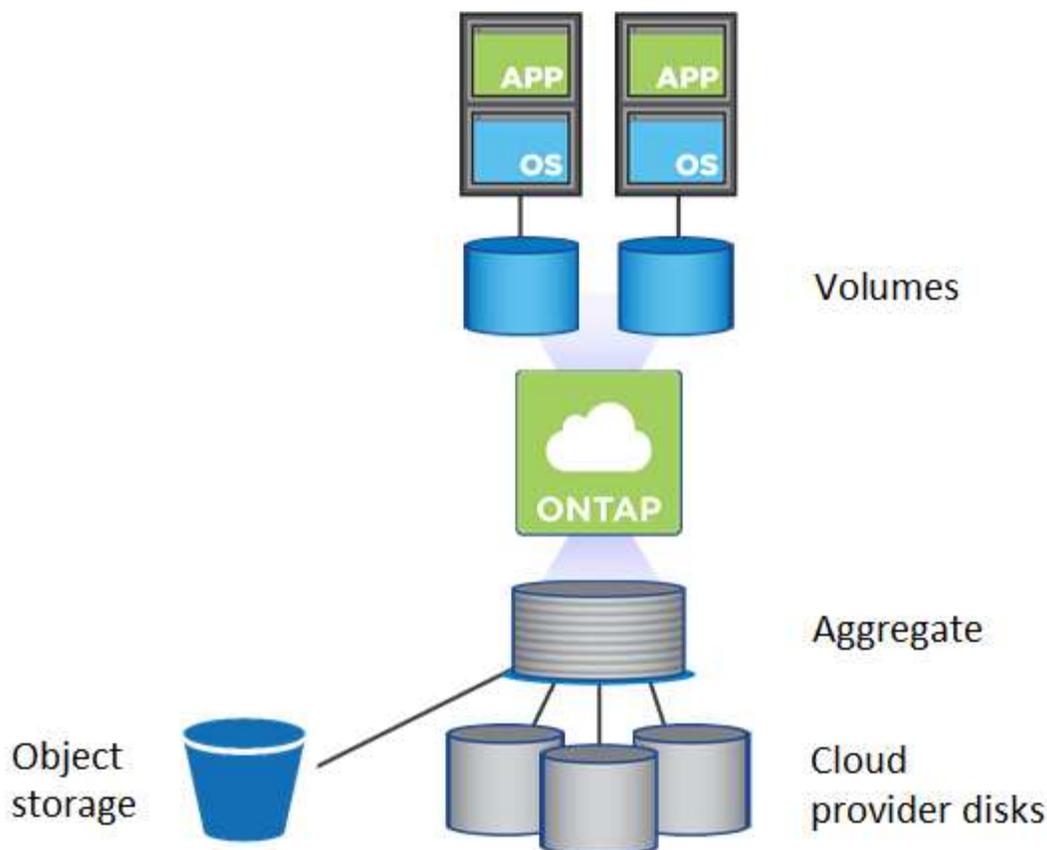
Entender como o Cloud Volumes ONTAP usa o storage de nuvem pode ajudar você a entender seus custos de storage.



Todos os discos e agregados devem ser criados e excluídos diretamente do BlueXP . Você não deve executar essas ações de outra ferramenta de gerenciamento. Isso pode afetar a estabilidade do sistema, dificultar a capacidade de adicionar discos no futuro e, potencialmente, gerar taxas redundantes de provedores de nuvem.

Visão geral

A Cloud Volumes ONTAP usa o storage de fornecedor de nuvem como discos e os agrupa em uma ou mais agregados. Agregados fornecem storage para um ou mais volumes.



Vários tipos de discos de nuvem são suportados. Você escolhe o tipo de disco ao criar um volume e o tamanho de disco padrão ao implantar o Cloud Volumes ONTAP.



A quantidade total de storage comprada de um fornecedor de nuvem é a *capacidade bruta*. A *capacidade utilizável* é menor porque aproximadamente 12 a 14% é sobrecarga reservada para uso Cloud Volumes ONTAP. Por exemplo, se o BlueXP criar um agregado de 500 GiB, a capacidade utilizável será de 442,94 GiB.

Storage da AWS

Na AWS, o Cloud Volumes ONTAP usa o armazenamento EBS para dados de usuário e armazenamento NVMe local como Flash Cache em alguns tipos de instâncias do EC2.

Armazenamento EBS

Na AWS, um agregado pode conter até 6 discos com o mesmo tamanho. Mas se você tiver uma configuração que suporte o recurso volumes elásticos do Amazon EBS, um agregado pode conter até 8 discos. ["Saiba mais sobre o suporte para volumes elásticos"](#).

O tamanho máximo do disco é de 16 TiB.

O tipo de disco EBS subjacente pode ser SSDs de uso geral (GP3 ou GP2), SSD IOPS provisionado (IO1) ou HDD otimizado para throughput (st1). Você pode emparelhar um disco EBS com o Amazon S3 para ["categorize os dados inativos em storage de objetos de baixo custo"](#).



A disposição em camadas dos dados no storage de objetos não é recomendada quando se usa HDDs otimizados para taxa de transferência (st1).

Storage NVMe local

Alguns tipos de instâncias do EC2 incluem storage NVMe local, que o Cloud Volumes ONTAP usa como "Flash Cache".

- [Ligações relacionadas*](#)
- ["Documentação da AWS: Tipos de volume do EBS"](#)
- ["Saiba como escolher tipos de disco e tamanhos de disco para seus sistemas na AWS"](#)
- ["Analisar os limites de armazenamento do Cloud Volumes ONTAP na AWS"](#)
- ["Revise as configurações compatíveis do Cloud Volumes ONTAP na AWS"](#)

Storage Azure

No Azure, um agregado pode conter até 12 discos com o mesmo tamanho. O tipo de disco e o tamanho máximo do disco dependem se você usa um sistema de nó único ou um par de HA:

Sistemas de nó único

Os sistemas de nó único podem usar esses tipos de discos gerenciados do Azure:

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

Cada tipo de disco gerenciado tem um tamanho máximo de disco de 32 TIB.

É possível emparelhar um disco gerenciado com o storage Azure Blob ao ["categorize os dados inativos em storage de objetos de baixo custo"](#).

Pares HA

Os pares DE HA usam dois tipos de discos que oferecem alto desempenho para workloads com uso intenso de e/S a um custo mais alto:

- *Blobs de página Premium* com um tamanho máximo de disco de 8 TIB
- *Managed Disks* com um tamanho máximo de disco de 32 TIB
- [Ligações relacionadas*](#)
- ["Saiba como escolher tipos de disco e tamanhos de disco para seus sistemas no Azure"](#)
- ["Lançamento de um par de HA do Cloud Volumes ONTAP no Azure"](#)
- ["Documentação do Microsoft Azure: Tipos de disco gerenciados do Azure"](#)
- ["Documentação do Microsoft Azure: Visão geral dos blobs de páginas do Azure"](#)
- ["Analisar os limites de armazenamento do Cloud Volumes ONTAP no Azure"](#)

Storage do Google Cloud

No Google Cloud, um agregado pode conter até 6 discos com o mesmo tamanho. O tamanho máximo do disco é de 64 TIB.

O tipo de disco pode ser *Zonal SSD Persistent Disks*, *Zonal Balanced Persistent Disks* ou *Zonal Standard Persistent Disks*. É possível emparelhar discos persistentes com um bucket do Google Storage ao "[categorize os dados inativos em storage de objetos de baixo custo](#)".

- [Ligações relacionadas*](#)
- ["Documentação do Google Cloud: Opções de armazenamento"](#)
- ["Análise os limites de armazenamento do Cloud Volumes ONTAP no Google Cloud"](#)

Tipo de RAID

O tipo RAID para cada agregado Cloud Volumes ONTAP é RAID0 (striping). A Cloud Volumes ONTAP conta com o fornecedor de nuvem para disponibilidade e durabilidade de disco. Nenhum outro tipo de RAID é suportado.

Peças sobressalentes quentes

O RAID0 não suporta o uso de hot spares para redundância.

A criação de discos não utilizados (hot spares) anexados a uma instância do Cloud Volumes ONTAP é uma despesa desnecessária e pode impedir o provisionamento de espaço adicional conforme necessário. Portanto, não é recomendado.

Volumes elásticos na AWS

O suporte ao recurso volumes elásticos do Amazon EBS com um agregado Cloud Volumes ONTAP fornece melhor desempenho e capacidade adicional, ao mesmo tempo que permite que o BlueXP aumente automaticamente a capacidade de disco subjacente conforme necessário.

Benefícios

- Crescimento dinâmico de disco

O BlueXP pode aumentar dinamicamente o tamanho dos discos enquanto o Cloud Volumes ONTAP está em execução e enquanto os discos ainda estão conectados.

- Melhor desempenho

Os agregados habilitados com volumes elásticos podem ter até oito discos que são igualmente utilizados em dois grupos RAID. Essa configuração fornece mais taxa de transferência e performance consistente.

- Agregados maiores

O suporte para oito discos oferece uma capacidade agregada máxima de 128 TIB. Esses limites são maiores que o limite de seis discos e o limite de 96 TIB para agregados que não estão habilitados com o recurso volumes elásticos.

Observe que os limites totais de capacidade do sistema permanecem os mesmos.

Configurações compatíveis

O recurso volumes elásticos do Amazon EBS é compatível com versões específicas do Cloud Volumes ONTAP e tipos de disco EBS específicos.

Versão Cloud Volumes ONTAP

O recurso Elastic volumes é suportado com *new* sistemas Cloud Volumes ONTAP criados a partir da versão 9.11.0 ou posterior. O recurso é *não* suportado com sistemas Cloud Volumes ONTAP existentes que foram implantados antes de 9.11.0.

Por exemplo, o recurso volumes elásticos não é suportado se você criou um sistema Cloud Volumes ONTAP 9.9.0 e, em seguida, atualizou esse sistema para a versão 9.11.0. Deve ser um novo sistema implantado usando a versão 9.11.0 ou posterior.

Tipos de disco EBS

O recurso volumes elásticos é ativado automaticamente no nível agregado ao usar SSDs de uso geral (GP3) ou SSDs IOPS provisionados (IO1). O recurso volumes elásticos não é compatível com agregados que usam qualquer outro tipo de disco.

Permissões AWS necessárias

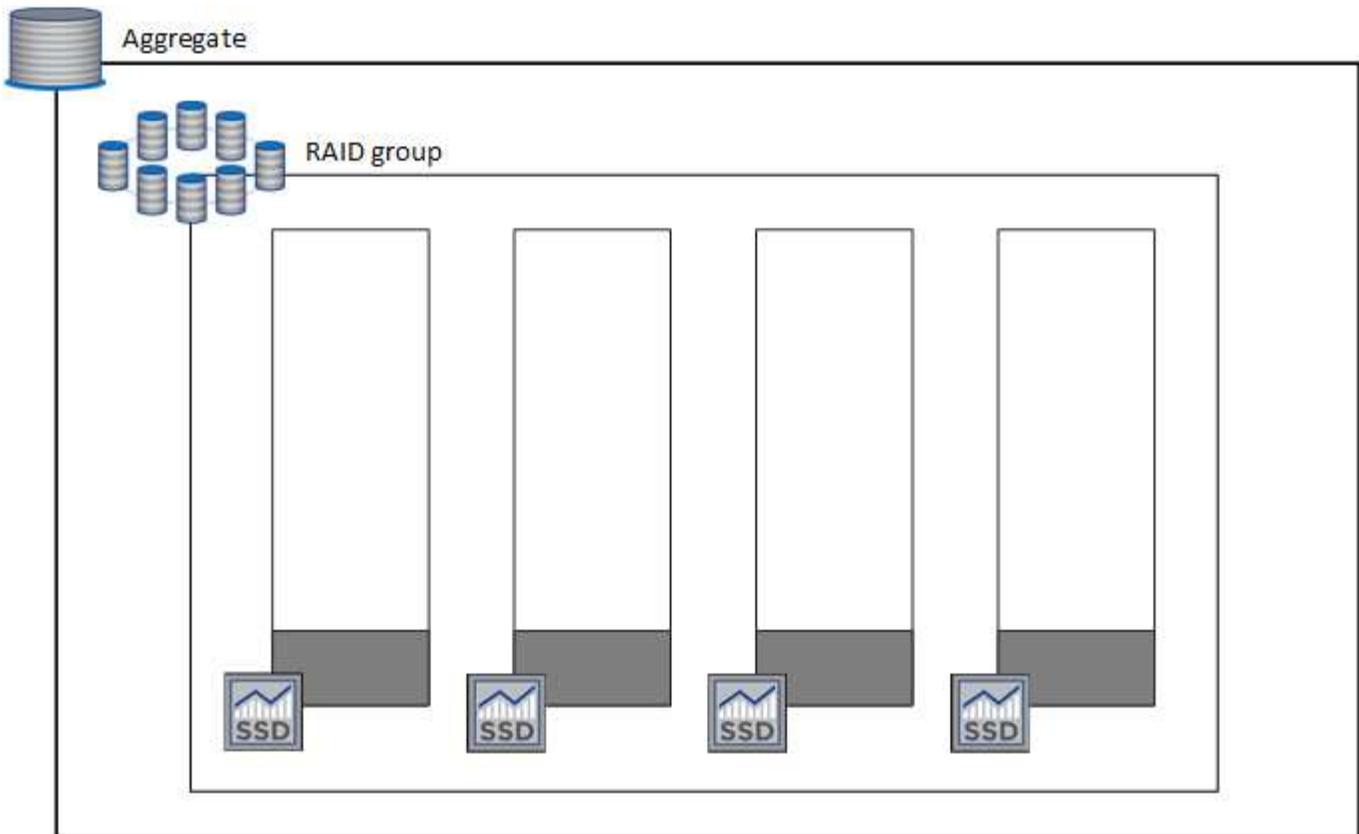
A partir da versão 3.9.19, o conector requer as seguintes permissões para habilitar e gerenciar o recurso volumes elásticos em um agregado Cloud Volumes ONTAP:

- EC2:DescribeVolumesModificações
- EC2:Modifyvolume

Essas permissões estão incluídas no ["As políticas fornecidas pela NetApp"](#)

Como funciona o suporte para volumes elásticos

Um agregado que tenha o recurso Elastic volumes habilitado é composto por um ou dois grupos RAID. Cada grupo RAID tem quatro discos idênticos que têm a mesma capacidade. Aqui está um exemplo de um agregado 10 TIB que tem quatro discos que são 2,5 TIB cada:



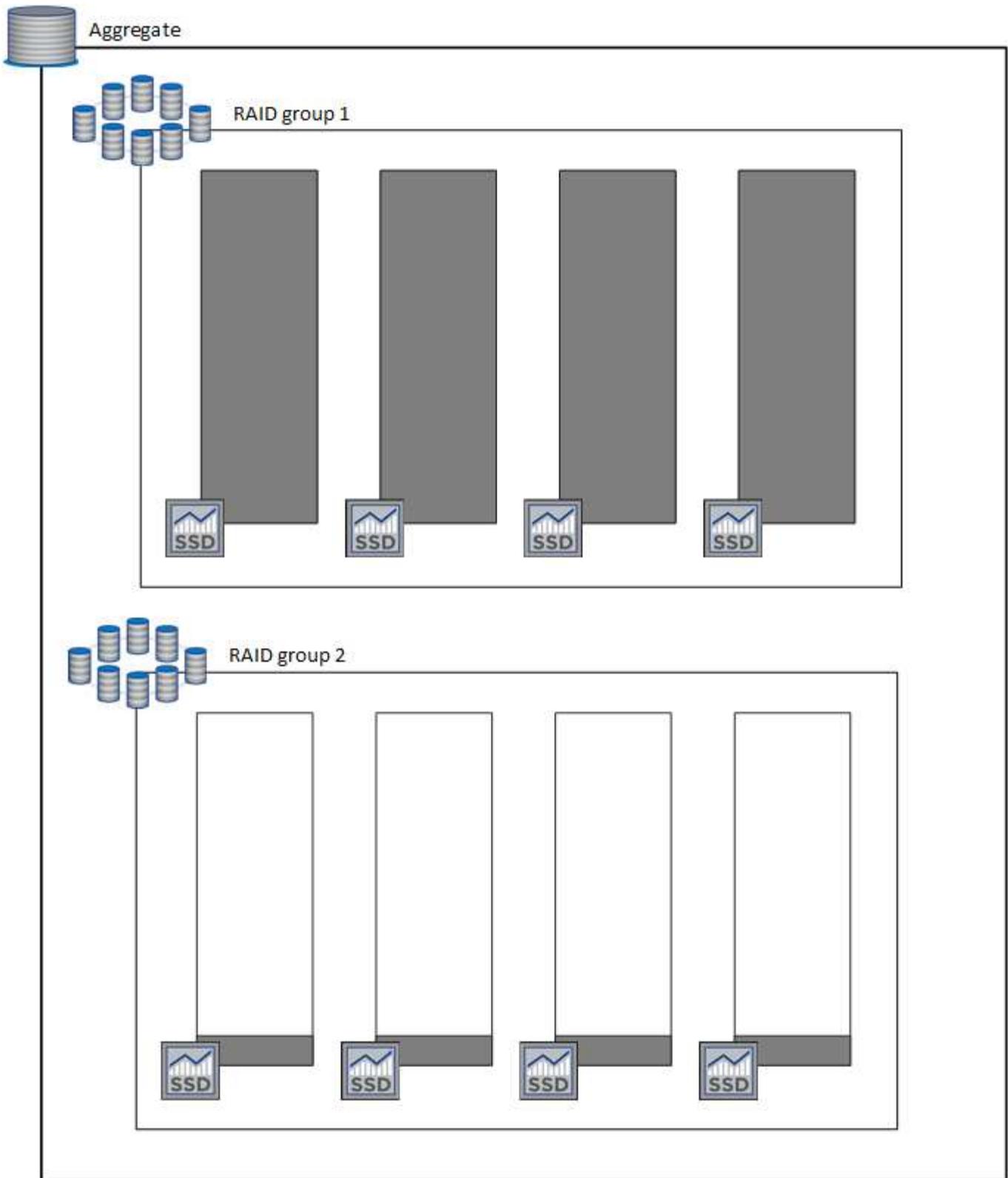
Quando o BlueXP cria um agregado, ele começa com um grupo RAID. Se for necessária capacidade adicional, o BlueXP aumentará o agregado aumentando a capacidade de todos os discos no grupo RAID pela mesma quantidade. O aumento de capacidade é de, no mínimo, 256 GiB ou 10% do tamanho do agregado.

Por exemplo, se você tiver um agregado de 1 TIB, cada disco será de 250 GiB. 10% da capacidade do agregado é de 100 GiB. Isso é inferior a 256 GiB, então o tamanho do agregado é aumentado pelo mínimo de 256 GiB (ou 64 GiB para cada disco).

O BlueXP aumenta o tamanho dos discos enquanto o sistema Cloud Volumes ONTAP está em execução e enquanto os discos ainda estão conectados. A alteração não causa interrupções.

Se um agregado atingir 64 TIB (ou 16 TIB em cada disco), o BlueXP criará um segundo grupo RAID para capacidade adicional. Este segundo grupo RAID funciona como o primeiro: Tem quatro discos com a mesma capacidade e pode crescer até 64 TIB. Isso significa que um agregado pode ter uma capacidade máxima de 128 TIB.

Aqui está um exemplo de um agregado com dois grupos RAID. O limite de capacidade foi atingido no primeiro grupo RAID, enquanto os discos no segundo grupo RAID têm bastante espaço livre.



O que acontece quando você cria um volume

Se você criar um volume que use GP3 ou IO1 discos, o BlueXP criará o volume em um agregado da seguinte forma:

- Se houver um agregado GP3 ou IO1 existente que tenha volumes elásticos ativados, o BlueXP criará o volume nesse agregado.

- Se houver vários agregados GP3 ou IO1 que tenham volumes elásticos ativados, o BlueXP criará o volume no agregado que requer a menor quantidade de recursos.
- Se o sistema tiver apenas GP3 ou IO1 agregados que não estejam habilitados para volumes elásticos, o volume será criado nesse agregado.



Embora este cenário seja improvável, é possível em dois casos:

- Você desativou explicitamente o recurso volumes elásticos ao criar um agregado a partir da API.
- Você criou um novo sistema Cloud Volumes ONTAP a partir da interface do usuário, caso em que o recurso volumes elásticos é desativado no agregado inicial. Reveja [Limitações](#) abaixo para saber mais.

- Se nenhum agregado existente tiver capacidade suficiente, o BlueXP criará o agregado com volumes elásticos ativados e, em seguida, criará o volume nesse novo agregado.

O tamanho do agregado é baseado no tamanho do volume solicitado mais uma capacidade adicional de 10%.

Modo de gerenciamento de capacidade

O modo de gerenciamento de capacidade para um conector funciona com volumes elásticos semelhantes a como ele funciona com outros tipos de agregados:

- Quando o modo Automático está ativado (esta é a predefinição), o BlueXP aumenta automaticamente o tamanho dos agregados se for necessária capacidade adicional.
- Se você alterar o modo de gerenciamento de capacidade para Manual, o BlueXP solicitará sua aprovação para adquirir capacidade adicional.

["Saiba mais sobre o modo de gerenciamento de capacidade"](#).

Limitações

Aumentar o tamanho de um agregado pode levar até 6 horas. Durante esse período, a BlueXP não pode solicitar nenhuma capacidade adicional para esse agregado.

Como trabalhar com volumes elásticos

Você pode trabalhar com volumes elásticos no BlueXP da seguinte forma:

- Crie um novo sistema que tenha volumes elásticos ativados no agregado inicial ao usar discos GP3 ou IO1

["Saiba como criar o sistema Cloud Volumes ONTAP"](#)

- Crie um novo volume em um agregado que tenha volumes elásticos ativados

Se você criar um volume que use GP3 ou IO1 discos, o BlueXP criará automaticamente o volume em um agregado que tenha volumes elásticos ativados. Para obter mais detalhes, [O que acontece quando você cria um volume](#) consulte .

["Saiba como criar volumes"](#).

- Crie um novo agregado que tenha volumes elásticos ativados

Os volumes elásticos são ativados automaticamente em novos agregados que usam discos GP3 ou IO1, desde que o sistema Cloud Volumes ONTAP tenha sido criado a partir da versão 9.11.0 ou posterior.

Ao criar o agregado, o BlueXP solicitará o tamanho da capacidade do agregado. Isso é diferente de outras configurações em que você escolhe um tamanho de disco e número de discos.

A captura de tela a seguir mostra um exemplo de um novo agregado composto por GP3 discos.

1 Disk Type 2 Aggregate details 3 Tiering Data 4 Review

Select Disk Type

Disk Type

GP3 - General Purpose SSD Dynamic Performance

 **General Purpose SSD (gp3) Disk Properties**

Description: General purpose SSD volume that balances price and performance (performance level is independent of storage capacity)

IOPS Value  Throughput MB/s 

12000  250 

["Saiba como criar agregados"](#).

- Identificar agregados que têm volumes elásticos ativados

Quando você acessa a página Alocação avançada, você pode identificar se o recurso volumes elásticos está habilitado em um agregado. No exemplo a seguir, o agrg1 tem volumes elásticos ativados.

The screenshot shows the configuration for an aggregation named 'aggr1'. At the top right, it indicates the aggregation is 'ONLINE'. Below this, there are two columns: 'INFO' and 'CAPACITY'.

INFO		CAPACITY	
Disk Type	GP3 3000 IOPS	Provisioned size	907.12 GiB
Disks	4	EBS Used	1.13 GiB
Volumes	2	S3 Used	0 GiB
Elastic Volumes	Enabled		
S3 Tiering	Enabled		

- Adicionar capacidade a um agregado

Enquanto o BlueXP adiciona capacidade a agregados automaticamente conforme necessário, você pode aumentar manualmente a capacidade.

["Saiba como aumentar a capacidade agregada"](#).

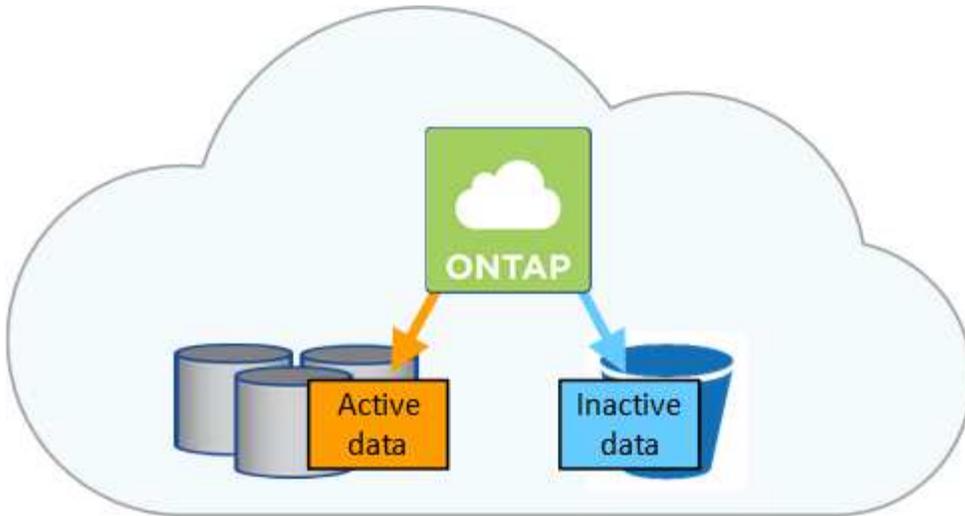
- Replique dados para um agregado que tenha volumes elásticos ativados

Se o sistema Cloud Volumes ONTAP de destino suportar volumes elásticos, um volume de destino será colocado em um agregado que tenha volumes elásticos ativados (desde que você escolha um disco GP3 ou IO1).

["Saiba como configurar a replicação de dados"](#)

Visão geral de categorização de dados

Reduza seus custos de storage habilitando a disposição automatizada de dados inativos em storage de objetos de baixo custo. Os dados ativos permanecem em SSDs ou HDDs de alta performance, enquanto os dados inativos são dispostos em camadas em storage de objetos de baixo custo. Isso permite recuperar espaço no storage primário e reduzir o storage secundário.



A disposição de dados em categorias é baseada na tecnologia FabricPool. O Cloud Volumes ONTAP fornece categorização de dados para todos os clusters do Cloud Volumes ONTAP sem uma licença adicional. Quando você ativa a disposição de dados em categorias, os dados dispostos em camadas no storage de objetos incorrem em cobranças. Consulte a documentação do seu provedor de nuvem para obter detalhes sobre os custos de armazenamento de objetos.

Categorização de dados no AWS

Ao habilitar a disposição de dados em categorias na AWS, o Cloud Volumes ONTAP usa o EBS como uma camada de desempenho para dados ativos e o AWS S3 como uma camada de capacidade para dados inativos.

Camada de performance

A categoria de performance pode ser SSDs de uso geral (GP3 ou GP2) ou SSDs IOPS provisionados (IO1).

A disposição em camadas dos dados no storage de objetos não é recomendada quando se usa HDDs otimizados para taxa de transferência (st1).

Camada de capacidade

Um sistema Cloud Volumes ONTAP categoriza dados inativos em um único bucket do S3.

O BlueXP cria um único bucket do S3 para cada ambiente de trabalho e o nomeia *Fabric-pool-cluster unique identifier*. Não é criado um bucket S3 diferente para cada volume.

Quando o BlueXP cria o bucket S3, ele usa as seguintes configurações padrão:

- Classe de armazenamento: Padrão
- Encriptação predefinida: Desativada
- Bloquear acesso público: Bloquear todo o acesso público
- Propriedade do objeto: ACLs habilitadas
- Controle de versão do bucket: Desativado
- Bloqueio de objetos: Desativado

Classes de armazenamento

A classe de armazenamento padrão para dados em camadas na AWS é *Standard*. O padrão é ideal para dados acessados com frequência armazenados em várias zonas de disponibilidade.

Se você não planeja acessar os dados inativos, você pode reduzir seus custos de armazenamento alterando a classe de armazenamento para um dos seguintes: *Intelligent Tiering*, *One-Zone unless Access*, *Standard-unreallow Access* ou *S3 Glacier Instant Retrieval*. Quando você altera a classe de armazenamento, os dados inativos começam na classe de armazenamento padrão e passam para a classe de armazenamento selecionada, se os dados não forem acessados após 30 dias.

Os custos de acesso são maiores se você acessar os dados, então leve isso em consideração antes de alterar a classe de storage. "[Documentação do Amazon S3: Saiba mais sobre as classes de armazenamento do Amazon S3](#)".

Você pode selecionar uma classe de armazenamento ao criar o ambiente de trabalho e pode alterá-la a qualquer momento depois. Para obter instruções sobre como alterar a classe de armazenamento, "[Disposição em camadas dos dados inativos em storage de objetos de baixo custo](#)" consulte .

A classe de storage para disposição de dados em categorias é de todo o sistema, não é por volume.

Categorização de dados no Azure

Ao habilitar a categorização de dados no Azure, o Cloud Volumes ONTAP usa discos gerenciados do Azure como uma categoria de performance para dados ativos e o storage Blob do Azure como uma categoria de capacidade para dados inativos.

Camada de performance

A camada de performance pode ser SSDs ou HDDs.

Camada de capacidade

Um sistema Cloud Volumes ONTAP categoriza dados inativos em um único contêiner de Blob.

O BlueXP cria uma nova conta de storage com um contêiner para cada ambiente de trabalho do Cloud Volumes ONTAP. O nome da conta de armazenamento é aleatório. Não é criado um recipiente diferente para cada volume.

O BlueXP cria a conta de armazenamento com as seguintes configurações:

- Camada de acesso: Quente
- Desempenho: Padrão
- Redundância: Armazenamento localmente redundante (LRS)
- Conta: StorageV2 (finalidade geral v2)
- Exigir transferência segura para operações de API REST: Ativado
- Acesso à chave da conta de armazenamento: Ativado
- Versão mínima de TLS: Versão 1,2
- Criptografia de infraestrutura: Desativada

Camadas de acesso ao storage

A camada de acesso de storage padrão para dados em camadas no Azure é o nível *hot*. A camada quente é ideal para dados acessados com frequência na camada de capacidade.

Se você não planeja acessar os dados inativos no nível de capacidade, pode escolher o nível de storage *cool*, onde os dados inativos são retidos por um mínimo de 30 dias. Você também pode optar pelo nível *cold*, onde os dados inativos são armazenados por um mínimo de 90 dias. Com base em seus requisitos de storage e considerações de custo, você pode selecionar o nível mais adequado às suas necessidades. Quando você altera o nível de storage para *COOL* ou *COLD*, os dados do nível de capacidade inativo são movidos diretamente para o nível de storage frio ou frio. As camadas fria e fria oferecem custos de storage menores em comparação com a camada quente, mas elas geram custos de acesso mais altos. Portanto, leve isso em consideração antes de alterar a camada de storage. Consulte a ["Documentação do Microsoft Azure: Saiba mais sobre os níveis de acesso ao armazenamento do Azure Blob"](#).

Você pode selecionar uma camada de storage ao criar o ambiente de trabalho e alterá-la a qualquer momento. Para obter detalhes sobre como alterar a camada de storage, ["Disposição em camadas dos dados inativos em storage de objetos de baixo custo"](#) consulte .

A camada de acesso a storage para categorização de dados é de todo o sistema, não é por volume.

Categorização de dados no Google Cloud

Ao habilitar a categorização de dados no Google Cloud, o Cloud Volumes ONTAP usa discos persistentes como uma categoria de performance para dados ativos e um bucket do Google Cloud Storage como uma categoria de capacidade para dados inativos.

Camada de performance

A camada de performance pode ser discos persistentes de SSD, discos persistentes balanceados ou discos persistentes padrão.

Camada de capacidade

Um sistema Cloud Volumes ONTAP alinha dados inativos com um único bucket do Google Cloud Storage.

O BlueXP cria um bucket para cada ambiente de trabalho e o nomeia *Fabric-pool-cluster unique identifier*. Não é criado um intervalo diferente para cada volume.

Quando o BlueXP cria o bucket, ele usa as seguintes configurações padrão:

- Tipo de localização: Região
- Classe de armazenamento: Padrão
- Acesso público: Sujeito a ACLs de objeto
- Controle de acesso: Refinado
- Proteção: Nenhuma
- Criptografia de dados: Chave gerenciada pelo Google

Classes de armazenamento

A classe de armazenamento padrão para dados em camadas é a classe *Standard Storage*. Se os dados forem acessados com pouca frequência, você poderá reduzir seus custos de armazenamento alterando para *Nearline Storage* ou *Coldline Storage*. Quando você altera a classe de armazenamento, os dados inativos subsequentes são movidos diretamente para a classe que você selecionou.



Todos os dados inativos existentes manterão a classe de armazenamento padrão quando você alterar a classe de armazenamento. Para alterar a classe de storage de dados inativos existentes, você deve executar a designação manualmente.

Os custos de acesso são maiores se você acessar os dados, então leve isso em consideração antes de

alterar a classe de storage. Para saber mais, ["Documentação do Google Cloud: Classes de armazenamento"](#) consulte .

Você pode selecionar uma camada de storage ao criar o ambiente de trabalho e alterá-la a qualquer momento. Para obter detalhes sobre como alterar a classe de armazenamento, ["Disposição em camadas dos dados inativos em storage de objetos de baixo custo"](#) consulte .

A classe de storage para disposição de dados em categorias é de todo o sistema, não é por volume.

Disposição de dados em categorias e limites de capacidade

Se você habilitar a disposição de dados em categorias, o limite de capacidade de um sistema permanecerá o mesmo. O limite se estende pela camada de performance e pela camada de capacidade.

Políticas de disposição em camadas de volume

Para habilitar a disposição de dados em categorias, você deve selecionar uma política de disposição em categorias de volume ao criar, modificar ou replicar um volume. Pode selecionar uma política diferente para cada volume.

Algumas políticas de disposição em categorias têm um período de resfriamento mínimo associado, que define o tempo em que os dados do usuário em um volume precisam permanecer inativos para que os dados sejam considerados "frios" e movidos para o nível de capacidade. O período de resfriamento começa quando os dados são gravados no agregado.



Você pode alterar o período mínimo de resfriamento e o limite agregado padrão de 50% (mais sobre isso abaixo). ["Saiba como alterar o período de arrefecimento"](#) e ["saiba como alterar o limite"](#).

O BlueXP permite que você escolha uma das seguintes políticas de disposição em categorias de volume ao criar ou modificar um volume:

Apenas Snapshot

Depois que um agregado atinge a capacidade de 50%, o Cloud Volumes ONTAP classifica os dados inativos dos usuários das cópias Snapshot que não estão associados ao sistema de arquivos ativo à categoria de capacidade. O período de resfriamento é de aproximadamente 2 dias.

Se forem lidos, os blocos de dados inativos na camada de capacidade aquecem e são movidos para a categoria de performance.

Tudo

Todos os dados (não incluindo metadados) são imediatamente marcados como frios e dispostos em camadas no storage de objetos o mais rápido possível. Não há necessidade de esperar 48 horas para que novos blocos em um volume fiquem frios. Observe que os blocos localizados no volume antes da política tudo ser definida exigem 48 horas para ficarem frios.

Se lidos, os blocos de dados inativos na categoria de nuvem não são gravados de volta na categoria de performance. Esta política está disponível a partir do ONTAP 9.6.

Auto

Depois que um agregado atinge a capacidade de 50%, o Cloud Volumes ONTAP dispõe de blocos de dados inativos em um volume para uma categoria de capacidade. Os dados inativos incluem não apenas cópias Snapshot, mas também dados de usuários inativos do sistema de arquivos ativo. O período de resfriamento é de aproximadamente 31 dias.

Esta política é suportada a partir do Cloud Volumes ONTAP 9,4.

Se forem lidos por leituras aleatórias, os blocos de dados inativos na camada de capacidade aquecem e migram para a camada de performance. Se forem lidos por leituras sequenciais, como as associadas a verificações de índice e antivírus, os blocos de dados inativos permanecem inativos e não se movem para o nível de desempenho.

Nenhum

Mantém os dados de um volume na categoria de performance, impedindo que ele seja migrado para a categoria de capacidade.

Ao replicar um volume, você pode escolher se deseja categorizar os dados em storage de objetos. Se o fizer, o BlueXP aplica a política **Backup** ao volume de proteção de dados. A partir do Cloud Volumes ONTAP 9,6, a política de disposição em camadas **All** substitui a política de backup.

A desativação do Cloud Volumes ONTAP afeta o período de resfriamento

Os blocos de dados são resfriados por exames de resfriamento. Durante este processo, os blocos que não foram usados têm a temperatura do bloco movida (resfriada) para o próximo valor mais baixo. O tempo de resfriamento padrão depende da política de disposição em categorias de volume:

- Auto: 31 dias
- Somente snapshot: 2 dias

O Cloud Volumes ONTAP deve estar em execução para que o exame de arrefecimento funcione. Se o Cloud Volumes ONTAP estiver desligado, o resfriamento também parará. Como resultado, você pode experimentar tempos de resfriamento mais longos.



Quando o Cloud Volumes ONTAP é desligado, a temperatura de cada bloco é preservada até que você reinicie o sistema. Por exemplo, se a temperatura de um bloco for 5 quando você desligar o sistema, a temperatura ainda será 5 quando você ligar o sistema novamente.

Configuração de categorização de dados

Para obter instruções e uma lista de configurações suportadas, "[Disposição em camadas dos dados inativos em storage de objetos de baixo custo](#)" consulte .

Gerenciamento de storage

O BlueXP oferece gerenciamento simplificado e avançado do storage Cloud Volumes ONTAP.



Todos os discos e agregados devem ser criados e excluídos diretamente do BlueXP . Você não deve executar essas ações de outra ferramenta de gerenciamento. Isso pode afetar a estabilidade do sistema, dificultar a capacidade de adicionar discos no futuro e, potencialmente, gerar taxas redundantes de provedores de nuvem.

Provisionamento de storage

O BlueXP facilita o provisionamento de storage para Cloud Volumes ONTAP ao comprar discos e gerenciar agregados para você. Você simplesmente precisa criar volumes. Você pode usar uma opção avançada de alocação para provisionar agregados, se desejar.

Provisionamento simplificado

Agregados fornecem storage de nuvem para volumes. O BlueXP cria agregados para você quando inicia uma instância e quando você provisiona volumes adicionais.

Quando você cria um volume, o BlueXP faz uma de três coisas:

- Ele coloca o volume em um agregado existente que tem espaço livre suficiente.
- Ele coloca o volume em um agregado existente comprando mais discos para esse agregado.

No caso de um agregado na AWS que suporte volumes elásticos, o BlueXP também aumenta o tamanho dos discos em um grupo RAID. ["Saiba mais sobre o suporte para volumes elásticos"](#).

- Ele compra discos para um novo agregado e coloca o volume nesse agregado.

O BlueXP determina onde colocar um novo volume analisando vários fatores: O tamanho máximo de um agregado, se o thin Provisioning está habilitado e os limites de espaço livre para agregados.

Seleção de tamanho de disco para agregados na AWS

Quando o BlueXP cria novos agregados para o Cloud Volumes ONTAP na AWS, ele aumenta gradualmente o tamanho do disco em um agregado, à medida que o número de agregados no sistema aumenta. O BlueXP faz isso para garantir que você possa utilizar a capacidade máxima do sistema antes de atingir o número máximo de discos de dados permitidos pela AWS.

Por exemplo, o BlueXP pode escolher os seguintes tamanhos de disco:

Número agregado	Tamanho do disco	Capacidade de agregado máxima
1	500 GiB	3 TIB
4	1 TIB	6 TIB
6	2 TIB	12 TIB



Esse comportamento não se aplica a agregados que suportam o recurso volumes elásticos do Amazon EBS. Os agregados que têm volumes elásticos ativados são compostos por um ou dois grupos RAID. Cada grupo RAID tem quatro discos idênticos que têm a mesma capacidade. ["Saiba mais sobre o suporte para volumes elásticos"](#).

Você pode escolher o tamanho do disco usando a opção de alocação avançada.

Alocação avançada

Em vez de permitir que o BlueXP gerencie agregados para você, você pode fazer isso sozinho. ["Na página Alocação avançada"](#), você pode criar novos agregados que incluem um número específico de discos, adicionar discos a um agregado existente e criar volumes em agregados específicos.

Gerenciamento de capacidade

A organização ou o administrador da conta do BlueXP pode escolher se o BlueXP notifica você sobre decisões de capacidade de storage ou se o BlueXP gerencia automaticamente os requisitos de capacidade para você.

Esse comportamento é determinado pelo *Capacity Management Mode* em um conector. O modo de

gerenciamento de capacidade afeta todos os sistemas Cloud Volumes ONTAP gerenciados por esse conector. Se você tiver outro conector, ele pode ser configurado de forma diferente.

Gerenciamento automático de capacidade

Por padrão, o modo de gerenciamento de capacidade é definido como automático. Neste modo, o BlueXP verifica a relação de espaço livre a cada 15 minutos para determinar se a relação de espaço livre cai abaixo do limite especificado. Se for necessário mais capacidade, o BlueXP iniciará automaticamente a compra de novos discos, excluirá coleções de discos não utilizados (agregados), moverá volumes entre agregados conforme necessário e tentará evitar falhas de disco.

Os exemplos a seguir ilustram como esse modo funciona:

- Se um agregado atingir o limite de capacidade e tiver espaço para mais discos, a BlueXP comprará novos discos para esse agregado automaticamente, para que os volumes possam continuar a crescer.

No caso de um agregado na AWS que suporte volumes elásticos, o BlueXP também aumenta o tamanho dos discos em um grupo RAID. ["Saiba mais sobre o suporte para volumes elásticos"](#).

- Se um agregado atingir o limite de capacidade e não puder suportar nenhum disco adicional, o BlueXP moverá automaticamente um volume desse agregado para um agregado com capacidade disponível ou para um novo agregado.

Se o BlueXP criar um novo agregado para o volume, ele escolherá um tamanho de disco que acomoda o tamanho desse volume.

Note que o espaço livre está agora disponível no agregado original. Volumes existentes ou novos volumes podem usar esse espaço. O espaço não pode ser retornado ao provedor de nuvem neste cenário.

- Se um agregado não contiver volumes por mais de 12 horas, o BlueXP o excluirá.

Gerenciamento de LUNs com gerenciamento automático de capacidade

O gerenciamento automático de capacidade do BlueXP não se aplica a LUNs. Quando o BlueXP cria um LUN, ele desativa o recurso de crescimento automático.

Gerenciamento manual de capacidade

Se a Organização BlueXP ou o administrador da conta definir o modo de gerenciamento de capacidade como manual, o BlueXP exibirá as mensagens Ação necessárias quando as decisões de capacidade devem ser tomadas. Os mesmos exemplos descritos no modo automático aplicam-se ao modo manual, mas cabe a você aceitar as ações.

Saiba mais

["Saiba como modificar o modo de gerenciamento de capacidade"](#).

Velocidade de gravação

O BlueXP permite que você escolha velocidade de gravação normal ou alta para a maioria das configurações do Cloud Volumes ONTAP. Antes de escolher uma velocidade de gravação, você deve entender as diferenças entre as configurações normal e alta e os riscos e recomendações ao usar alta velocidade de gravação.

Velocidade de gravação normal

Quando você escolhe a velocidade de gravação normal, os dados são gravados diretamente no disco. Quando os dados são gravados diretamente no disco, reduz a probabilidade de perda de dados no caso de uma falha não planejada do sistema ou uma falha em cascata envolvendo uma interrupção não planejada do sistema (somente pares de HA).

A velocidade de gravação normal é a opção padrão.

Alta velocidade de gravação

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

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

Quando usar alta velocidade de gravação

A alta velocidade de gravação é uma boa opção se for necessário um desempenho de gravação rápido para sua carga de trabalho e você pode resistir ao risco de perda de dados no caso de uma interrupção não planejada do sistema ou uma falha em cascata envolvendo uma interrupção não planejada do sistema (somente pares de HA).

Recomendações ao usar alta velocidade de gravação

Se você habilitar a alta velocidade de gravação, garanta a proteção de gravação na camada da aplicação ou que as aplicações possam tolerar a perda de dados, se isso ocorrer.

Alta velocidade de gravação com um par de HA na AWS

Se você planeja habilitar a alta velocidade de gravação em um par de HA na AWS, deve entender a diferença nos níveis de proteção entre uma implantação de zona de disponibilidade múltipla (AZ) e uma única implantação de AZ. A implantação de um par de HA em vários AZs oferece mais resiliência e pode ajudar a reduzir as chances de perda de dados.

["Saiba mais sobre pares de HA na AWS"](#).

Configurações compatíveis com alta velocidade de gravação

Nem todas as configurações do Cloud Volumes ONTAP suportam alta velocidade de gravação. Essas configurações usam velocidade de gravação normal por padrão.

AWS

Se você usar um sistema de nó único, o Cloud Volumes ONTAP oferece suporte à alta velocidade de gravação em todos os tipos de instância.

A partir da versão 9,8, o Cloud Volumes ONTAP suporta alta velocidade de gravação com pares de HA ao usar quase todos os tipos de instâncias EC2 suportadas, exceto M5.xlarge e R5.xlarge.

["Saiba mais sobre as instâncias do Amazon EC2 suportadas pelo Cloud Volumes ONTAP"](#).

Azure

Se você usar um sistema de nó único, o Cloud Volumes ONTAP oferece suporte à alta velocidade de gravação em todos os tipos de VM.

Se você usar um par de HA, o Cloud Volumes ONTAP oferece suporte à alta velocidade de gravação com vários tipos de VM, a partir da versão 9,8. Vá para a ["Notas de versão do Cloud Volumes ONTAP"](#) para ver os tipos de VM que suportam alta velocidade de gravação.

Google Cloud

Se você usar um sistema de nó único, o Cloud Volumes ONTAP oferece suporte a alta velocidade de gravação em todos os tipos de máquina.

Se você usar um par de HA, o Cloud Volumes ONTAP oferece suporte à alta velocidade de gravação com vários tipos de VM, a partir da versão 9.13.0. Vá para a ["Notas de versão do Cloud Volumes ONTAP"](#) para ver os tipos de VM que suportam alta velocidade de gravação.

["Saiba mais sobre os tipos de máquina compatíveis com o Cloud Volumes ONTAP"](#).

Como selecionar uma velocidade de gravação

Você pode escolher uma velocidade de gravação ao criar um novo ambiente de trabalho e pode ["altere a velocidade de gravação de um sistema existente"](#).

O que esperar se ocorrer perda de dados

Se ocorrer perda de dados devido à alta velocidade de gravação, o sistema de Gerenciamento de Eventos (EMS) relata os dois eventos a seguir:

- Cloud Volumes ONTAP 9.12.1 ou posterior

```
NOTICE nv.data.loss.possible: An unexpected shutdown occurred while in
high write speed mode, which possibly caused a loss of data.
* Cloud Volumes ONTAP 9.11.0 a 9.11.1
```

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due
to dirty shutdown with High Write Speed mode"
```

```
ERROR wafl.root.content.changed: Contents of the root volume '' might
have changed. Verify that all recent configuration changes are still in
effect..
* Cloud Volumes ONTAP 9,8 a 9.10.1
```

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due to dirty shutdown"
```

```
ERROR wafl.root.content.changed: Contents of the root volume '' might have changed. Verify that all recent configuration changes are still in effect.
```

Quando isso acontece, o Cloud Volumes ONTAP deve ser capaz de inicializar e continuar fornecendo dados sem a intervenção do usuário.

Como parar o acesso aos dados se ocorrer perda de dados

Se você estiver preocupado com a perda de dados, deseja que os aplicativos parem de ser executados após a perda de dados e o acesso aos dados seja retomado após o problema de perda de dados ser resolvido corretamente, você pode usar a opção NVFAIL da CLI para atingir esse objetivo.

Para ativar a opção NVFAIL

```
vol modify -volume <vol-name> -nvfail on
```

Para verificar as definições de NVFAIL

```
vol show -volume <vol-name> -fields nvfail
```

Para desativar a opção NVFAIL

```
vol modify -volume <vol-name> -nvfail off
```

Quando a perda de dados ocorre, um volume NFS ou iSCSI com NVFAIL habilitado deve parar de fornecer dados (não há impactos no CIFS, que é um protocolo sem monitoração de estado). Para obter mais detalhes, "[Como o NVFAIL afeta o acesso a volumes NFS ou LUNs](#)" consulte .

Para verificar o estado NVFAIL

```
vol show -fields in-nvfailed-state
```

Depois que o problema de perda de dados for resolvido corretamente, você pode limpar o estado NVFAIL e o volume estará disponível para acesso aos dados.

Para limpar o estado NVFAIL

```
vol modify -volume <vol-name> -in-nvfailed-state false
```

Flash Cache

Algumas configurações do Cloud Volumes ONTAP incluem storage NVMe local, que o Cloud Volumes ONTAP usa como *Flash Cache* para melhor desempenho.

O que é Flash Cache?

O Flash Cache acelera o acesso aos dados por meio do armazenamento em cache inteligente em tempo real dos dados do usuário lidos recentemente e dos metadados do NetApp. Ele é eficaz para cargas de trabalho com uso intenso de leitura aleatória, incluindo bancos de dados, e-mail e serviços de arquivos.

Configurações compatíveis

O flash Cache é compatível com configurações Cloud Volumes ONTAP específicas. Veja as configurações suportadas no ["Notas de versão do Cloud Volumes ONTAP"](#)

Limitações

- Ao configurar o Flash Cache para Cloud Volumes ONTAP 9.12.0 ou anterior na AWS, a compactação deve ser desativada em todos os volumes para aproveitar as melhorias de desempenho do Flash Cache. Ao implantar ou atualizar para o Cloud Volumes ONTAP 9.12.1 ou posterior, não é necessário desativar a compactação.

Não escolher eficiência de storage ao criar um volume a partir do BlueXP ou criar um volume e, em seguida ["Desative a compressão de dados usando a CLI"](#), .

- O reaquecimento do cache após uma reinicialização não é suportado com o Cloud Volumes ONTAP.

STORAGE WORM

Você pode ativar o storage WORM (uma gravação, muitas leituras) em um sistema Cloud Volumes ONTAP para reter arquivos de forma não modificada por um período de retenção especificado. O storage WORM em nuvem é baseado na tecnologia SnapLock, o que significa que os arquivos WORM são protegidos no nível do arquivo.

O recurso WORM está disponível para uso com subscrições bring Your own license (BYOL) e marketplace para suas licenças sem custo adicional. Entre em Contato com seu representante de vendas da NetApp para adicionar WORM à sua licença atual.

Como o storage WORM funciona

Depois que um arquivo foi comprometido com o storage WORM, ele não pode ser modificado, mesmo depois que o período de retenção expirou. Um relógio à prova de violação determina quando o período de retenção para um arquivo WORM expirou.

Após o período de retenção ter terminado, você é responsável por excluir quaisquer arquivos que você não precisa mais.

Ativar o storage WORM

A forma como você ativa o storage WORM depende da versão do Cloud Volumes ONTAP que você está usando.

Versão 9.10.1 e posterior

A partir do Cloud Volumes ONTAP 9.10.1, você tem a opção de ativar ou desativar WORM no nível de volume.

Ao criar um novo ambiente de trabalho do Cloud Volumes ONTAP, você será solicitado a ativar ou desativar o storage WORM:

- Se você habilitar o storage WORM ao criar um ambiente de trabalho, cada volume que você cria do BlueXP tem WORM ativado. Mas você pode usar o Gerenciador de sistemas do ONTAP ou a CLI do ONTAP para criar volumes com WORM desativado.
- Se você desativar o storage WORM ao criar um ambiente de trabalho, cada volume criado com o BlueXP ,

o Gerenciador de sistemas do ONTAP ou a ONTAP CLI tem WORM desativado.

Versão 9.10.0 e anterior

Você pode ativar o storage WORM em um sistema Cloud Volumes ONTAP ao criar um novo ambiente de trabalho. Cada volume que você cria com o BlueXP tem WORM ativado. Não é possível desativar o storage WORM em volumes individuais.

Armazenando arquivos no WORM

Você pode usar uma aplicação para vincular arquivos ao WORM em NFS ou CIFS, ou usar a CLI da ONTAP para vincular automaticamente arquivos ao WORM. Você também pode usar um arquivo anexado WORM para reter dados gravados de forma incremental, como informações de log.

Depois de ativar o storage WORM em um sistema Cloud Volumes ONTAP, você precisa usar a CLI da ONTAP para todo o gerenciamento de storage WORM. Para obter instruções, ["Documentação do ONTAP"](#) consulte .

Habilitando WORM em um ambiente de trabalho do Cloud Volumes ONTAP

Você pode habilitar o storage WORM ao criar um ambiente de trabalho do Cloud Volumes ONTAP no BlueXP . Você também pode habilitar o WORM em um ambiente de trabalho se o WORM não estiver ativado durante a criação. Depois de ativá-lo, não é possível desativar WORM.

Sobre esta tarefa

- O WORM é suportado no ONTAP 9.10,1 e posterior.
- O WORM com backup é suportado no ONTAP 9.11,1 e posterior.

Passos

1. Na página Canvas, clique duas vezes no nome do ambiente de trabalho no qual você deseja habilitar WORM.
2. Na guia Visão geral, clique no painel recursos e, em seguida, clique no ícone de lápis ao lado de **WORM**.

Se WORM já estiver ativado no sistema, o ícone de lápis será desativado.

3. Na página **WORM**, defina o período de retenção para o relógio de conformidade do cluster.

Para obter mais informações, ["Documentação do ONTAP: Inicialize o Relógio de conformidade"](#) consulte .

4. Clique em **Definir**.

Depois de terminar

Você pode verificar o status de **WORM** no painel recursos. Depois que o WORM é ativado, a licença do SnapLock é instalada automaticamente no cluster. Você pode visualizar a licença SnapLock no Gerenciador de sistemas do ONTAP.

Excluindo arquivos WORM

Você pode excluir arquivos WORM durante o período de retenção usando o recurso de exclusão privilegiada.

Para obter instruções, ["Documentação do ONTAP"](#) consulte .

WORM e categorização de dados

Ao criar um novo sistema Cloud Volumes ONTAP 9,8 ou posterior, é possível habilitar o storage WORM e disposição de dados em camadas. Ao habilitar a disposição de dados em categorias com storage WORM, você pode categorizar os dados em um armazenamento de objetos na nuvem.

Você deve entender o seguinte sobre como habilitar o storage WORM e disposição de dados em camadas:

- Os dados dispostos em camadas em storage de objetos não incluem a funcionalidade WORM do ONTAP. Para garantir a funcionalidade WORM completa, você precisará configurar as permissões de bucket corretamente.
- Os dados dispostos em camadas no storage de objetos não possuem a funcionalidade WORM, o que significa que tecnicamente qualquer pessoa com acesso total a buckets e contêineres pode apagar os objetos dispostos em camadas pelo ONTAP.
- Reverter ou fazer downgrade para o Cloud Volumes ONTAP 9,8 é bloqueado depois de ativar WORM e disposição em camadas.

Limitações

- O storage WORM no Cloud Volumes ONTAP opera sob um modelo de "administrador de storage confiável". Embora os arquivos WORM sejam protegidos contra alterações ou modificações, os volumes podem ser excluídos por um administrador de cluster mesmo que esses volumes contenham dados WORM não expirados.
- Além do modelo de administrador de storage confiável, o storage WORM no Cloud Volumes ONTAP também opera implicitamente sob um modelo de "administrador de nuvem confiável". Um administrador da nuvem pode excluir dados WORM antes de sua data de expiração, removendo ou editando o storage de nuvem diretamente do fornecedor da nuvem.

Informações relacionadas

- ["Crie cópias de Snapshot à prova de violações para storage WORM"](#)

Pares de alta disponibilidade

Pares de alta disponibilidade na AWS

Uma configuração de alta disponibilidade (HA) do Cloud Volumes ONTAP fornece operações ininterruptas e tolerância de falhas. Na AWS, os dados são espelhados de forma síncrona entre os dois nós.

Componentes HA

Na AWS, as configurações do Cloud Volumes ONTAP HA incluem os seguintes componentes:

- Dois nós de Cloud Volumes ONTAP cujos dados são espelhados de forma síncrona entre si.
- Uma instância de mediador que fornece um canal de comunicação entre os nós para auxiliar nos processos de takeover do storage e giveback.

Mediador

Aqui estão alguns detalhes importantes sobre a instância do mediador na AWS:

Tipo de instância

t3-micro

Discos

Dois discos st1 de 8 GiB e 4 GiB

Sistema operacional

Debian 11



Para o Cloud Volumes ONTAP 9.10.0 e versões anteriores, o Debian 10 foi instalado no mediador.

Atualizações

Quando você atualiza o Cloud Volumes ONTAP, o BlueXP também atualiza a instância do mediador conforme necessário.

Acesso à instância

Quando você cria um par de HA do Cloud Volumes ONTAP a partir do BlueXP, será solicitado a fornecer um par de chaves para a instância do mediador. Você pode usar esse par de chaves para acesso SSH usando o `admin` usuário.

Agentes de terceiros

Agentes de terceiros ou extensões de VM não são suportados na instância do mediador.

Takeover de storage e giveback

Se um nó ficar inativo, o outro nó poderá fornecer dados para que seu parceiro forneça serviços de dados contínuos. Os clientes podem acessar os mesmos dados do nó do parceiro porque os dados foram espelhados de forma síncrona para o parceiro.

Depois que o nó for reiniciado, o parceiro deverá sincronizar novamente os dados antes que ele possa retornar o armazenamento. O tempo necessário para sincronizar novamente os dados depende da quantidade de dados alterados enquanto o nó estava inativo.

Por padrão, o takeover, a ressincronização e a giveback do storage são automáticos. Nenhuma ação do usuário é necessária.

RPO e rto

Uma configuração de HA mantém a alta disponibilidade dos dados da seguinte forma:

- O objetivo do ponto de restauração (RPO) é de 0 segundos. Seus dados são consistentes transacionalmente, sem perda de dados.
- O objetivo de tempo de recuperação (rto) é de 120 segundos. Em caso de interrupção, os dados devem estar disponíveis em 120 segundos ou menos.

Modelos de IMPLANTAÇÃO DE HA

Você pode garantir a alta disponibilidade de seus dados implantando uma configuração de HA em várias zonas de disponibilidade (AZs) ou em uma única zona de disponibilidade (AZ). Você deve rever mais detalhes sobre cada configuração para escolher qual melhor se adapta às suas necessidades.

Várias zonas de disponibilidade

A implantação de uma configuração de HA em várias zonas de disponibilidade (AZs) garante alta disponibilidade de seus dados se ocorrer uma falha com uma AZ ou uma instância que execute um nó Cloud Volumes ONTAP. Você deve entender como os endereços IP nas afetam o acesso aos dados e o failover de storage.

Acesso a dados NFS e CIFS

Quando uma configuração de HA é espalhada por várias zonas de disponibilidade, *endereços IP flutuantes* ativa o acesso do cliente nas. Os endereços IP flutuantes, que devem estar fora dos blocos CIDR para todos os VPCs na região, podem migrar entre nós quando ocorrem falhas. Eles não são acessíveis nativamente para clientes que estão fora da VPC, a menos que você "[Configure um gateway de trânsito da AWS](#)".

Se não for possível configurar um gateway de trânsito, os endereços IP privados estarão disponíveis para clientes nas que estejam fora da VPC. No entanto, esses endereços IP são estáticos – eles não podem fazer failover entre nós.

Você deve analisar os requisitos para endereços IP flutuantes e tabelas de rota antes de implantar uma configuração de HA em várias zonas de disponibilidade. Você deve especificar os endereços IP flutuantes ao implantar a configuração. Os endereços IP privados são criados automaticamente pelo BlueXP .

Para obter mais informações, "[Requisitos de rede da AWS para o Cloud Volumes ONTAP HA em vários AZs](#)" consulte .

Acesso a dados iSCSI

A comunicação de dados entre VPC não é um problema, uma vez que o iSCSI não usa endereços IP flutuantes.

Takeover e giveback para iSCSI

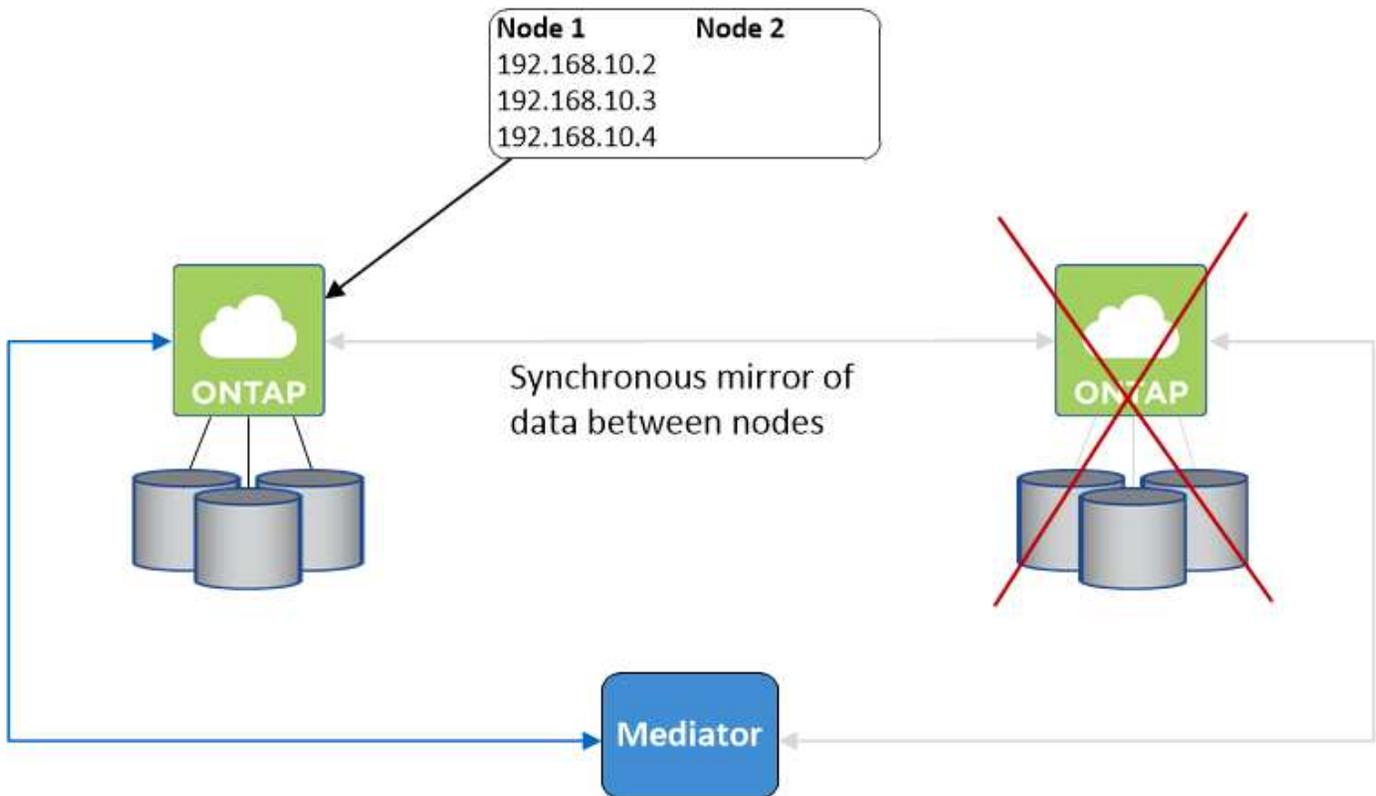
Para iSCSI, o Cloud Volumes ONTAP usa e/S multipath (MPIO) e Acesso de Unidade lógica assimétrica (ALUA) para gerenciar o failover de caminho entre os caminhos otimizados para ativos e não otimizados.



Para obter informações sobre quais configurações de host específicas suportam ALUA, consulte o "[Ferramenta de Matriz de interoperabilidade do NetApp](#)" e o "[Guia de HOSTS DE SAN e clientes DE nuvem](#)" do sistema operacional do seu host.

Takeover e giveback para nas

Quando o controle ocorre em uma configuração nas usando IPs flutuantes, o endereço IP flutuante do nó que os clientes usam para acessar dados se move para o outro nó. A imagem a seguir mostra a aquisição de armazenamento em uma configuração nas usando IPs flutuantes. Se o nó 2 descer, o endereço IP flutuante do nó 2 será movido para o nó 1.



Os IPs de dados nas usados para acesso VPC externo não podem migrar entre nós se ocorrerem falhas. Se um nó ficar offline, você deverá remontar manualmente os volumes para clientes fora da VPC usando o endereço IP no outro nó.

Depois que o nó com falha voltar online, remonte os clientes para volumes usando o endereço IP original. Essa etapa é necessária para evitar a transferência de dados desnecessários entre dois nós de HA, o que pode causar impactos significativo no desempenho e na estabilidade.

Você pode identificar facilmente o endereço IP correto do BlueXP selecionando o volume e clicando em **comando de montagem**.

Zona de disponibilidade única

A implantação de uma configuração de HA em uma única zona de disponibilidade (AZ) pode garantir alta disponibilidade de seus dados se uma instância que executa um nó Cloud Volumes ONTAP falhar. Todos os dados podem ser acessados de forma nativa de fora da VPC.

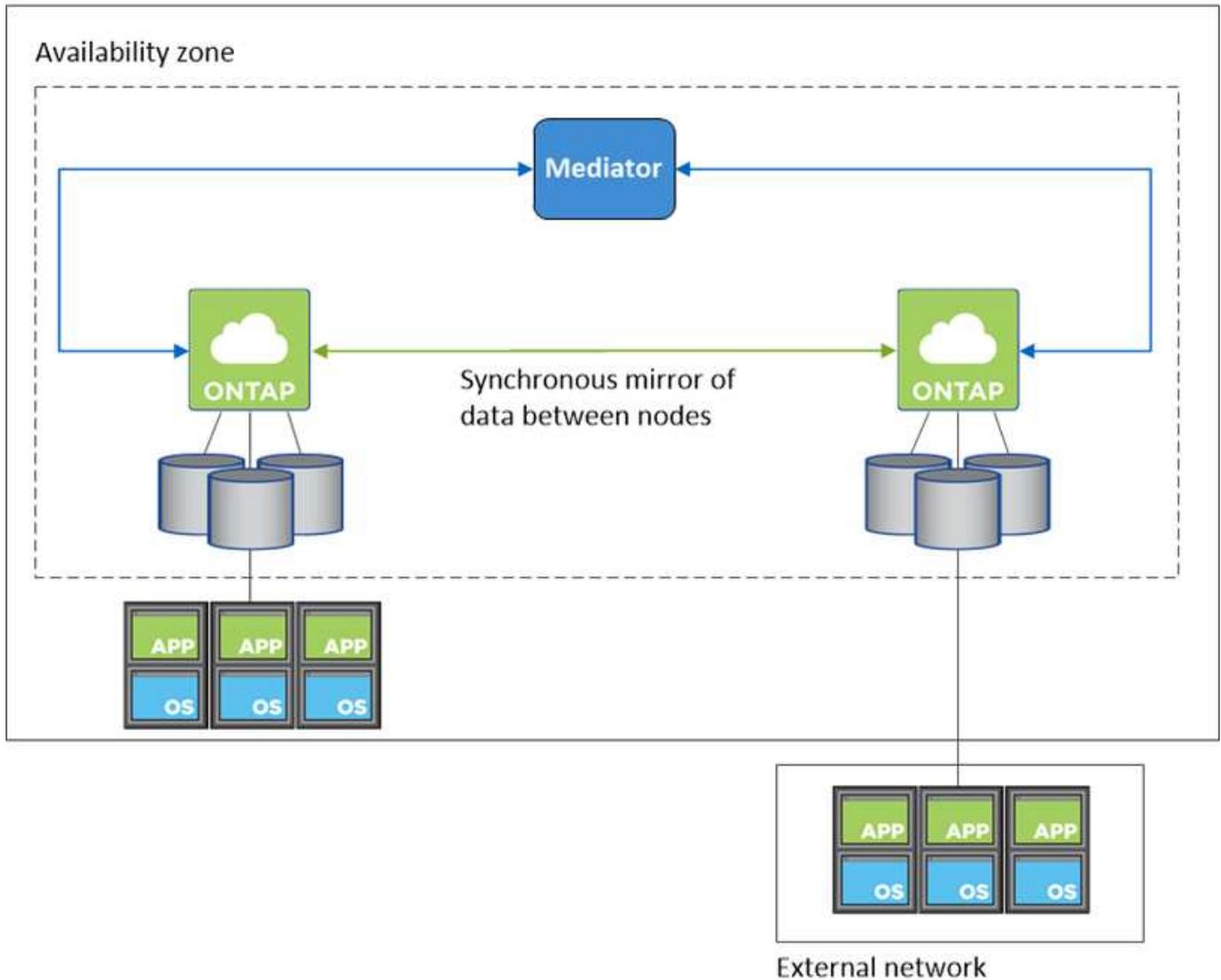


A BlueXP cria um "[Grupo de posicionamento do AWS Spread](#)" e lança os dois nós de HA nesse grupo de posicionamento. O grupo de posicionamento reduz o risco de falhas simultâneas, espalhando as instâncias por um hardware subjacente distinto. Esse recurso melhora a redundância do ponto de vista da computação e não do ponto de vista da falha de disco.

Acesso a dados

Como essa configuração está em uma única AZ, ela não requer endereços IP flutuantes. Você pode usar o mesmo endereço IP para acesso a dados a partir da VPC e de fora da VPC.

A imagem a seguir mostra uma configuração de HA em uma única AZ. Os dados são acessíveis a partir da VPC e de fora da VPC.



Takeover e giveback

Para iSCSI, o Cloud Volumes ONTAP usa e/S multipath (MPIO) e Acesso de Unidade lógica assimétrica (ALUA) para gerenciar o failover de caminho entre os caminhos otimizados para ativos e não otimizados.



Para obter informações sobre quais configurações de host específicas suportam ALUA, consulte o ["Ferramenta de Matriz de interoperabilidade do NetApp"](#) e o ["Guia de HOSTS DE SAN e clientes DE nuvem"](#) do sistema operacional do seu host.

Para configurações nas, os endereços IP de dados podem migrar entre nós de HA se ocorrerem falhas. Isso garante o acesso do cliente ao armazenamento.

Zonas locais da AWS

As zonas locais da AWS são uma implantação de infraestrutura onde storage, computação, banco de dados e outros serviços selecionados da AWS estão localizados perto de grandes cidades e áreas do setor. Com as zonas locais da AWS, você pode aproximar os serviços da AWS, o que melhora a latência de suas cargas de trabalho e mantém bancos de dados localmente. No Cloud Volumes ONTAP,

Você pode implantar uma única configuração AZ ou várias AZ nas zonas locais da AWS.



As zonas locais da AWS são suportadas ao usar o BlueXP nos modos padrão e privado. Neste momento, as zonas locais da AWS não são suportadas ao usar o BlueXP no modo restrito.

Exemplo de configurações da AWS local Zone

O Cloud Volumes ONTAP na AWS suporta apenas o modo de alta disponibilidade (HA) em uma única zona de disponibilidade. Implantações de nó único não são compatíveis.

O Cloud Volumes ONTAP não é compatível com categorização de dados, disposição em camadas na nuvem e instâncias não qualificadas nas zonas locais da AWS.

A seguir estão exemplos de configurações:

- Zona de disponibilidade única: Os nós de cluster e o mediador estão na mesma zona local.
- Várias zonas de disponibilidade em várias configurações de zona de disponibilidade, há três instâncias, dois nós e um mediador. Uma instância das três instâncias deve estar em uma zona separada. Você pode escolher como configurar isso.

Aqui estão três exemplos de configurações:

- Cada nó de cluster está em uma zona local diferente e o mediador em uma zona de disponibilidade pública.
- Um nó de cluster em uma zona local, o mediador em uma zona local e o segundo nó de cluster estão em uma zona de disponibilidade.
- Cada nó de cluster e o mediador estão em zonas locais separadas.

Tipos de disco e instância suportados

O único tipo de disco suportado é GP2. As seguintes famílias de tipos de instância EC2 com tamanhos xlarge a 4xlarge são atualmente suportadas:

- M5
- C5
- C5d
- R5
- R5d



O Cloud Volumes ONTAP é compatível apenas com essas configurações. Selecionar tipos de disco não suportados ou instâncias não qualificadas na configuração da zona local da AWS pode resultar em falha de implantação. A disposição de dados em categorias para o AWS S3 não está disponível nas zonas locais da AWS devido à falta de conectividade.

Consulte a documentação da AWS para obter os detalhes mais recentes e completos do ["EC2 tipos de instância em zonas locais"](#).

Como o storage funciona em um par de HA

Ao contrário de um cluster do ONTAP, o storage em um par de HA do Cloud Volumes ONTAP não é

compartilhado entre nós. Em vez disso, os dados são espelhados de forma síncrona entre os nós para que os dados estejam disponíveis em caso de falha.

Alocação de armazenamento

Quando você cria um novo volume e discos adicionais são necessários, o BlueXP aloca o mesmo número de discos para ambos os nós, cria um agregado espelhado e cria o novo volume. Por exemplo, se forem necessários dois discos para o volume, o BlueXP aloca dois discos por nó para um total de quatro discos.

Configurações de storage

Você pode usar um par de HA como uma configuração ativo-ativo, na qual ambos os nós fornecem dados aos clientes ou como uma configuração ativo-passivo, na qual o nó passivo responde a solicitações de dados somente se ele tiver ocupado o storage para o nó ativo.



Você pode configurar uma configuração ativo-ativo somente quando usar o BlueXP na visualização do sistema de armazenamento.

Expectativas de desempenho

Uma configuração do Cloud Volumes ONTAP HA replica sincronamente os dados entre nós, o que consome a largura de banda da rede. Como resultado, você pode esperar o seguinte desempenho em comparação com uma configuração de Cloud Volumes ONTAP de nó único:

- Para configurações de HA que atendem dados de apenas um nó, a performance de leitura é comparável à performance de leitura de uma configuração de nó único, enquanto a performance de gravação é menor.
- Para configurações de HA que atendem dados de ambos os nós, a performance de leitura é superior à performance de leitura de uma configuração de nó único, e a performance de gravação é igual ou superior.

Para obter mais detalhes sobre o desempenho do Cloud Volumes ONTAP, "[Desempenho](#)" consulte .

Acesso do cliente ao armazenamento

Os clientes devem acessar volumes NFS e CIFS usando o endereço IP de dados do nó no qual o volume reside. Se os clientes nas acessarem um volume usando o endereço IP do nó do parceiro, o tráfego vai entre os dois nós, o que reduz o desempenho.



Se você mover um volume entre nós em um par de HA, remonte o volume usando o endereço IP do outro nó. Caso contrário, você pode experimentar desempenho reduzido. Se os clientes suportarem referências NFSv4 ou redirecionamento de pastas para CIFS, você pode habilitar esses recursos nos sistemas Cloud Volumes ONTAP para evitar a reinstalação do volume. Para obter detalhes, consulte a documentação do ONTAP.

Você pode identificar facilmente o endereço IP correto por meio da opção *Mount Command* no painel gerenciar volumes no BlueXP .

Volume Actions

View volume details

Mount command

Clone volume

Edit volume tags

Edit volume settings

Delete volume

Protection Actions

Advanced Actions

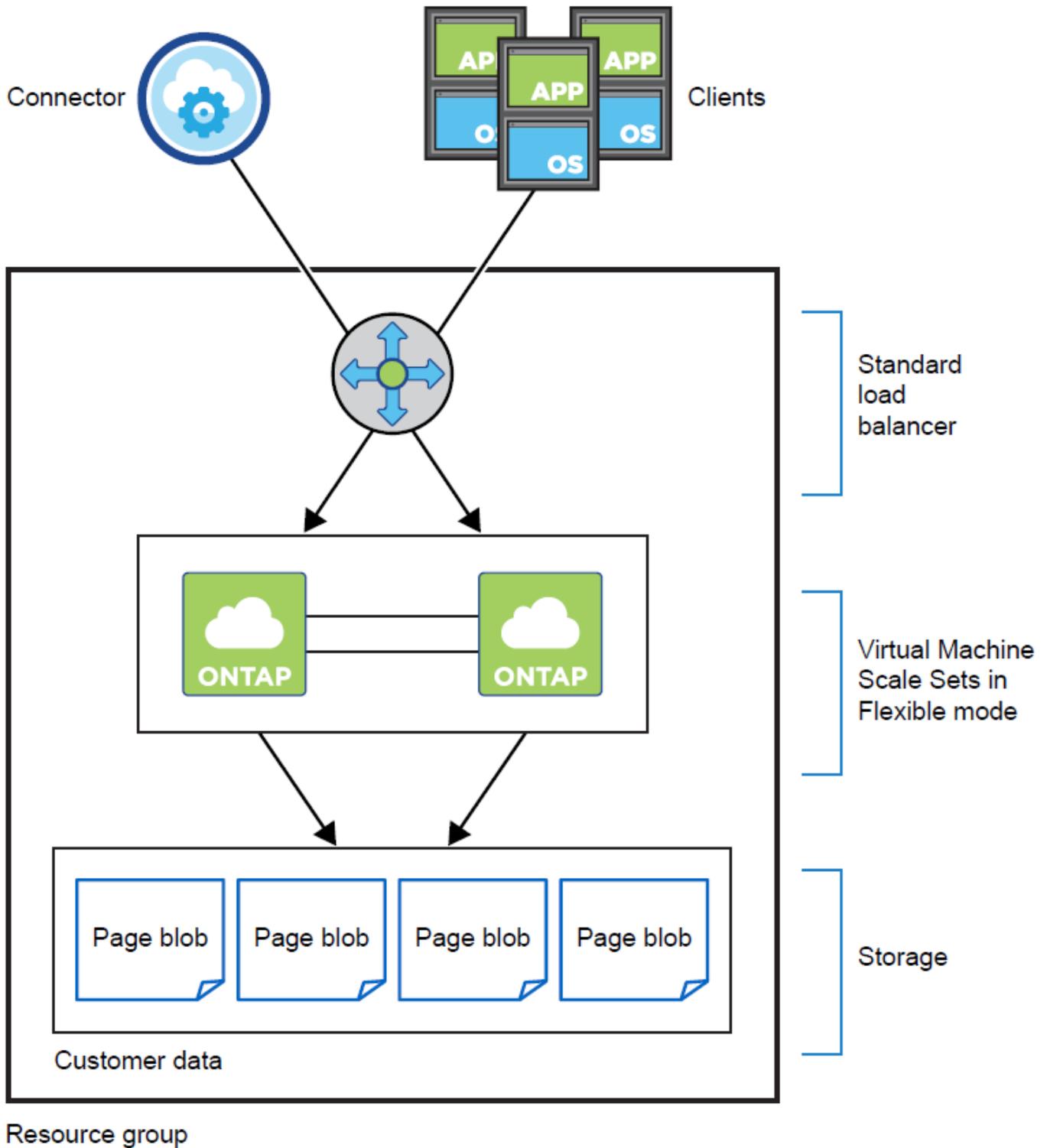
Pares de alta disponibilidade no Azure

Um par de alta disponibilidade (HA) da Cloud Volumes ONTAP fornece confiabilidade empresarial e operações contínuas em caso de falhas em seu ambiente de nuvem. No Azure, o storage é compartilhado entre os dois nós.

Componentes HA

Configuração de zona de disponibilidade única de HA com blobs de página

Uma configuração de blob de página HA do Cloud Volumes ONTAP no Azure inclui os seguintes componentes:



Observe o seguinte sobre os componentes do Azure que o BlueXP implanta para você:

Azure Standard Load Balancer

O balanceador de carga gerencia o tráfego de entrada para o par de HA do Cloud Volumes ONTAP.

VMs em zonas de disponibilidade únicas

A partir do Cloud Volumes ONTAP 9.15.1, você pode criar e gerenciar máquinas virtuais heterogêneas (VMs) em uma única zona de disponibilidade (AZ). Você pode implantar nós de alta disponibilidade (HA) em domínios de falha separados dentro da mesma AZ, garantindo a disponibilidade ideal. Para saber mais sobre o modo de orquestração flexível que permite essa capacidade, "[Documentação do Microsoft Azure: Conjuntos de escala de máquinas virtuais](#)" consulte .

Discos

Os dados do cliente residem nos blobs da página do Premium Storage. Cada nó tem acesso ao storage do outro nó. Também é necessário armazenamento adicional para "[dados de inicialização, raiz e núcleo](#)"o .

Contas de armazenamento

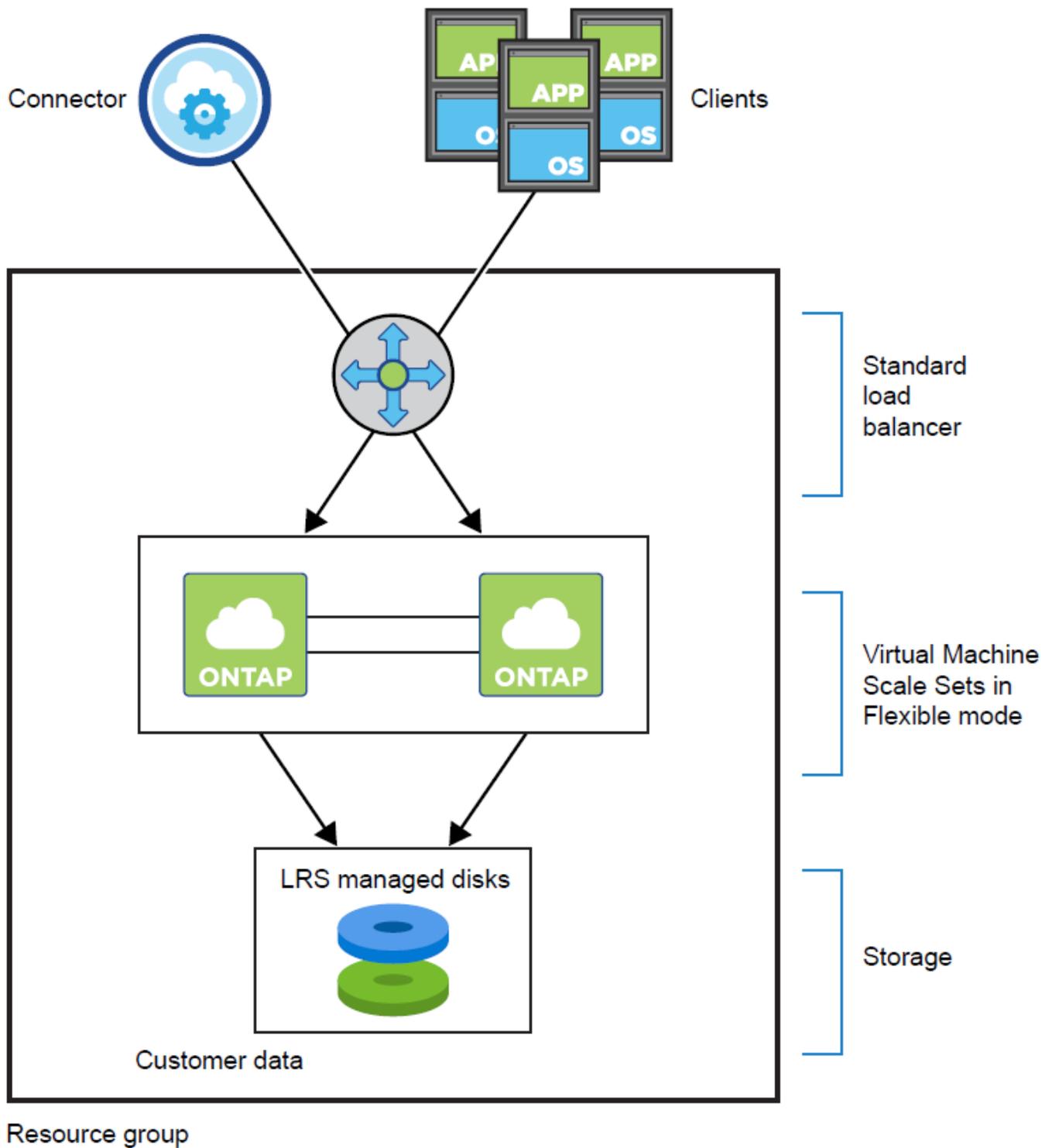
- Uma conta de armazenamento é necessária para discos gerenciados.
- Uma ou mais contas de armazenamento são necessárias para os blobs de página de armazenamento Premium, uma vez que o limite de capacidade de disco por conta de armazenamento é atingido.

["Documentação do Microsoft Azure: Escalabilidade do Azure Storage e metas de desempenho para contas de storage"](#).

- Uma conta de storage é necessária para a disposição de dados em categorias no storage Azure Blob.
- A partir do Cloud Volumes ONTAP 9,7, as contas de storage criadas pelo BlueXP para pares de HA são contas de storage v2 de uso geral.
- Você pode habilitar uma conexão HTTPS de um par de HA do Cloud Volumes ONTAP 9,7 para contas de storage do Azure ao criar um ambiente de trabalho. Observe que ativar essa opção pode afetar o desempenho de gravação. Não é possível alterar a configuração depois de criar o ambiente de trabalho.

Configuração de zona de disponibilidade única DE HA com discos gerenciados compartilhados

Uma configuração de zona de disponibilidade única do Cloud Volumes ONTAP HA executada em cima do disco gerenciado compartilhado inclui os seguintes componentes:



Observe o seguinte sobre os componentes do Azure que o BlueXP implanta para você:

Azure Standard Load Balancer

O balanceador de carga gerencia o tráfego de entrada para o par de HA do Cloud Volumes ONTAP.

VMs em zonas de disponibilidade únicas

A partir do Cloud Volumes ONTAP 9.15.1, você pode criar e gerenciar máquinas virtuais heterogêneas (VMs) em uma única zona de disponibilidade (AZ). Você pode implantar nós de alta disponibilidade (HA) em domínios de falha separados dentro da mesma AZ, garantindo a disponibilidade ideal. Para saber mais sobre o modo de orquestração flexível que permite essa capacidade, ["Documentação do Microsoft Azure:](#)

[Conjuntos de escala de máquinas virtuais](#)" consulte .

A implantação por zona usa discos gerenciados SSD Premium v2 quando as seguintes condições são atendidas:

- A versão do Cloud Volumes ONTAP é 9.15.1 ou posterior.
- A região e a zona selecionadas suportam discos gerenciados Premium SSD v2. Para obter informações sobre as regiões suportadas, ["Site do Microsoft Azure: Produtos disponíveis por região"](#) consulte .
- A subscrição está registada para a Microsoft ["Recurso Microsoft.Compute/VMOrchestratorZonalMultiFD"](#).

Discos

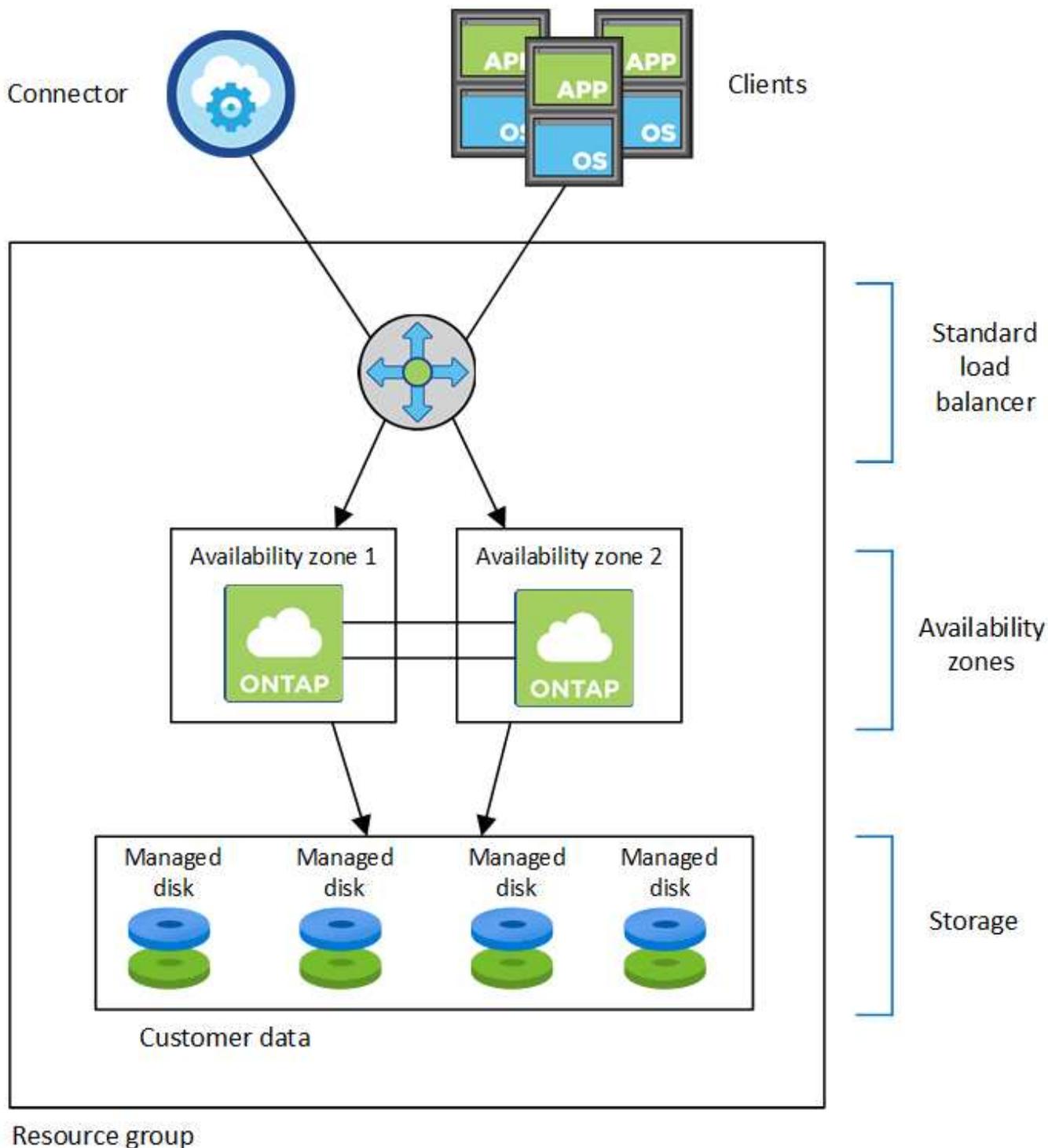
Os dados do cliente residem em discos gerenciados LRS (armazenamento localmente redundante). Cada nó tem acesso ao storage do outro nó. Também é necessário armazenamento adicional para ["Dados de inicialização, raiz, raiz do parceiro, núcleo e NVRAM"](#)o .

Contas de armazenamento

As contas de storage são usadas em implantações baseadas em disco gerenciado para gerenciar logs de diagnóstico e disposição em camadas no storage blob.

Configuração de várias zonas de disponibilidade de HA

Uma configuração de várias zonas de disponibilidade do Cloud Volumes ONTAP HA no Azure inclui os seguintes componentes:



Observe o seguinte sobre os componentes do Azure que o BlueXP implanta para você:

Azure Standard Load Balancer

O balanceador de carga gerencia o tráfego de entrada para o par de HA do Cloud Volumes ONTAP.

Zonas de disponibilidade

A configuração de várias zonas de disponibilidade DE HA utiliza um modelo de implantação em que dois nós de Cloud Volumes ONTAP são implantados em diferentes zonas de disponibilidade, garantindo que os nós estejam em diferentes domínios de falha para fornecer redundância e disponibilidade. Para saber como os conjuntos de escala de máquinas virtuais no modo de orquestração flexível podem usar zonas de

disponibilidade no Azure, "[Documentação do Microsoft Azure: Crie um conjunto de escala de Máquina Virtual que use zonas de disponibilidade](#)" consulte .

Discos

Os dados do cliente residem em discos gerenciados de armazenamento redundante de zona (ZRS). Cada nó tem acesso ao storage do outro nó. Também é necessário armazenamento adicional para "[dados de inicialização, raiz, raiz do parceiro e núcleo](#)"o .

Contas de armazenamento

As contas de storage são usadas em implantações baseadas em disco gerenciado para gerenciar logs de diagnóstico e disposição em camadas no storage blob.

RPO e rto

Uma configuração de HA mantém a alta disponibilidade dos dados da seguinte forma:

- O objetivo do ponto de restauração (RPO) é de 0 segundos. Seus dados são consistentes transacionalmente, sem perda de dados.
- O objetivo de tempo de recuperação (rto) é de 120 segundos. Em caso de interrupção, os dados devem estar disponíveis em 120 segundos ou menos.

Takeover de storage e giveback

Semelhante a um cluster físico do ONTAP, o storage em um par de HA do Azure é compartilhado entre nós. As conexões com o armazenamento do parceiro permitem que cada nó acesse o armazenamento do outro no caso de um *takeover*. Os mecanismos de failover de caminho de rede garantem que os clientes e hosts continuem a se comunicar com o nó sobrevivente. O parceiro *devolve* armazenamento quando o nó é colocado de volta na linha.

Para configurações nas, os endereços IP de dados são migrados automaticamente entre nós de HA se ocorrerem falhas.

Para iSCSI, o Cloud Volumes ONTAP usa e/S multipath (MPIO) e Acesso de Unidade lógica assimétrica (ALUA) para gerenciar o failover de caminho entre os caminhos otimizados para ativos e não otimizados.



Para obter informações sobre quais configurações de host específicas suportam ALUA, consulte o "[Ferramenta de Matriz de interoperabilidade do NetApp](#)" e o "[Guia de HOSTS DE SAN e clientes DE nuvem](#)" do sistema operacional do seu host.

Por padrão, o takeover, a resincronização e a giveback do storage são automáticos. Nenhuma ação do usuário é necessária.

Configurações de storage

Você pode usar um par de HA como uma configuração ativo-ativo, na qual ambos os nós fornecem dados aos clientes ou como uma configuração ativo-passivo, na qual o nó passivo responde às solicitações de dados somente se ele assumiu o storage do nó ativo.

Pares de alta disponibilidade no Google Cloud

Uma configuração de alta disponibilidade (HA) do Cloud Volumes ONTAP fornece operações ininterruptas e tolerância de falhas. No Google Cloud, os dados são

espelhados de forma síncrona entre os dois nós.

Componentes HA

As configurações do Cloud Volumes ONTAP HA no Google Cloud incluem os seguintes componentes:

- Dois nós de Cloud Volumes ONTAP cujos dados são espelhados de forma síncrona entre si.
- Uma instância de mediador que fornece um canal de comunicação entre os nós para auxiliar nos processos de takeover do storage e giveback.
- Uma ou três zonas (recomendado).

Se você escolher três zonas, os dois nós e o mediador estarão em zonas separadas do Google Cloud.

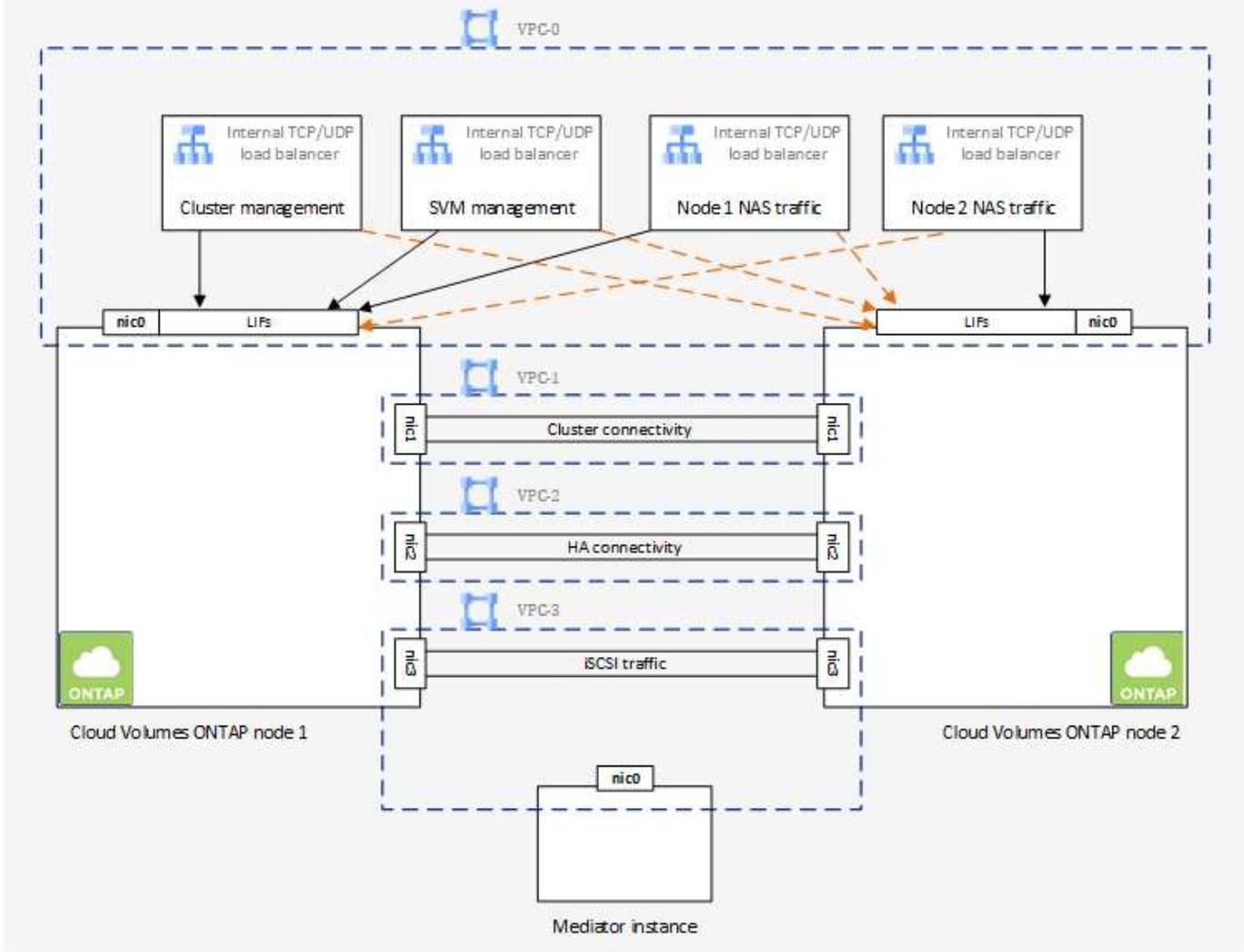
- Quatro nuvens privadas virtuais (VPCs).

A configuração usa quatro VPCs porque o GCP exige que cada interface de rede resida em uma rede VPC separada.

- Quatro balanceadores de carga internos do Google Cloud (TCP/UDP) que gerenciam o tráfego de entrada para o par de HA do Cloud Volumes ONTAP.

["Saiba mais sobre os requisitos de rede"](#), Incluindo mais detalhes sobre balanceadores de carga, VPCs, endereços IP internos, sub-redes e muito mais.

A imagem conceitual a seguir mostra um par de HA do Cloud Volumes ONTAP e seus componentes:



Mediador

Aqui estão alguns detalhes importantes sobre a instância de mediador no Google Cloud:

Tipo de instância

e2-micro (uma instância f1-micro foi usada anteriormente)

Discos

Dois discos persistentes padrão que são 10 GiB cada

Sistema operacional

Debian 11



Para o Cloud Volumes ONTAP 9.10.0 e versões anteriores, o Debian 10 foi instalado no mediador.

Atualizações

Quando você atualiza o Cloud Volumes ONTAP, o BlueXP também atualiza a instância do mediador conforme necessário.

Acesso à instância

Para o Debian, o usuário padrão da nuvem é `admin`. O Google Cloud cria e adiciona um certificado para `admin` o usuário quando o acesso SSH é solicitado através da linha de comando do Google Cloud Console ou `gcloud`. Você pode especificar `sudo` para obter Privileges raiz.

Agentes de terceiros

Agentes de terceiros ou extensões de VM não são suportados na instância do mediador.

Takeover de storage e giveback

Se um nó ficar inativo, o outro nó poderá fornecer dados para que seu parceiro forneça serviços de dados contínuos. Os clientes podem acessar os mesmos dados do nó do parceiro porque os dados foram espelhados de forma síncrona para o parceiro.

Depois que o nó for reiniciado, o parceiro deverá sincronizar novamente os dados antes que ele possa retornar o armazenamento. O tempo necessário para sincronizar novamente os dados depende da quantidade de dados alterados enquanto o nó estava inativo.

Por padrão, o takeover, a resincronização e a giveback do storage são automáticos. Nenhuma ação do usuário é necessária.

RPO e rto

Uma configuração de HA mantém a alta disponibilidade dos dados da seguinte forma:

- O objetivo do ponto de restauração (RPO) é de 0 segundos.

Seus dados são consistentes transacionalmente, sem perda de dados.

- O objetivo de tempo de recuperação (rto) é de 120 segundos.

Em caso de interrupção, os dados devem estar disponíveis em 120 segundos ou menos.

Modelos de IMPLANTAÇÃO DE HA

Você pode garantir a alta disponibilidade de seus dados implantando uma configuração de HA em várias zonas ou em uma única zona.

Várias zonas (recomendado)

A implantação de uma configuração de HA em três zonas garante a disponibilidade contínua dos dados em caso de falha em uma zona. Observe que o desempenho de gravação é um pouco menor em comparação com o uso de uma única zona, mas é mínimo.

Zona única

Quando implantada em uma única zona, uma configuração do Cloud Volumes ONTAP HA usa uma política de posicionamento de distribuição. Essa política garante que uma configuração de HA seja protegida de um ponto único de falha na zona, sem ter que usar zonas separadas para conseguir o isolamento de falhas.

Esse modelo de implantação reduz seus custos porque não há cobranças de saída de dados entre zonas.

Como o storage funciona em um par de HA

Ao contrário de um cluster do ONTAP, o storage em um par de HA do Cloud Volumes ONTAP no GCP não é compartilhado entre nós. Em vez disso, os dados são espelhados de forma síncrona entre os nós para que os dados estejam disponíveis em caso de falha.

Alocação de armazenamento

Quando você cria um novo volume e discos adicionais são necessários, o BlueXP aloca o mesmo número de discos para ambos os nós, cria um agregado espelhado e cria o novo volume. Por exemplo, se forem necessários dois discos para o volume, o BlueXP aloca dois discos por nó para um total de quatro discos.

Configurações de storage

Você pode usar um par de HA como uma configuração ativo-ativo, na qual ambos os nós fornecem dados aos clientes ou como uma configuração ativo-passivo, na qual o nó passivo responde a solicitações de dados somente se ele tiver ocupado o storage para o nó ativo.

Expectativas de performance para uma configuração de HA

Uma configuração do Cloud Volumes ONTAP HA replica sincronamente os dados entre nós, o que consome a largura de banda da rede. Como resultado, você pode esperar o seguinte desempenho em comparação com uma configuração de Cloud Volumes ONTAP de nó único:

- Para configurações de HA que atendem dados de apenas um nó, a performance de leitura é comparável à performance de leitura de uma configuração de nó único, enquanto a performance de gravação é menor.
- Para configurações de HA que atendem dados de ambos os nós, a performance de leitura é superior à performance de leitura de uma configuração de nó único, e a performance de gravação é igual ou superior.

Para obter mais detalhes sobre o desempenho do Cloud Volumes ONTAP, "[Desempenho](#)" consulte .

Acesso do cliente ao armazenamento

Os clientes devem acessar volumes NFS e CIFS usando o endereço IP de dados do nó no qual o volume reside. Se os clientes nas acessarem um volume usando o endereço IP do nó do parceiro, o tráfego vai entre os dois nós, o que reduz o desempenho.



Se você mover um volume entre nós em um par de HA, remonte o volume usando o endereço IP do outro nó. Caso contrário, você pode experimentar desempenho reduzido. Se os clientes suportarem referências NFSv4 ou redirecionamento de pastas para CIFS, você pode habilitar esses recursos nos sistemas Cloud Volumes ONTAP para evitar a reinstalação do volume. Para obter detalhes, consulte a documentação do ONTAP.

Você pode identificar facilmente o endereço IP correto por meio da opção *Mount Command* no painel gerenciar volumes no BlueXP .

Volume Actions

View volume details

Mount command

Clone volume

Edit volume tags

Edit volume settings

Delete volume

Protection Actions

Advanced Actions

Links relacionados

- ["Saiba mais sobre os requisitos de rede"](#)
- ["Saiba como começar a usar o GCP"](#)

Ações indisponíveis durante a aquisição

Quando um nó em um par de HA não está disponível, o outro nó fornece dados para seu parceiro fornecer serviço de dados contínuo. Isso é chamado *storage Takeover*. Várias ações ficam indisponíveis até que o armazenamento esteja concluído.



Quando um nó em um par de HA não está disponível, o estado do ambiente de trabalho no BlueXP é *degradado*.

As seguintes ações não estão disponíveis na takeover de storage da BlueXP :

- Registro de suporte
- Alterações de licença
- Alterações de tipo de instância ou VM
- Alterações de velocidade de gravação
- Configuração CIFS
- Alterar a localização dos backups de configuração
- Definir a palavra-passe do cluster
- Gerenciamento de discos e agregados (alocação avançada)

Essas ações estão disponíveis novamente após a conclusão do armazenamento de dados da giveback e o estado do ambiente de trabalho volta ao normal.

Segurança

O Cloud Volumes ONTAP é compatível com a criptografia de dados e oferece proteção contra vírus e ransomware.

Criptografia de dados em repouso

O Cloud Volumes ONTAP oferece suporte às seguintes tecnologias de criptografia:

- Soluções de criptografia NetApp (NVE e NAE)
- AWS Key Management Service
- Criptografia do Serviço de storage do Azure
- Criptografia padrão do Google Cloud Platform

Você pode usar as soluções de criptografia NetApp com criptografia nativa do seu provedor de nuvem, que criptografa os dados no nível do hipervisor. Fazer isso forneceria criptografia dupla, que pode ser desejada para dados muito confidenciais. Quando os dados criptografados são acessados, eles não são criptografados duas vezes, uma no nível do hipervisor (usando chaves do provedor de nuvem) e outra vez usando soluções de criptografia NetApp (usando chaves de um gerenciador de chaves externo).

Soluções de criptografia NetApp (NVE e NAE)

O Cloud Volumes ONTAP ["Criptografia de volume NetApp \(NVE\) e criptografia agregada NetApp \(NAE\)"](#) suporta . NVE e NAE são soluções baseadas em software que permitem a criptografia de volumes em repouso compatível com FIPS (140-2) em conformidade com dados em repouso de volumes. Tanto o NVE quanto o NAE usam criptografia AES de 256 bits.

- O NVE criptografa os dados em repouso um volume por vez. Cada volume de dados tem sua própria chave de criptografia exclusiva.
- O NAE é uma extensão do NVE - ele criptografa os dados para cada volume e os volumes compartilham uma chave no agregado. O NAE também permite que blocos comuns em todos os volumes do agregado

sejam desduplicados.

Tanto o NVE quanto o NAE são compatíveis com um gerenciador de chaves externo.

```
] endif::azure[] ifndef::gcp[] endif::gcp[
```

Os novos agregados têm a encriptação de agregados NetApp (NAE) ativada por predefinição depois de configurar um gestor de chaves externo. Novos volumes que não fazem parte de um agregado NAE terão a criptografia de volume NetApp (NVE) ativada por padrão (por exemplo, se você tiver agregados existentes que foram criados antes de configurar um gerenciador de chaves externo).

Configurar um gerenciador de chaves suportado é o único passo necessário. Para obter instruções de configuração, "[Criptografando volumes com soluções de criptografia NetApp](#)" consulte .

AWS Key Management Service

Ao iniciar um sistema Cloud Volumes ONTAP na AWS, é possível ativar a criptografia de dados usando o "[AWS Key Management Service \(KMS\)](#)". O BlueXP solicita chaves de dados usando uma chave mestra do cliente (CMK).



Não é possível alterar o método de criptografia de dados da AWS depois de criar um sistema Cloud Volumes ONTAP.

Se você quiser usar essa opção de criptografia, certifique-se de que o AWS KMS esteja configurado adequadamente. Para obter informações, "[Configurando o AWS KMS](#)" consulte .

Criptografia do Serviço de storage do Azure

Os dados são criptografados automaticamente no Cloud Volumes ONTAP no Azure usando "[Criptografia do Serviço de storage do Azure](#)" uma chave gerenciada pela Microsoft.

Você pode usar suas próprias chaves de criptografia, se preferir. "[Saiba como configurar o Cloud Volumes ONTAP para usar uma chave gerenciada pelo cliente no Azure](#)".

Criptografia padrão do Google Cloud Platform

"[Criptografia de dados em repouso do Google Cloud Platform](#)" É ativado por padrão para o Cloud Volumes ONTAP. Nenhuma configuração é necessária.

Embora o Google Cloud Storage sempre criptografe seus dados antes de serem gravados no disco, você pode usar as APIs do BlueXP para criar um sistema Cloud Volumes ONTAP que use *chaves de criptografia gerenciadas pelo cliente*. Essas são as chaves que você gera e gerencia no GCP usando o Cloud Key Management Service. "[Saiba mais](#)".

Verificação de vírus ONTAP

Você pode usar a funcionalidade de antivírus integrada em sistemas ONTAP para proteger os dados contra o comprometimento por vírus ou outros códigos maliciosos.

A verificação de vírus do ONTAP, chamada *Vscan*, combina o melhor software antivírus de terceiros com recursos do ONTAP que oferecem a flexibilidade necessária para controlar quais arquivos são verificados e quando.

Para obter informações sobre os fornecedores, software e versões compatíveis com o Vscan, consulte o

["Matriz de interoperabilidade do NetApp"](#).

Para obter informações sobre como configurar e gerenciar a funcionalidade antivírus em sistemas ONTAP, consulte o ["Guia de configuração do antivírus do ONTAP 9"](#).

Proteção contra ransomware

Os ataques de ransomware podem custar tempo, recursos e reputação aos negócios. Com o BlueXP, você implementa a solução NetApp para ransomware, que oferece ferramentas eficazes de visibilidade, detecção e correção.

- O BlueXP identifica volumes que não estão protegidos por uma política do Snapshot e permite ativar a política padrão do Snapshot nesses volumes.

As cópias snapshot são somente leitura, o que impede a corrupção de ransomware. Eles também podem fornecer a granularidade para criar imagens de uma única cópia de arquivo ou uma solução completa de recuperação de desastres.

- O BlueXP também permite bloquear extensões de arquivos ransomware comuns habilitando a solução FPolicy da ONTAP.

Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

1 Enable Snapshot Copy Protection



50 %
Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes

Activate Snapshot Policy

2 Block Ransomware File Extensions



ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

View Denied File Names

Activate FPolicy

["Saiba como implementar a solução NetApp para ransomware"](#).

Desempenho

Você pode analisar os resultados de performance para decidir quais workloads são apropriados para o Cloud Volumes ONTAP.

Relatórios técnicos de desempenho

- Cloud Volumes ONTAP para AWS

["Relatório Técnico da NetApp 4383: Caracterização de desempenho do Cloud Volumes ONTAP em Serviços Web da Amazon com cargas de trabalho de aplicativos"](#)

- Cloud Volumes ONTAP para Microsoft Azure

["Relatório técnico da NetApp 4671: Caracterização de desempenho do Cloud Volumes ONTAP no Azure com cargas de trabalho de aplicação"](#)

- [Cloud Volumes ONTAP para Google Cloud](#)

["Relatório técnico da NetApp 4816: Caracterização de desempenho do Cloud Volumes ONTAP para o Google Cloud"](#)

Desempenho da CPU

Os nós do Cloud Volumes ONTAP são altamente utilizados (mais de 90%) nas ferramentas de monitoramento do seu provedor de nuvem. Isso ocorre porque o ONTAP reserva todos os vCPUs apresentados à máquina virtual para que eles estejam disponíveis quando necessário.

Para obter informações, consulte a ["artigo da base de conhecimento do NetApp sobre como monitorar a utilização da CPU do ONTAP usando a CLI"](#)

Gerenciamento de licenças para BYOL baseado em nós

Cada sistema Cloud Volumes ONTAP que tenha uma licença bring Your own license (BYOL) baseada em nós precisa ter uma licença de sistema instalada com uma assinatura ativa. O BlueXP simplifica o processo gerenciando licenças para você e exibindo um aviso antes que elas expirem.



Uma licença baseada em nó é a geração anterior do BYOL para Cloud Volumes ONTAP. Uma licença baseada em nó está disponível apenas para renovações de licença.

["Saiba mais sobre as opções de licenciamento do Cloud Volumes ONTAP"](#).

["Saiba mais sobre como gerenciar licenças baseadas em nós"](#).

Licenças de sistema BYOL

Uma licença baseada em nó fornece até 368 TIB de capacidade para um único nó ou par de HA.

Você pode comprar várias licenças para um sistema BYOL da Cloud Volumes ONTAP para alocar mais de 368 TIB de capacidade. Por exemplo, você pode comprar duas licenças para alocar até 736 TIB de capacidade para o Cloud Volumes ONTAP. Ou você pode comprar quatro licenças para obter até 1,4 PIB.

O número de licenças que você pode comprar para um único sistema de nó ou par de HA é ilimitado.

Esteja ciente de que os limites de disco podem impedir que você alcance o limite de capacidade usando discos sozinhos. Você pode ir além do limite de disco pelo ["disposição em camadas dos dados inativos no storage de objetos"](#). Para obter informações sobre limites de disco, ["Limites de armazenamento nas Notas de versão do Cloud Volumes ONTAP"](#) consulte .

Gerenciamento de licenças para um novo sistema

Quando você cria um sistema BYOL baseado em nós, o BlueXP solicita o número de série da sua licença e da conta do site de suporte da NetApp. O BlueXP usa a conta para baixar o arquivo de licença do NetApp e instalá-lo no sistema Cloud Volumes ONTAP.

"Saiba como adicionar contas do site de suporte da NetApp ao BlueXP".

Se o BlueXP não conseguir aceder ao ficheiro de licença através da ligação segura à Internet, pode ["Obtenha o arquivo você mesmo e, em seguida, carregue manualmente o arquivo para o BlueXP"](#).

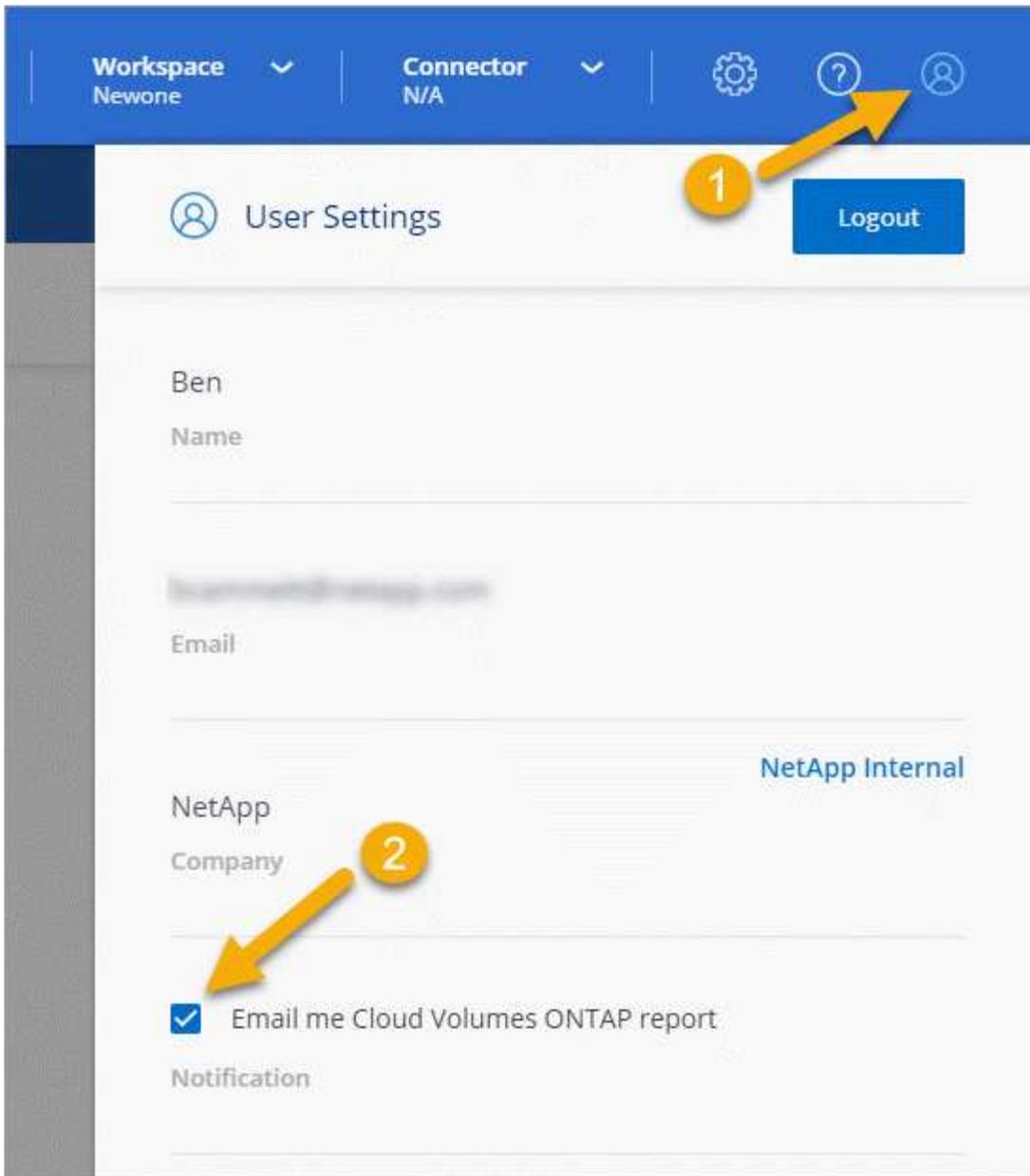
Expiração da licença

O BlueXP exibe um aviso 30 dias antes de uma licença baseada em nó expirar e novamente quando a licença expirar. A imagem a seguir mostra um aviso de expiração de 30 dias que aparece na interface do usuário:



Pode selecionar o ambiente de trabalho para rever a mensagem.

O BlueXP inclui um aviso de expiração de licença no relatório do Cloud Volumes ONTAP enviado por e-mail para você, se você for um administrador de conta ou organização do BlueXP e tiver ativado a opção:



O relatório enviado por e-mail inclui o aviso de expiração da licença a cada 2 semanas.

Se não renovar a licença a tempo, o sistema Cloud Volumes ONTAP desliga-se. Se você reiniciá-lo, ele se desliga novamente.

Renovação da licença

Quando você renova uma assinatura BYOL baseada em nós entrando em Contato com um representante da NetApp, a BlueXP obtém automaticamente a nova licença do NetApp e a instala no sistema Cloud Volumes ONTAP.

Se o BlueXP não conseguir aceder ao ficheiro de licença através da ligação segura à Internet, pode ["Obtenha o arquivo você mesmo e, em seguida, carregue manualmente o arquivo para o BlueXP"](#).

Transferência de licença para um novo sistema

Uma licença BYOL baseada em nó é transferível entre sistemas Cloud Volumes ONTAP quando você exclui um sistema existente e cria um novo usando a mesma licença.

Por exemplo, você pode querer excluir um sistema licenciado existente e, em seguida, usar a licença com um novo sistema BYOL em um VPC/VNet ou provedor de nuvem diferente. Observe que somente números de série *agnósticos na nuvem* funcionam em qualquer provedor de nuvem. Os números de série agnósticos em nuvem começam com o prefixo *908xxxx*.

É importante notar que sua licença BYOL está vinculada à sua empresa e a um conjunto específico de credenciais do site de suporte da NetApp.

AutoSupport e consultor digital

O componente AutoSupport do ONTAP coleta telemetria e envia-a para análise. O consultor digital da Active IQ (também conhecido como consultor digital) analisa os dados da AutoSupport e fornece cuidados e otimização proativos. Usando inteligência artificial, o Digital Advisor pode identificar possíveis problemas e ajudá-lo a resolvê-los antes que eles afetem seu negócio.

O Digital Advisor permite otimizar sua infraestrutura de dados em toda a nuvem híbrida global, fornecendo análises preditivas práticas e suporte proativo por meio de um portal baseado na nuvem e aplicativo móvel. Insights e recomendações orientados por dados do consultor digital estão disponíveis para todos os clientes da NetApp com um contrato de SupportEdge ativo (os recursos variam de acordo com o produto e a camada de suporte).

Aqui estão algumas coisas que você pode fazer com o Digital Advisor:

- Planejar atualizações.

O consultor digital identifica problemas no seu ambiente que podem ser resolvidos ao atualizar para uma versão mais recente do ONTAP e o componente do consultor de atualização ajuda você a Planejar uma atualização bem-sucedida.

- Veja o bem-estar do sistema.

Seu painel do Digital Advisor relata quaisquer problemas de bem-estar e ajuda você a corrigir esses problemas. Monitore a capacidade do sistema para garantir que você nunca fique sem espaço de armazenamento. Veja casos de suporte para o seu sistema.

- Gerenciar a performance.

O Digital Advisor mostra o desempenho do sistema por um período mais longo do que você pode ver no Gerenciador de sistemas do ONTAP. Identifique problemas de configuração e sistema que estejam afetando a performance. Maximizar a eficiência: Visualize as métricas de eficiência de storage e identifique maneiras de armazenar mais dados em menos espaço.

- Ver inventário e configuração.

O Digital Advisor exibe o inventário completo e as informações de configuração de software e hardware. Veja quando os contratos de serviço estão expirando e renove-os para garantir que você permaneça suportado.

Informações relacionadas

- ["Documentação do NetApp: Consultor digital"](#)
- ["Inicie o Digital Advisor"](#)
- ["Serviços da SupportEdge"](#)

Configuração padrão para Cloud Volumes ONTAP

Entender como o Cloud Volumes ONTAP é configurado por padrão pode ajudá-lo a configurar e administrar seus sistemas, especialmente se você estiver familiarizado com o ONTAP porque a configuração padrão do Cloud Volumes ONTAP é diferente do ONTAP.

Configuração predefinida

- O BlueXP cria uma VM de storage de fornecimento de dados quando implanta o Cloud Volumes ONTAP. Algumas configurações suportam VMs de storage adicionais. ["Saiba mais sobre como gerenciar VMs de armazenamento"](#).

A partir da versão do BlueXP 3.9.5, o relatório de espaço lógico é ativado na VM de storage inicial. Quando o espaço é relatado logicamente, o ONTAP relata o espaço de volume de modo que todo o espaço físico salvo pelos recursos de eficiência de storage também seja reportado como usado. Para obter informações sobre recursos de eficiência de storage in-line, consulte o artigo da base de conhecimento ["KB: Quais recursos de eficiência de armazenamento em linha são suportados pelo CVO?"](#)

- O BlueXP instala automaticamente as seguintes licenças de recurso do ONTAP no Cloud Volumes ONTAP:
 - CIFS
 - FlexCache
 - FlexClone
 - ISCSI
 - Gerenciamento de chaves de criptografia de vários locatários (MTEKM), começando com o Cloud Volumes ONTAP 9.12.1 GA
 - Criptografia de volume do NetApp (somente para sistemas traga sua própria licença (BYOL) ou pay-as-you-go registrado (PAYGO))
 - NFS `ifdef::aws[] endif::aws[] ifdef::azure[] endif::azure[]`
 - SnapMirror
 - SnapRestore
 - SnapVault
- Várias interfaces de rede são criadas por padrão:
 - Um LIF de gerenciamento de clusters
 - Um LIF entre clusters
- LIF de gerenciamento de SVM em sistemas de HA no Azure
- LIF de gerenciamento de SVM em sistemas de HA no Google Cloud
- LIF de gerenciamento de SVM em sistemas de nó único na AWS

- Um LIF de gerenciamento de nós

No Google Cloud, esse LIF é combinado com o LIF entre clusters.

- Um iSCSI data LIF
- LIF de dados CIFS e NFS



O failover de LIF é desativado por padrão para o Cloud Volumes ONTAP devido aos requisitos do provedor de nuvem. A migração de um LIF para uma porta diferente rompe o mapeamento externo entre endereços IP e interfaces de rede na instância, tornando o LIF inacessível.

- O Cloud Volumes ONTAP envia backups de configuração para o conetor usando HTTP.

Os backups são acessíveis a partir do `http://ipaddress/occm/offboxconfig/` onde *ipaddress* é o endereço IP do host do conetor.

Você pode usar os backups para reconfigurar seu sistema Cloud Volumes ONTAP. Para obter mais informações sobre backups de configuração, "[Documentação do ONTAP](#)" consulte .

- O BlueXP define alguns atributos de volume de maneira diferente de outras ferramentas de gerenciamento (Gerenciador de sistema do ONTAP ou CLI do ONTAP, por exemplo).

A tabela a seguir lista os atributos de volume que o BlueXP define de forma diferente dos padrões:

Atributo	Valor definido por BlueXP
Modo de tamanho automático	crescer
Dimensionamento automático máximo	1.000 por cento A Organização BlueXP ou o administrador da conta pode modificar esse valor a partir da página Configurações.
Estilo de segurança	NTFS para volumes CIFS UNIX para volumes NFS
Estilo de garantia de espaço	nenhum
Permissões UNIX (somente NFS)	777

+

Para obter informações sobre esses atributos, "[ONTAP volume criar man page](#)" consulte .

Discos internos para dados do sistema

Além do storage para dados do usuário, a BlueXP também compra storage de nuvem para dados do sistema.

AWS

- Três discos por nó para dados de inicialização, raiz e núcleo:
 - 47 gib IO1 disco para dados de inicialização
 - 140 gib disco GP3 para dados de raiz
 - 540 gib disco GP2 para dados do núcleo
- Para pares de HA:
 - Dois volumes st1 do EBS para a instância do mediador, um de aproximadamente 8 GiB como disco raiz e um de 4 GiB como disco de dados
 - Um disco 140 gib GP3 em cada nó para conter uma cópia dos dados raiz do outro nó



Em algumas zonas, o tipo de disco EBS disponível só pode ser GP2.

- Um instantâneo EBS para cada disco de arranque e disco raiz



Os instantâneos são criados automaticamente após a reinicialização.

- Quando você ativa a criptografia de dados na AWS usando o Serviço de Gerenciamento de chaves (KMS), os discos de inicialização e raiz do Cloud Volumes ONTAP também são criptografados. Isso inclui o disco de inicialização da instância de mediador em um par de HA. Os discos são criptografados usando o CMK selecionado quando você cria o ambiente de trabalho.



Na AWS, o NVRAM está no disco de inicialização.

Azure (nó único)

- Três discos SSD premium:
 - Um disco 10 GiB para dados de inicialização
 - Um disco de 140 GiB para dados de raiz
 - Um disco de 512 GiB para NVRAM

Se a máquina virtual que você escolheu para o Cloud Volumes ONTAP oferecer suporte a SSDs Ultra, o sistema usará um SSD Ultra de 32 GiB para NVRAM, em vez de um SSD premium.

- Um disco rígido padrão de 1024 GiB para guardar núcleos
- Um snapshot do Azure para cada disco de inicialização e disco raiz
- Por padrão, cada disco no Azure é criptografado em repouso.

Se a máquina virtual que você escolheu para o Cloud Volumes ONTAP oferecer suporte ao disco gerenciado Premium SSD v2 como discos de dados, o sistema usará um disco gerenciado de 32 GB SSD premium v2 para NVRAM e outro como disco raiz.

Azure (par de HA)

HA pares com blob de página

- Dois discos SSD premium de 10 GiB para o volume de inicialização (um por nó)
- Dois blobs de página de armazenamento Premium de 140 GiB para o volume raiz (um por nó)
- Dois discos HDD padrão de 1024 GiB para salvar núcleos (um por nó)
- Dois discos SSD premium de 512 GiB para NVRAM (um por nó)
- Um snapshot do Azure para cada disco de inicialização e disco raiz



Os instantâneos são criados automaticamente após a reinicialização.

- Por padrão, cada disco no Azure é criptografado em repouso.

Pares DE HA com discos gerenciados compartilhados em várias zonas de disponibilidade

- Dois discos SSD premium de 10 GiB para o volume de inicialização (um por nó)
- Dois discos SSD premium de 512 GiB para o volume raiz (um por nó)
- Dois discos HDD padrão de 1024 GiB para salvar núcleos (um por nó)
- Dois discos SSD premium de 512 GiB para NVRAM (um por nó)
- Um snapshot do Azure para cada disco de inicialização e disco raiz



Os instantâneos são criados automaticamente após a reinicialização.

- Por padrão, cada disco no Azure é criptografado em repouso.

Pares DE HA com discos gerenciados compartilhados em zonas de disponibilidade únicas

- Dois discos SSD premium de 10 GiB para o volume de inicialização (um por nó)
- Dois discos gerenciados compartilhados SSD Premium de 512 GiB para o volume raiz (um por nó)
- Dois discos HDD padrão de 1024 GiB para salvar núcleos (um por nó)
- Dois discos gerenciados SSD premium de 512 GiB para NVRAM (um por nó)

Se a sua máquina virtual suportar discos gerenciados SSD premium v2 como discos de dados, ela usará 32 discos gerenciados SSD premium v2 GiB para NVRAM e 512 discos gerenciados compartilhados SSD premium v2 GiB para o volume raiz.

Você pode implantar pares de HA em uma única zona de disponibilidade e usar discos gerenciados SSD v2 Premium quando as seguintes condições forem atendidas:

- A versão do Cloud Volumes ONTAP é 9.15.1 ou posterior.
- A região e a zona selecionadas suportam discos gerenciados Premium SSD v2. Para obter informações sobre as regiões suportadas, "[Site do Microsoft Azure: Produtos disponíveis por região](#)" consulte .
- A subscrição está registada para a Microsoft "[Recurso Microsoft.Compute/VMOrchestratorZonalMultiFD](#)".

Google Cloud (nó único)

- Um disco persistente SSD de 10 GiB para dados de inicialização
- Um disco persistente SSD de 64 GiB para dados de raiz

- Um disco persistente SSD de 500 GiB para NVRAM
- Um disco persistente padrão de 315 GiB para salvar núcleos
- Snapshots para dados de inicialização e raiz



Os instantâneos são criados automaticamente após a reinicialização.

- Os discos de inicialização e raiz são criptografados por padrão.

Google Cloud (par de HA)

- Dois discos persistentes SSD de 10 GiB para dados de inicialização
- Quatro discos persistentes SSD de 64 GiB para dados de raiz
- Dois discos persistentes SSD de 500 GiB para NVRAM
- Dois discos persistentes padrão de 315 GiB para salvar núcleos
- Um disco persistente padrão de 10 GiB para dados de mediador
- Um disco persistente padrão 10 GiB para dados de inicialização do mediador
- Snapshots para dados de inicialização e raiz



Os instantâneos são criados automaticamente após a reinicialização.

- Os discos de inicialização e raiz são criptografados por padrão.

Onde residem os discos

O BlueXP estabelece o armazenamento da seguinte forma:

- Os dados de inicialização residem em um disco conectado à instância ou à máquina virtual.

Este disco, que contém a imagem de arranque, não está disponível para o Cloud Volumes ONTAP.

- Os dados de raiz, que contêm a configuração e os logs do sistema, residem no aggr0.
- O volume raiz da máquina virtual de storage (SVM) reside no aggr1.
- Os volumes de dados também residem em aggr1.

Conhecimento e apoio

Registre-se para obter suporte

O Registro de suporte é necessário para receber suporte técnico específico da BlueXP e de suas soluções e serviços de storage. O Registro de suporte também é necessário para habilitar fluxos de trabalho importantes para sistemas Cloud Volumes ONTAP.

O Registro para suporte não ativa o suporte do NetApp para um serviço de arquivos de provedor de nuvem. Para obter suporte técnico relacionado a um serviço de arquivo de provedor de nuvem, sua infraestrutura ou qualquer solução usando o serviço, consulte "obter ajuda" na documentação do BlueXP para esse produto.

- ["Amazon FSX para ONTAP"](#)
- ["Azure NetApp Files"](#)
- ["Cloud Volumes Service para Google Cloud"](#)

Visão geral do Registro de suporte

Existem duas formas de Registro para ativar o direito de suporte:

- Registrar o número de série da sua conta BlueXP (o número de série 960xxxxxxxx de 20 dígitos localizado na página recursos de suporte no BlueXP).

Isso serve como seu ID de assinatura de suporte único para qualquer serviço no BlueXP . Cada assinatura de suporte no nível de conta do BlueXP deve ser registrada.

- Registrando os números de série do Cloud Volumes ONTAP associados a uma assinatura no mercado do seu provedor de nuvem (estes são números de série de 20 dígitos 909201xxxxxxxx).

Esses números de série são comumente referidos como *PAYGO serial numbers* e são gerados pelo BlueXP no momento da implantação do Cloud Volumes ONTAP.

Registrar ambos os tipos de números de série permite recursos como abrir tickets de suporte e geração automática de casos. O Registro é concluído adicionando contas do site de suporte da NetApp (NSS) ao BlueXP , conforme descrito abaixo.

Registre o BlueXP para obter suporte ao NetApp

Para se Registrar para obter suporte e ativar o direito de suporte, um usuário em sua organização (ou conta) do BlueXP deve associar uma conta do site de suporte da NetApp ao login do BlueXP . A forma como você se Registra no suporte da NetApp depende se você já tem uma conta do site de suporte da NetApp (NSS).

Cliente existente com uma conta NSS

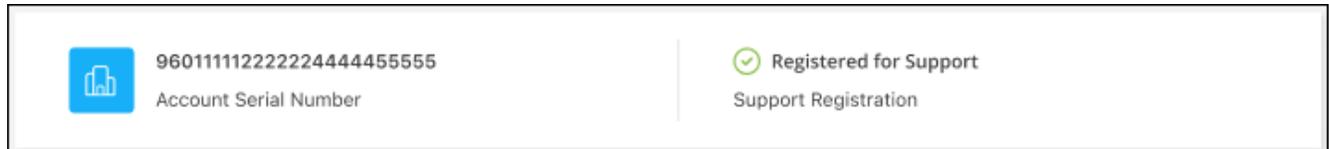
Se você é um cliente da NetApp com uma conta NSS, você simplesmente precisa se Registrar para obter suporte através do BlueXP .

Passos

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.
2. Selecione **credenciais do usuário**.

3. Selecione **Adicionar credenciais NSS** e siga o prompt de autenticação do site de suporte da NetApp (NSS).
4. Para confirmar que o processo de Registro foi bem-sucedido, selecione o ícone Ajuda e selecione **suporte**.

A página **recursos** deve mostrar que sua organização do BlueXP está registrada para suporte.



Observe que outros usuários do BlueXP não verão esse mesmo status de Registro de suporte se não tiverem associado uma conta do site de suporte da NetApp ao login do BlueXP . No entanto, isso não significa que sua organização do BlueXP não esteja registrada para suporte. Desde que um usuário na organização tenha seguido esses passos, sua organização foi registrada.

Cliente existente, mas sem conta NSS

Se você já é um cliente NetApp com licenças e números de série existentes, mas *no* conta NSS, você precisa criar uma conta NSS e associá-la ao seu login no BlueXP .

Passos

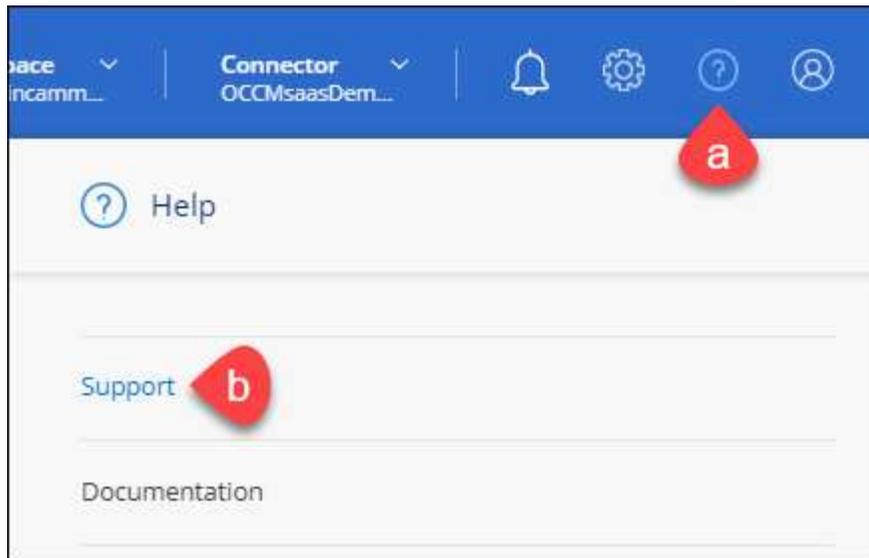
1. Crie uma conta do site de suporte da NetApp preenchendo o. "[Formulário de Registro do usuário do site de suporte da NetApp](#)"
 - a. Certifique-se de selecionar o nível de usuário apropriado, que normalmente é **Cliente NetApp/Usuário final**.
 - b. Certifique-se de copiar o número de série da conta BlueXP (960xxxx) usado acima para o campo de número de série. Isto irá acelerar o processamento da conta.
2. Associe a sua nova conta NSS ao seu login no BlueXP executando as etapas em [Cliente existente com uma conta NSS](#).

Novo na NetApp

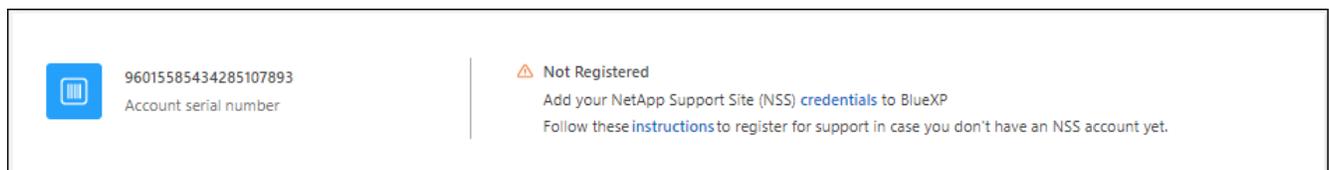
Se você é novo no NetApp e não tem uma conta NSS, siga cada passo abaixo.

Passos

1. No canto superior direito do console do BlueXP , selecione o ícone Ajuda e selecione **suporte**.



2. Localize o número de série da ID da conta na página Registro de suporte.



3. Navegue "[Site de Registro de suporte da NetApp](#)" e selecione **não sou um Cliente NetApp registrado**.

4. Preencha os campos obrigatórios (aqueles com asteriscos vermelhos).

5. No campo **linha de produtos**, selecione **Cloud Manager** e, em seguida, selecione seu provedor de cobrança aplicável.

6. Copie o número de série da sua conta a partir da etapa 2 acima, complete a verificação de segurança e confirme se leu a Política de Privacidade de dados globais da NetApp.

Um e-mail é enviado imediatamente para a caixa de correio fornecida para finalizar esta transação segura. Certifique-se de verificar suas pastas de spam se o e-mail de validação não chegar em poucos minutos.

7. Confirme a ação a partir do e-mail.

A confirmação envia sua solicitação à NetApp e recomenda que você crie uma conta do site de suporte da NetApp.

8. Crie uma conta do site de suporte da NetApp preenchendo o. "[Formulário de Registro do usuário do site de suporte da NetApp](#)"

a. Certifique-se de selecionar o nível de usuário apropriado, que normalmente é **Cliente NetApp/Usuário final**.

b. Certifique-se de copiar o número de série da conta (960xxxx) usado acima para o campo de número de série. Isto irá acelerar o processamento.

Depois de terminar

O NetApp deve entrar em Contato com você durante esse processo. Este é um exercício de integração única para novos usuários.

Depois de ter sua conta do site de suporte da NetApp, associe a conta ao login do BlueXP , executando as

etapas em [Cliente existente com uma conta NSS](#).

Associar credenciais NSS para suporte ao Cloud Volumes ONTAP

A associação das credenciais do site de suporte da NetApp à sua organização do BlueXP é necessária para ativar os seguintes fluxos de trabalho principais para o Cloud Volumes ONTAP:

- Registro de sistemas Cloud Volumes ONTAP de pagamento conforme o uso para suporte

Fornecer sua conta NSS é necessário para ativar o suporte para o seu sistema e para obter acesso aos recursos de suporte técnico da NetApp.

- Implantando o Cloud Volumes ONTAP quando você traz sua própria licença (BYOL)

É necessário fornecer a sua conta NSS para que o BlueXP possa carregar a sua chave de licença e ativar a subscrição para o período que adquiriu. Isso inclui atualizações automáticas para renovações de prazo.

- Atualizar o software Cloud Volumes ONTAP para a versão mais recente

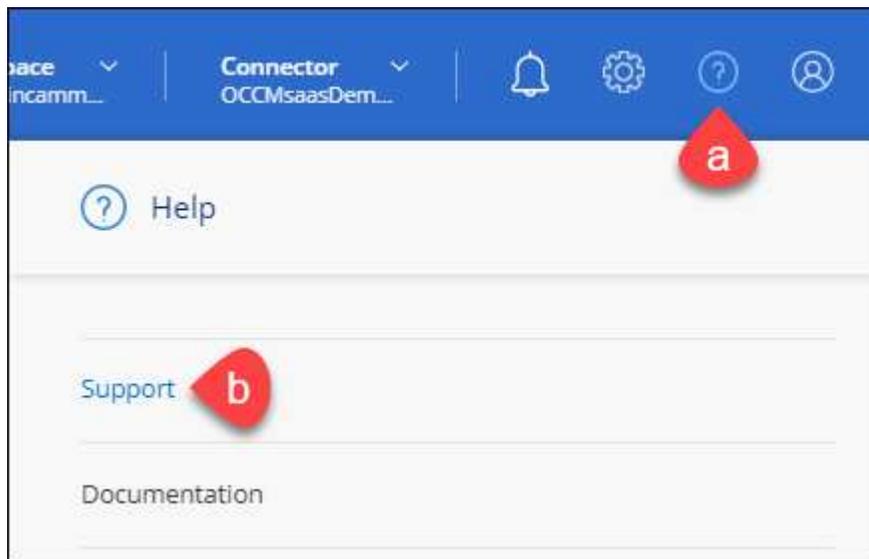
Associar credenciais NSS à sua organização do BlueXP é diferente da conta NSS associada a um login de usuário do BlueXP .

Essas credenciais do NSS estão associadas ao ID específico da organização do BlueXP . Os utilizadores que pertencem à organização BlueXP podem aceder a estas credenciais a partir de **suporte > Gestão NSS**.

- Se você tiver uma conta no nível do cliente, pode adicionar uma ou mais contas NSS.
- Se você tiver uma conta de parceiro ou revendedor, você pode adicionar uma ou mais contas NSS, mas elas não podem ser adicionadas ao lado de contas de nível de cliente.

Passos

1. No canto superior direito do console do BlueXP , selecione o ícone Ajuda e selecione **suporte**.



2. Selecione **NSS Management > Add NSS Account** (Gestão NSS > Adicionar conta NSS*).
3. Quando for solicitado, selecione **continuar** para ser redirecionado para uma página de login da Microsoft.

O NetApp usa o Microsoft Entra ID como provedor de identidade para serviços de autenticação

específicos para suporte e licenciamento.

4. Na página de login, forneça seu endereço de e-mail e senha registrados no site de suporte da NetApp para executar o processo de autenticação.

Essas ações permitem que o BlueXP use sua conta NSS para tarefas como downloads de licenças, verificação de atualização de software e futuros Registros de suporte.

Observe o seguinte:

- A conta NSS tem de ser uma conta ao nível do cliente (não uma conta de convidado ou temporária). Você pode ter várias contas NSS no nível do cliente.
- Só pode haver uma conta NSS se essa conta for uma conta de nível de parceiro. Se você tentar adicionar contas NSS no nível do cliente e existir uma conta no nível do parceiro, você receberá a seguinte mensagem de erro:

"O tipo de cliente NSS não é permitido para esta conta, uma vez que já existem utilizadores NSS de tipo diferente."

O mesmo acontece se você tiver contas NSS pré-existentes no nível do cliente e tentar adicionar uma conta no nível do parceiro.

- Após o login bem-sucedido, o NetApp armazenará o nome de usuário do NSS.

Este é um ID gerado pelo sistema que mapeia para o seu e-mail. Na página **NSS Management**, você pode exibir seu e-mail no ******* menu.

- Se você precisar atualizar seus tokens de credenciais de login, há também uma opção **Atualizar credenciais** ******* no menu.

Usando esta opção, você solicita que você faça login novamente. Observe que o token para essas contas expira após 90 dias. Uma notificação será postada para alertá-lo sobre isso.

Obtenha ajuda

A NetApp oferece suporte ao BlueXP e seus serviços de nuvem de várias maneiras. Amplas opções gratuitas de suporte autônomo estão disponíveis 24 horas por dia, 7 dias por semana, como artigos da base de conhecimento (KB) e um fórum da comunidade. O seu registro de suporte inclui suporte técnico remoto através de Bilheteira na Web.

Obtenha suporte para um serviço de arquivos do provedor de nuvem

Para obter suporte técnico relacionado a um serviço de arquivo de provedor de nuvem, sua infraestrutura ou qualquer solução usando o serviço, consulte "obter ajuda" na documentação do BlueXP para esse produto.

- ["Amazon FSX para ONTAP"](#)
- ["Azure NetApp Files"](#)
- ["Cloud Volumes Service para Google Cloud"](#)

Para receber suporte técnico específico da BlueXP e de suas soluções e serviços de storage, use as opções de suporte descritas abaixo.

Use opções de suporte autônomo

Estas opções estão disponíveis gratuitamente, 24 horas por dia, 7 dias por semana:

- Documentação

A documentação do BlueXP que você está visualizando no momento.

- ["Base de conhecimento"](#)

PESQUISE na base de conhecimento do BlueXP para encontrar artigos úteis para solucionar problemas.

- ["Comunidades"](#)

Junte-se à comunidade BlueXP para seguir as discussões em curso ou criar novas.

Crie um caso com o suporte do NetApp

Além das opções de suporte autônomo acima, você pode trabalhar com um especialista de suporte da NetApp para resolver quaisquer problemas depois de ativar o suporte.

Antes de começar

- Para usar o recurso **criar um caso**, primeiro você deve associar suas credenciais do site de suporte da NetApp ao login do BlueXP . ["Saiba como gerenciar credenciais associadas ao seu login no BlueXP"](#).
- Se você estiver abrindo um caso para um sistema ONTAP com um número de série, sua conta NSS deve estar associada ao número de série desse sistema.

Passos

1. No BlueXP , selecione **Ajuda > suporte**.
 2. Na página **recursos**, escolha uma das opções disponíveis em suporte técnico:
 - a. Selecione **Ligue para nós** se quiser falar com alguém no telefone. Você será direcionado para uma página no NetApp.com que lista os números de telefone que você pode ligar.
 - b. Selecione **criar um caso** para abrir um ticket com um especialista em suporte da NetApp:
 - **Serviço**: Selecione o serviço ao qual o problema está associado. Por exemplo, BlueXP quando específico para um problema de suporte técnico com fluxos de trabalho ou funcionalidade dentro do serviço.
 - **Ambiente de trabalho**: Se aplicável ao armazenamento, selecione **Cloud Volumes ONTAP** ou **no local** e, em seguida, o ambiente de trabalho associado.

A lista de ambientes de trabalho está dentro do escopo da organização (ou conta) do BlueXP , do projeto (ou da área de trabalho) e do conector que você selecionou no banner superior do serviço.
- **Prioridade do caso**: Escolha a prioridade para o caso, que pode ser baixa, média, alta ou Crítica.

Para saber mais detalhes sobre essas prioridades, passe o Mouse sobre o ícone de informações ao lado do nome do campo.
 - **Descrição do problema**: Forneça uma descrição detalhada do seu problema, incluindo quaisquer mensagens de erro aplicáveis ou etapas de solução de problemas que você executou.
 - **Endereços de e-mail adicionais**: Insira endereços de e-mail adicionais se você quiser que outra

pessoa saiba sobre esse problema.

- **Anexo (Opcional):** Carregue até cinco anexos, um de cada vez.

Os anexos estão limitados a 25 MB por ficheiro. As seguintes extensões de arquivo são suportadas: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.

The screenshot shows a web form for creating a support case. At the top, it says 'ntapitdemo' with an edit icon and 'NetApp Support Site Account'. Below this is a horizontal line. There are two dropdown menus: 'Service' with 'Select' and 'Working Enviroment' (note the typo) with 'Select'. Below these is a 'Case Priority' dropdown with 'Low - General guidance' and an information icon. The 'Issue Description' section has a text area with the placeholder text: 'Provide detailed description of problem, applicable error messages and troubleshooting steps taken.' Below that is an 'Additional Email Addresses (Optional)' text input field with 'Type here' and an information icon. At the bottom is an 'Attachment (Optional)' section with 'No files selected', an 'Upload' button with an upward arrow icon, and a trash can icon with a hand cursor over it.

Depois de terminar

Um pop-up aparecerá com o número do seu caso de suporte. Um especialista em suporte da NetApp irá rever o seu caso e voltar para você em breve.

Para obter um histórico de seus casos de suporte, você pode selecionar **Configurações > linha do tempo** e procurar ações chamadas "criar caso de suporte". Um botão à direita permite expandir a ação para ver detalhes.

É possível que você encontre a seguinte mensagem de erro ao tentar criar um caso:

"Você não está autorizado a criar um caso contra o serviço selecionado"

Esse erro pode significar que a conta NSS e a empresa de Registro com a qual está associada não são a mesma empresa de Registro para o número de série da conta BlueXP (ou seja. 960xxxx) ou o número de

série do ambiente de trabalho. Pode procurar assistência utilizando uma das seguintes opções:

- Use o chat no produto
- Envie um caso não técnico em <https://mysupport.netapp.com/site/help>

Gerenciar seus casos de suporte (prévia)

Você pode visualizar e gerenciar casos de suporte ativos e resolvidos diretamente do BlueXP . Você pode gerenciar os casos associados à sua conta NSS e à sua empresa.

O gerenciamento de casos está disponível como uma prévia. Planejamos refinar essa experiência e adicionar melhorias nos próximos lançamentos. Por favor, envie-nos feedback usando o chat no produto.

Observe o seguinte:

- O painel de gerenciamento de casos na parte superior da página oferece duas visualizações:
 - A vista à esquerda mostra o total de casos abertos nos últimos 3 meses pela conta do usuário NSS que você forneceu.
 - A visualização à direita mostra o total de casos abertos nos últimos 3 meses ao nível da sua empresa com base na sua conta NSS de utilizador.

Os resultados na tabela refletem os casos relacionados à exibição selecionada.

- Você pode adicionar ou remover colunas de interesse e pode filtrar o conteúdo de colunas como prioridade e Status. Outras colunas fornecem apenas capacidades de ordenação.

Veja os passos abaixo para obter mais detalhes.

- Em um nível por caso, oferecemos a capacidade de atualizar notas de caso ou fechar um caso que ainda não esteja no status fechado ou pendente fechado.

Passos

1. No BlueXP , selecione **Ajuda > suporte**.
2. Selecione **Gerenciamento de casos** e, se for solicitado, adicione sua conta NSS ao BlueXP .

A página **Gerenciamento de casos** mostra casos abertos relacionados à conta NSS associada à conta de usuário do BlueXP . Esta é a mesma conta NSS que aparece na parte superior da página **NSS Management**.

3. Opcionalmente, modifique as informações exibidas na tabela:
 - Em **casos da organização**, selecione **Exibir** para ver todos os casos associados à sua empresa.
 - Modifique o intervalo de datas escolhendo um intervalo de datas exato ou escolhendo um intervalo de tempo diferente.

Search: Cases opened on the last 3 months Create a case

Date created	Last updated	Priority	Status (5)	
December 22, 2022	December 29, 2022	Medium (P3)	Assigned	...
December 21, 2022	December 28, 2022	Medium (P3)	Active	...
December 15, 2022	December 27, 2022	Medium (P3)	Pending customer	...
December 14, 2022	December 26, 2022	Low (P4)	Solution proposed	...

- Filtre o conteúdo das colunas.

Search: Cases opened on the last 3 months Create a case

Last updated	Priority	Status (5)	
December 29, 2022	Critical (P1)	Active	...
December 28, 2022	High (P2)	Pending customer	...
December 27, 2022	Medium (P3)	Solution proposed	...
December 26, 2022	Low (P4)	Pending closed	...
		Closed	...

- Altere as colunas que aparecem na tabela selecionando  e escolhendo as colunas que você deseja exibir.

Search: Cases opened on the last 3 months Create a case

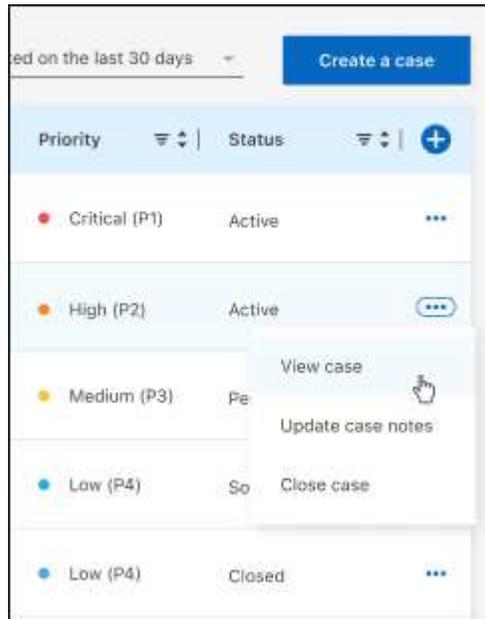
Last updated	Priority	Status (5)	
December 29, 2022	Critical (P1)	Last updated	...
December 28, 2022	High (P2)	Priority	...
December 27, 2022	Medium (P3)	Cluster name	...
December 26, 2022	Low (P4)	Case owner	...
		Opened by	...

4. Gerencie um caso existente ●●●selecionando e selecionando uma das opções disponíveis:

- **Ver caso:** Veja detalhes completos sobre um caso específico.
- * Atualizar notas de caso*: Forneça detalhes adicionais sobre o seu problema ou selecione **carregar arquivos** para anexar até um máximo de cinco arquivos.

Os anexos estão limitados a 25 MB por ficheiro. As seguintes extensões de arquivo são suportadas: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.

- * Fechar caso*: Forneça detalhes sobre por que você está fechando o caso e selecione **Fechar caso**.



Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

Direitos de autor

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marcas comerciais

NetApp, o logotipo DA NetApp e as marcas listadas na página de marcas comerciais da NetApp são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Patentes

Uma lista atual de patentes de propriedade da NetApp pode ser encontrada em:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Política de privacidade

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

Código aberto

Os arquivos de aviso fornecem informações sobre direitos autorais de terceiros e licenças usadas no software NetApp.

- ["Aviso para BlueXP"](#)
- ["Aviso para o Cloud Volumes ONTAP"](#)
- ["Aviso para ONTAP"](#)

Informações sobre direitos autorais

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

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

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU 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.