



Documentação do Cloud Volumes ONTAP

Cloud Volumes ONTAP

NetApp
October 06, 2025

This PDF was generated from <https://docs.netapp.com/pt-br/storage-management-cloud-volumes-ontap/index.html> on October 06, 2025. Always check docs.netapp.com for the latest.

Índice

Documentação do Cloud Volumes ONTAP	1
Notas de lançamento	2
Novidades no Cloud Volumes ONTAP	2
6 de outubro de 2025	2
4 de setembro de 2025	2
11 de agosto de 2025	2
14 de julho de 2025	3
25 de junho de 2025	3
29 de maio de 2025	3
12 de maio de 2025	4
16 de abril de 2025	4
14 de abril de 2025	4
3 de abril de 2025	4
28 de março de 2025	5
12 de março de 2025	5
10 de março de 2025	5
6 de março de 2025	5
03 de março de 2025	5
18 de fevereiro de 2025	6
10 de fevereiro de 2025	6
9 de dezembro de 2024	7
11 de novembro de 2024	7
25 de outubro de 2024	8
7 de outubro de 2024	9
9 de setembro de 2024	9
23 de agosto de 2024	9
22 de agosto de 2024	9
8 de agosto de 2024	10
10 de junho de 2024	10
17 de maio de 2024	10
23 de abril de 2024	10
8 de março de 2024	11
5 de março de 2024	11
2 de fevereiro de 2024	11
16 de janeiro de 2024	12
8 de janeiro de 2024	12
6 de dezembro de 2023	12
5 de dezembro de 2023	12
10 de novembro de 2023	13
8 de novembro de 2023	13
1 de novembro de 2023	13
23 de outubro de 2023	14
6 de outubro de 2023	14

10 de setembro de 2023	14
30 de julho de 2023	14
26 de julho de 2023	15
2 de julho de 2023	15
26 de junho de 2023	16
4 de junho de 2023	16
7 de maio de 2023	16
4 de abril de 2023	17
3 de abril de 2023	17
13 de março de 2023	19
5 de março de 2023	19
5 de fevereiro de 2023	20
1 de janeiro de 2023	21
15 de dezembro de 2022	21
8 de dezembro de 2022	21
4 de dezembro de 2022	21
15 de novembro de 2022	22
6 de novembro de 2022	22
18 de setembro de 2022	22
31 de julho de 2022	23
18 de julho de 2022	25
3 de julho de 2022	25
7 de junho de 2022	26
2 de maio de 2022	28
3 de abril de 2022	30
27 de fevereiro de 2022	30
9 de fevereiro de 2022	30
6 de fevereiro de 2022	31
30 de janeiro de 2022	31
2 de janeiro de 2022	31
28 de novembro de 2021	33
4 de outubro de 2021	34
2 de setembro de 2021	34
7 de julho de 2021	35
30 de maio de 2021	37
24 de maio de 2021	38
11 de abril de 2021	38
8 de março de 2021	39
4 de janeiro de 2021	40
3 de novembro de 2020	41
Limitações conhecidas	41
O console não oferece suporte à criação de volumes FlexGroup	41
O console não oferece suporte ao S3 com o Cloud Volumes ONTAP	41
O console não oferece suporte à recuperação de desastres para VMs de armazenamento	42
Notas de versão do Cloud Volumes ONTAP	42

Começar	43
Saiba mais sobre o Cloud Volumes ONTAP	43
Versões ONTAP suportadas para implantações do Cloud Volumes ONTAP	44
AWS	44
Azul	45
Google Cloud	46
Comece na Amazon Web Services	47
Início rápido para Cloud Volumes ONTAP na AWS	47
Planeje sua configuração do Cloud Volumes ONTAP na AWS	48
Configure sua rede	52
Configurar o Cloud Volumes ONTAP para usar uma chave gerenciada pelo cliente na AWS	77
Configurar funções do AWS IAM para nós do Cloud Volumes ONTAP	81
Configurar licenciamento para Cloud Volumes ONTAP na AWS	90
Implante o Cloud Volumes ONTAP na AWS usando implantação rápida	97
Inicie o Cloud Volumes ONTAP no AWS	101
Implantar o Cloud Volumes ONTAP no AWS Secret Cloud ou no AWS Top Secret Cloud	114
Comece no Microsoft Azure	130
Saiba mais sobre as opções de implantação do Cloud Volumes ONTAP no Azure	130
Introdução ao NetApp Console	131
Implantar o Cloud Volumes ONTAP no marketplace do Azure	184
Comece a usar o Google Cloud	188
Início rápido para o Cloud Volumes ONTAP no Google Cloud	188
Planeje sua configuração do Cloud Volumes ONTAP no Google Cloud	190
Configurar a rede do Google Cloud para o Cloud Volumes ONTAP	193
Configurar o VPC Service Controls para implantar o Cloud Volumes ONTAP no Google Cloud	205
Crie uma conta de serviço do Google Cloud para o Cloud Volumes ONTAP	207
Usando chaves de criptografia gerenciadas pelo cliente com o Cloud Volumes ONTAP	210
Configurar o licenciamento do Cloud Volumes ONTAP no Google Cloud	211
Inicie o Cloud Volumes ONTAP no Google Cloud	216
Verificação de imagem da plataforma Google Cloud	229
Use o Cloud Volumes ONTAP	241
Gerenciamento de licenças	241
Gerenciar licenciamento baseado em capacidade para Cloud Volumes ONTAP	241
Gerenciar assinaturas do Keystone para o Cloud Volumes ONTAP por meio do NetApp Console	246
Gerenciar licenciamento baseado em nó para Cloud Volumes ONTAP	250
Administração de volume e LUN	255
Crie um FlexVol volume em um sistema Cloud Volumes ONTAP	255
Gerenciar volumes em sistemas Cloud Volumes ONTAP	262
Dados Cloud Volumes ONTAP inativos em camadas para um armazenamento de objetos de baixo custo	271
Conecte-se a um LUN no Cloud Volumes ONTAP do seu sistema host	279
Acelere o acesso a dados com volumes FlexCache em um sistema Cloud Volumes ONTAP	280
Administração agregada	282
Crie um agregado para sistemas Cloud Volumes ONTAP	282
Gerenciar agregados para clusters do Cloud Volumes ONTAP	284

Gerenciar a capacidade agregada do Cloud Volumes ONTAP em um agente do Console	285
Administração de VM de armazenamento	287
Gerenciar VMs de armazenamento para Cloud Volumes ONTAP	287
Gerenciar VMs de armazenamento de serviço de dados para Cloud Volumes ONTAP na AWS	289
Gerenciar VMs de armazenamento de serviço de dados para Cloud Volumes ONTAP no Azure	296
Gerenciar VMs de armazenamento de dados para o Cloud Volumes ONTAP no Google Cloud	298
Configurar recuperação de desastres de VM de armazenamento para Cloud Volumes ONTAP	301
Segurança e criptografia de dados	302
Criptografe volumes no Cloud Volumes ONTAP com soluções de criptografia da NetApp	302
Gerencie chaves de criptografia Cloud Volumes ONTAP com o AWS Key Management Service	302
Gerencie chaves de criptografia Cloud Volumes ONTAP com o Azure Key Vault	303
Gerencie chaves de criptografia Cloud Volumes ONTAP com o Google Cloud KMS	311
Habilite soluções de proteção contra ransomware da NetApp para Cloud Volumes ONTAP	313
Crie cópias instantâneas invioláveis de arquivos WORM no Cloud Volumes ONTAP	316
Administração do sistema	317
Atualizar o software Cloud Volumes ONTAP	317
Registre os sistemas de pagamento conforme o uso do Cloud Volumes ONTAP	326
Converter uma licença baseada em nó do Cloud Volumes ONTAP em uma licença baseada em capacidade	327
Iniciar e parar um sistema Cloud Volumes ONTAP	330
Sincronizar a hora do sistema Cloud Volumes ONTAP usando o servidor NTP	333
Modificar a velocidade de gravação do sistema	333
Alterar a senha do administrador do cluster Cloud Volumes ONTAP	334
Adicionar, remover ou excluir sistemas	335
Administração AWS	337
Administração do Azure	340
Administração do Google Cloud	352
Administrar o Cloud Volumes ONTAP usando o System Manager	353
Administrar o Cloud Volumes ONTAP a partir da CLI	356
Saúde e eventos do sistema	357
Verifique a configuração do AutoSupport para o Cloud Volumes ONTAP	357
Configurar o EMS para sistemas Cloud Volumes ONTAP	361
Conceitos	362
Licenciamento	362
Licenciamento para Cloud Volumes ONTAP	362
Saiba mais sobre licenças baseadas em capacidade para o Cloud Volumes ONTAP	366
Armazenar	371
Protocolos de cliente suportados para Cloud Volumes ONTAP	371
Discos e agregados usados para clusters Cloud Volumes ONTAP	371
Saiba mais sobre o suporte para AWS Elastic Volumes com Cloud Volumes ONTAP	374
Saiba mais sobre camadas de dados com o Cloud Volumes ONTAP na AWS, Azure ou Google Cloud	380
Gerenciamento de armazenamento Cloud Volumes ONTAP	385
Velocidade de gravação	388
Cache Flash	391
Saiba mais sobre o armazenamento WORM no Cloud Volumes ONTAP	391

Pares de alta disponibilidade	393
Saiba mais sobre pares de alta disponibilidade do Cloud Volumes ONTAP na AWS	393
Saiba mais sobre pares de alta disponibilidade do Cloud Volumes ONTAP no Azure	400
Saiba mais sobre pares de alta disponibilidade do Cloud Volumes ONTAP no Google Cloud	406
Operações indisponíveis quando um nó no par Cloud Volumes ONTAP HA está offline	411
Saiba mais sobre a criptografia de dados Cloud Volumes ONTAP e a proteção contra ransomware	412
Criptografia de dados em repouso	412
Verificação de vírus ONTAP	414
Proteção contra ransomware	414
Saiba mais sobre o monitoramento de desempenho para cargas de trabalho do Cloud Volumes ONTAP	415
Relatórios técnicos de desempenho	415
Desempenho da CPU	415
Gerenciamento de licenças para BYOL baseado em nó	416
Licenças do sistema BYOL	416
Gerenciamento de licenças para um novo sistema	416
Expiração da licença	416
Renovação de licença	417
Transferência de licença para um novo sistema	417
Aprenda como o AutoSupport e o Digital Advisor são usados no Cloud Volumes ONTAP	417
Configurações padrão suportadas para Cloud Volumes ONTAP	418
Configuração padrão	418
Discos internos para dados do sistema	420
Conhecimento e suporte	424
Registre-se para obter suporte	424
Visão geral do registro de suporte	424
Registre o BlueXP para suporte da NetApp	424
Credenciais associadas do NSS para suporte do Cloud Volumes ONTAP	427
Obter ajuda	428
Obtenha suporte para um serviço de arquivo de provedor de nuvem	428
Use opções de autoapoio	429
Crie um caso com o suporte da NetApp	429
Gerencie seus casos de suporte (visualização)	431
Avisos legais	434
Direitos autorais	434
Marcas Registradas	434
Patentes	434
Política de Privacidade	434
Código aberto	434

Documentação do Cloud Volumes ONTAP

Notas de lançamento

Novidades no Cloud Volumes ONTAP

Saiba o que há de novo no gerenciamento do Cloud Volumes ONTAP no NetApp Console.

Os aprimoramentos descritos nesta página são específicos para gerenciar o Cloud Volumes ONTAP por meio do Console. Para saber o que há de novo no software Cloud Volumes ONTAP , ["acesse as Notas de versão do Cloud Volumes ONTAP"](#) .

6 de outubro de 2025

BlueXP agora é NetApp Console

O NetApp Console, criado com base na base aprimorada e reestruturada do BlueXP , fornece gerenciamento centralizado do armazenamento NetApp e do NetApp Data Services em ambientes locais e na nuvem em nível empresarial, fornecendo insights em tempo real, fluxos de trabalho mais rápidos e administração simplificada, de forma altamente segura e compatível.

Para obter detalhes sobre o que mudou, consulte o ["Notas de versão do NetApp Console"](#) .

Implantação simplificada do Cloud Volumes ONTAP na AWS

Agora você pode implantar o Cloud Volumes ONTAP na AWS usando um método de implantação rápida para configurações de nó único e de alta disponibilidade (HA). Esse processo simplificado reduz o número de etapas em comparação ao método avançado, define automaticamente os valores padrão em uma única página e minimiza a navegação, tornando a implantação mais rápida e fácil.

Para obter mais informações, consulte ["Implante o Cloud Volumes ONTAP na AWS usando implantação rápida"](#) .

4 de setembro de 2025

Cloud Volumes ONTAP 9.17.1 RC

Agora você pode usar o BlueXP para implantar e gerenciar o Release Candidate 1 do Cloud Volumes ONTAP 9.17.1 no Azure e no Google Cloud. No entanto, esta versão não está disponível para implantação e atualização na AWS.

["Saiba mais sobre esta versão do Cloud Volumes ONTAP"](#) .

11 de agosto de 2025

Fim da disponibilidade das licenças otimizadas

A partir de 11 de agosto de 2025, a licença Cloud Volumes ONTAP Optimized será descontinuada e não estará mais disponível para compra ou renovação nos marketplaces do Azure e do Google Cloud para assinaturas de pagamento conforme o uso (PAYGO). Se você tiver um contrato anual existente com uma licença otimizada, poderá continuar a usar a licença até o final do contrato. Quando sua licença Otimizada expirar, você poderá optar pelas licenças Cloud Volumes ONTAP Essentials ou Professional no BlueXP.

No entanto, a capacidade de adicionar ou renovar licenças otimizadas estará disponível por meio das APIs.

Para obter informações sobre pacotes de licenciamento, consulte ["Licenciamento para Cloud Volumes ONTAP"](#).

Para obter informações sobre como mudar para um método de carregamento diferente, consulte ["Gerenciar licenciamento baseado em capacidade"](#).

14 de julho de 2025

Suporte para proxy transparente

O BlueXP agora oferece suporte a servidores proxy transparentes, além das conexões proxy explícitas existentes. Ao criar ou modificar o BlueXP Connector, você pode configurar um servidor proxy transparente para gerenciar com segurança o tráfego de rede de e para o Cloud Volumes ONTAP.

Para obter mais informações sobre o uso de servidores proxy no Cloud Volumes ONTAP, consulte:

- ["Configurações de rede para oferecer suporte ao proxy do conector na AWS"](#)
- ["Configurações de rede para oferecer suporte ao proxy do conector no Azure"](#)
- ["Configurações de rede para oferecer suporte ao proxy do conector no Google Cloud"](#)

Novo tipo de VM com suporte para Cloud Volumes ONTAP no Azure

A partir do Cloud Volumes ONTAP 9.13.1, o L8s_v3 é suportado como um tipo de VM em zonas de disponibilidade únicas e múltiplas do Azure, para implantações de pares de alta disponibilidade (HA) novas e existentes.

Para mais informações, consulte ["Configurações com suporte no Azure"](#).

25 de junho de 2025

Disponibilidade restrita de licenciamento BYOL para Cloud Volumes ONTAP

A partir de 25 de junho de 2025, a NetApp restringiu o modelo de licenciamento "traga sua própria licença" (BYOL) para o Cloud Volumes ONTAP. A restrição se aplica a todos os clientes e implantações do Cloud Volumes ONTAP na AWS, Azure e Google Cloud. As únicas exceções são os clientes do setor público dos EUA e as implantações na região da China.

O suporte e os serviços da NetApp continuarão até o término do seu contrato BYOL, mas suas licenças expiradas não serão renovadas ou estendidas. Quando suas licenças BYOL expirarem, você deverá substituí-las por licenças baseadas em capacidade adquiridas por meio de suas assinaturas de marketplace em nuvem. Um modelo de licenciamento baseado em capacidade por meio de marketplaces de hiperescala otimiza a experiência de licenciamento e oferece maiores benefícios comerciais. Entre em contato com sua equipe de contas da NetApp ou com seus representantes de sucesso do cliente para discutir suas opções de conversão.

Para mais informações, consulte este comunicado ao cliente: ["CPC-00661: Alterações na política BYOL do Cloud Volumes ONTAP"](#).

29 de maio de 2025

Implantações em modo privado habilitadas para o Cloud Volumes ONTAP 9.15.1

Agora você pode implantar o Cloud Volumes ONTAP 9.15.1 no modo privado na AWS, Azure e Google Cloud. O modo privado está habilitado para implantações de nó único e de alta disponibilidade (HA) do Cloud Volumes ONTAP 9.15.1.

Para obter mais informações sobre implantações em modo privado, consulte <https://docs.netapp.com/us-en/bluexp-setup-admin/concept-modes.html#restricted-mode>["Saiba mais sobre os modos de implantação do BlueXP"] .

12 de maio de 2025

Descoberta de implantações feitas por meio do marketplace do Azure no BlueXP

O BlueXP agora tem a capacidade de descobrir os sistemas Cloud Volumes ONTAP implantados diretamente por meio do marketplace do Azure. Isso significa que agora você pode adicionar e gerenciar esses sistemas como ambientes de trabalho no BlueXP, assim como qualquer outro sistema Cloud Volumes ONTAP .

["Implantar o Cloud Volumes ONTAP no marketplace do Azure"](#)

16 de abril de 2025

Novas regiões com suporte no Azure

Agora você pode implantar o Cloud Volumes ONTAP 9.12.1 GA e posterior em zonas de disponibilidade únicas e múltiplas no Azure nas seguintes regiões. Isso inclui suporte para implantações de nó único e de alta disponibilidade (HA).

- Espanha Central
- México Central

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

14 de abril de 2025

Criação de VM de armazenamento automatizada por meio de APIs no Google Cloud

Agora você pode usar as APIs do BlueXP para automatizar a criação de VMs de armazenamento no Google Cloud. Você estava usando esse recurso em configurações de alta disponibilidade (HA) do Cloud Volumes ONTAP e agora também pode usá-lo em implantações de nó único. Ao usar as APIs do BlueXP , você pode facilmente criar, renomear e excluir VMs de armazenamento de serviço de dados adicionais no seu ambiente do Google Cloud, sem a necessidade de configurar manualmente as interfaces de rede, LIFs e LIFs de gerenciamento necessários. Essa automação simplifica o processo de gerenciamento de VMs de armazenamento.

["Gerenciar VMs de armazenamento de dados para o Cloud Volumes ONTAP no Google Cloud"](#)

3 de abril de 2025

Suporte para regiões da China para Cloud Volumes ONTAP 9.13.1 na AWS

Agora você pode implantar o Cloud Volumes ONTAP 9.13.1 na AWS nas regiões da China. Isso inclui suporte para implantações de nó único e de alta disponibilidade (HA). Somente licenças adquiridas diretamente da

NetApp são suportadas.

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

28 de março de 2025

Implantações em modo privado habilitadas para o Cloud Volumes ONTAP 9.14.1

Agora você pode implantar o Cloud Volumes ONTAP 9.14.1 no modo privado na AWS, Azure e Google Cloud. O modo privado é habilitado para implantações de nó único e de alta disponibilidade (HA) do Cloud Volumes ONTAP 9.14.1.

Para obter mais informações sobre implantações em modo privado, consulte <https://docs.netapp.com/us-en/bluexp-setup-admin/concept-modes.html#restricted-mode>["Saiba mais sobre os modos de implantação do BlueXP"^] .

12 de março de 2025

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 de HA no Azure para o Cloud Volumes ONTAP 9.12.1 GA e posteriores:

- EUA Central
- Governo dos EUA - Virgínia (Região do Governo dos EUA - Virgínia)

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

10 de março de 2025

Criação de VM de armazenamento automatizada por meio de APIs no Azure

Agora você pode usar as APIs do BlueXP para criar, renomear e excluir VMs de armazenamento de serviço de dados adicionais para o Cloud Volumes ONTAP no Azure. O uso das APIs automatiza o processo de criação de VM de armazenamento, incluindo a configuração das interfaces de rede necessárias, LIFs e um LIF de gerenciamento, caso você precise usar uma VM de armazenamento para fins de gerenciamento.

["Gerenciar VMs de armazenamento de serviço de dados para Cloud Volumes ONTAP no Azure"](#)

6 de março de 2025

Cloud Volumes ONTAP 9.16.1 GA

Agora você pode usar o BlueXP para implantar e gerenciar a versão de Disponibilidade Geral do Cloud Volumes ONTAP 9.16.1 no Azure e no Google Cloud. No entanto, esta versão não está disponível para implantação e atualização na AWS.

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

03 de março de 2025

Suporte para a região Norte da Nova Zelândia no Azure

A região Norte da Nova Zelândia agora tem suporte no Azure para configurações de nó único e alta disponibilidade (HA) do Cloud Volumes ONTAP 9.12.1 GA e posteriores. Observe que o tipo de instância Lsv3 não é suportado nesta região.

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

18 de fevereiro de 2025

Apresentando a implantação direta do Azure Marketplace

Agora você pode aproveitar a implantação direta do Azure Marketplace para implantar o Cloud Volumes ONTAP de forma fácil e rápida diretamente do Azure Marketplace. Usando esse método simplificado, você pode explorar os principais recursos e funcionalidades do Cloud Volumes ONTAP em seu ambiente sem precisar configurar o BlueXP Connector ou atender a outros critérios de integração necessários para implantar o Cloud Volumes ONTAP por meio do BlueXP.

- ["Saiba mais sobre as opções de implantação do Cloud Volumes ONTAP no Azure"](#)
- ["Implantar o Cloud Volumes ONTAP no marketplace do Azure"](#)

10 de fevereiro de 2025

Autenticação de usuário habilitada para acessar o System Manager a partir do BlueXP

Como administrador do BlueXP , agora você pode ativar a autenticação para usuários do ONTAP que acessam o ONTAP System Manager pelo BlueXP. Você pode habilitar esta opção editando as configurações do BlueXP Connector. Esta opção está disponível para os modos padrão e privado.

["Administrar o Cloud Volumes ONTAP usando o System Manager"](#) .

BlueXP Advanced View renomeado para System Manager

A opção para gerenciamento avançado do Cloud Volumes ONTAP do BlueXP por meio do ONTAP System Manager foi renomeada de **Advanced View** para **System Manager**.

["Administrar o Cloud Volumes ONTAP usando o System Manager"](#) .

Apresentando uma maneira mais simples de gerenciar licenças com a BlueXP digital wallet

Agora, você pode experimentar o gerenciamento simplificado de licenças do Cloud Volumes ONTAP usando pontos de navegação aprimorados na BlueXP digital wallet:

- Acesse facilmente as informações da sua licença do Cloud Volumes ONTAP nas guias **Administração > Licenças e assinaturas > Visão geral/Licenças diretas**.
- Clique em **Exibir** no painel Cloud Volume ONTAP na guia **Visão geral** para obter uma compreensão abrangente de suas licenças baseadas em capacidade. Esta visualização avançada oferece informações detalhadas sobre suas licenças e assinaturas.
- Se preferir a interface anterior, você pode clicar no botão **Alternar para a visualização legada** para visualizar os detalhes da licença por tipo e modificar os métodos de cobrança para suas licenças.

["Gerenciar licenças baseadas em capacidade"](#) .

9 de dezembro de 2024

Lista de VMs com suporte atualizada para o Azure para alinhamento com as 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 mais antigos e existentes. Novas implantações do Cloud Volumes ONTAP têm suporte no Azure somente a partir da versão 9.12.1. Recomendamos que você mude para o Es_v4 ou qualquer outra série compatível com o Cloud Volumes ONTAP 9.12.1 e posteriores. As máquinas das séries DS_v2 e Es_v3, no entanto, estarão disponíveis para novas implantações feitas por meio da API.

["Configurações com suporte no Azure"](#)

11 de novembro de 2024

Fim da disponibilidade de licenças baseadas em nós

A NetApp planejou o fim da disponibilidade (EOA) e o fim do suporte (EOS) do licenciamento baseado em nó do 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 o EOA das suas licenças baseadas em nós, você deve fazer a transição para o licenciamento baseado em capacidade usando a ferramenta de conversão de licenças BlueXP .

Para compromissos anuais ou de longo prazo, a NetApp recomenda que você entre em contato com seu representante da NetApp antes da data de 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 em uma assinatura sob demanda de pagamento conforme o uso (PAYGO), é importante planejar sua conversão antes da data de EOS. Para contratos de longo prazo e assinaturas PAYGO, você pode usar a ferramenta de conversão de licença BlueXP para uma conversão perfeita.

["Fim da disponibilidade de licenças baseadas em nós"](#) ["Converter uma licença baseada em nó do Cloud Volumes ONTAP em uma licença baseada em capacidade"](#)

Remoção de implantações baseadas em nós do BlueXP

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

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

- Clientes do setor público dos EUA
- Implantações em modo privado
- Implantações da região da China do Cloud Volumes ONTAP na AWS
- Se você tiver uma licença válida e não expirada por nó, traga sua própria licença (licença BYOL)

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

Adição de uma camada fria para dados do Cloud Volumes ONTAP no armazenamento de Blobs do Azure

O BlueXP agora permite que você selecione uma camada fria para armazenar os dados da camada de capacidade inativa no armazenamento de Blobs do Azure. Adicionar a camada fria às camadas quente e fria existentes oferece uma opção de armazenamento mais acessível e melhor eficiência de custos.

["Camadas 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 armazenamento para sistemas Cloud Volumes ONTAP no Azure. Ao desabilitar o acesso, você pode proteger seu endereço IP privado contra exposição, mesmo dentro da mesma VNet, caso seja necessário cumprir as políticas de segurança da sua organização. Esta opção também desabilita a hierarquização de dados para seus sistemas Cloud Volumes ONTAP e é aplicável tanto a pares de nós únicos quanto a pares de alta disponibilidade.

["Regras do grupo de segurança"](#) .

Habilitação do WORM após implantação do Cloud Volumes ONTAP

Agora você tem a capacidade de ativar o armazenamento WORM (gravação única e leitura múltipla) em um sistema Cloud Volumes ONTAP existente usando o BlueXP. Essa funcionalidade oferece a flexibilidade de habilitar o WORM em um ambiente de trabalho, mesmo que o WORM não tenha sido habilitado durante sua criação. Uma vez ativado, você não poderá desativar o WORM.

["Habilitando o 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 alinhamento com as 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 mais antigos e existentes. Novas implantações do Cloud Volumes ONTAP são suportadas no Google Cloud somente a partir da versão 9.8. Recomendamos que você mude para os tipos de máquinas da série n2 que são compatíveis com o Cloud Volumes ONTAP 9.8 e posteriores. As máquinas da série n1, no entanto, estarão disponíveis para novas implantações realizadas por meio da API.

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

Suporte de Zonas Locais para Amazon Web Services no modo privado

O BlueXP agora oferece suporte a AWS Local Zones para implantações de alta disponibilidade (HA) do Cloud Volumes ONTAP no modo privado. O suporte que antes era limitado apenas ao modo padrão agora foi 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, consulte ["Zonas locais da AWS"](#) .

7 de outubro de 2024

Experiência de usuário aprimorada na seleção de versão para atualização

A partir desta versão, ao tentar atualizar o Cloud Volumes ONTAP usando a notificação do 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.

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

9 de setembro de 2024

As funcionalidades WORM e ARP não são mais cobradas

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

O preço simplificado traz os seguintes benefícios:

- Contas que atualmente incluem WORM e ARP não incorrerão mais em cobranças por esses recursos. A partir de agora, sua fatura só terá cobranças pelo uso da capacidade, como era antes dessa alteração. WORM e ARP não serão mais incluídos em suas faturas futuras.
- Se suas contas atuais não incluem esses recursos, agora você pode optar por WORM e ARP sem custo adicional.
- Todas as ofertas do Cloud Volumes ONTAP para novas contas excluirão cobranças de WORM e ARP.

Saiba mais sobre esses recursos:

- ["Habilite soluções de proteção contra ransomware da NetApp para Cloud Volumes ONTAP"](#)
- ["Armazenamento WORM"](#)

23 de agosto de 2024

Região Canadá Oeste agora com suporte na AWS

A região Canadá Oeste agora tem suporte no AWS para Cloud Volumes ONTAP 9.12.1 GA e posteriores.

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

22 de agosto de 2024

Cloud Volumes ONTAP 9.15.1 GA

O BlueXP agora pode implantar e gerenciar a versão 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 obsoletos

Os pacotes de licenciamento baseados na capacidade do Edge Cache não estarão mais disponíveis para futuras implantações 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 no Azure.

Para configurações suportadas, consulte ["Configurações com suporte no Azure"](#).

Testes gratuitos para assinaturas do marketplace foram descontinuados

A licença de avaliação ou teste gratuito automático de 30 dias para assinaturas pagas conforme o uso no mercado do provedor de nuvem não estará mais disponível no Cloud Volumes ONTAP. A cobrança por qualquer tipo de assinatura do marketplace (PAYGO ou contrato anual) será ativada a partir do primeiro uso, sem período de teste gratuito.

10 de junho de 2024

Cloud Volumes ONTAP 9.15.0

O BlueXP agora 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 para zonas locais da Amazon Web Services

O suporte para AWS Local Zones agora está disponível para implantações do Cloud Volumes ONTAP HA. As Zonas Locais da AWS são uma implantação de infraestrutura onde armazenamento, computação, banco de dados e outros serviços selecionados da AWS estão localizados perto de grandes cidades e áreas industriais.



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

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

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 de HA no Azure para o Cloud Volumes ONTAP 9.12.1 GA e posteriores:

- Alemanha Centro-Oeste

- Polônia Central
- Oeste dos EUA 3
- Israel Central
- Itália Norte
- Canadá Central

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

Região de Joanesburgo agora com suporte no Google Cloud

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

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

Modelos de volume e tags não são mais suportados

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 correção 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 Mediator e o Connector agora oferecem suporte ao Amazon Instant Metadata Service v2 (IMDSv2) para todas as funções. O IMDSv2 oferece proteção aprimorada contra vulnerabilidades. Anteriormente, apenas o IMDSv1 era suportado.

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

5 de março de 2024

Cloud Volumes ONTAP 9.14.1 GA

O BlueXP agora pode implantar e gerenciar a versão 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 oferece suporte às seguintes VMs da série Edv5 a partir da versão 9.14.1.

- E4ds_v5
- E8ds_v5
- E20s_v5

- [E32ds_v5](#)
- [E48ds_v5](#)
- [E64ds_v5](#)

["Configurações com suporte no Azure"](#)

16 de janeiro de 2024

Lançamentos de patches no BlueXP

Os lançamentos de patches estão disponíveis no BlueXP apenas para as três versões mais recentes do Cloud Volumes ONTAP.

["Atualizar 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 com suporte no Azure"](#)

6 de dezembro de 2023

Cloud Volumes ONTAP 9.14.1 RC1

O BlueXP agora 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 FlexVol volume de 300 TiB

Agora você pode criar um FlexVol volume de até 300 TiB com o System Manager e o ONTAP CLI 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 novas regiões no Azure

Suporte de região de zona de disponibilidade única

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

- Tel Aviv
- Milão

Suporte a várias regiões de zona de disponibilidade

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

- Índia Central
- Noruega Oriental
- Suíça Norte
- África do Sul Norte
- Emirados Árabes Unidos Norte

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

10 de novembro de 2023

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

Região de Berlim agora com suporte no Google Cloud

A região de Berlim agora tem suporte no Google Cloud para Cloud Volumes ONTAP 9.12.1 GA e posteriores.

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

8 de novembro de 2023

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

Região de Tel Aviv agora com suporte na AWS

A região de Tel Aviv agora tem suporte no AWS para Cloud Volumes ONTAP 9.12.1 GA e posteriores.

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

1 de novembro de 2023

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

Região da Arábia Saudita agora com suporte no Google Cloud

A região da Arábia Saudita agora tem suporte no Google Cloud para Cloud Volumes ONTAP e no Connector for Cloud Volumes ONTAP 9.12.1 GA e posteriores.

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

23 de outubro de 2023

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

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 múltiplas zonas de disponibilidade de alta disponibilidade para o Cloud Volumes ONTAP 9.12.1 GA e posteriores:

- Austrália Oriental
- Leste Asiático
- França Central
- Norte da Europa
- Catar Central
- Suécia Central
- Europa Ocidental
- Oeste dos EUA 2

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

6 de outubro de 2023

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

Cloud Volumes ONTAP 9.14.0

O BlueXP agora pode implantar e gerenciar a versão 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 Connector.

Suporte para VMs da série Lsv3 no Azure

Os tipos de instância L48s_v3 e L64s_v3 agora são suportados 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 únicas e múltiplas, a partir da versão 9.13.1. Esses tipos de instância oferecem suporte ao Flash Cache.

["Exibir configurações compatíveis com o Cloud Volumes ONTAP no Azure"](#) ["Exibir limites de armazenamento para Cloud Volumes ONTAP no Azure"](#)

30 de julho de 2023

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

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 o Cloud Volumes ONTAP 9.13.1 e posteriores. Alta velocidade de gravação está disponível em todos os tipos de instância suportados. 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 juntos em implantações de nó único e de 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 agora estão disponíveis. A seguir estão as melhorias nos relatórios de uso:

- A unidade TiB agora está incluída no nome das colunas.
- Um novo campo "nó(s)" para números de série agora está incluído.
- Uma nova coluna "Tipo de carga de trabalho" agora está incluída no relatório de uso de VMs de armazenamento.
- Nomes de ambientes de trabalho agora incluídos em VMs de armazenamento e relatórios de uso de volume.
- 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, consulte ["Baixar relatórios de uso"](#).

26 de julho de 2023

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

Cloud Volumes ONTAP 9.13.1 GA

O BlueXP agora pode implantar e gerenciar a versão 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 Connector.

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

O Japan East e o Korea Central no Azure agora oferecem suporte a implantações de HA em várias zonas de disponibilidade para o Cloud Volumes ONTAP 9.12.1 GA e posteriores.

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

Suporte de proteção autônoma contra ransomware

A Proteção Autônoma contra Ransomware (ARP) agora é compatível com o Cloud Volumes ONTAP. O suporte a ARP está disponível no Cloud Volumes ONTAP versão 9.12.1 e superiores.

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

26 de junho de 2023

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

Cloud Volumes ONTAP 9.13.1 RC1

O BlueXP agora 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 Connector.

Atualização do seletor de versão de atualização do Cloud Volumes ONTAP

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

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

7 de maio de 2023

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

Região do Catar agora com suporte no Google Cloud

A região do Catar agora tem suporte no Google Cloud para Cloud Volumes ONTAP e no Connector for Cloud Volumes ONTAP 9.12.1 GA e posteriores.

Região Central da Suécia agora com suporte no Azure

A região Central da Suécia agora tem suporte no Azure para Cloud Volumes ONTAP e no Connector for Cloud Volumes ONTAP 9.12.1 GA e posteriores.

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

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

Detalhamento do uso de carregamento

Agora você pode descobrir o que está sendo cobrado quando assina licenças baseadas em capacidade. Os seguintes tipos de relatórios de uso estão disponíveis para download na 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 para download podem ser facilmente compartilhados com outras pessoas.

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

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

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

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

4 de abril de 2023

Suporte para regiões da China para AWS

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 suportados.
- Licenças adquiridas diretamente da NetApp são suportadas.

Para 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 Connector.

Região de Turim agora com suporte no Google Cloud

A região de Turim agora é compatível com o Google Cloud para Cloud Volumes ONTAP e o Connector for Cloud Volumes ONTAP 9.12.1 GA e posteriores.

Aprimoramento da BlueXP digital wallet

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

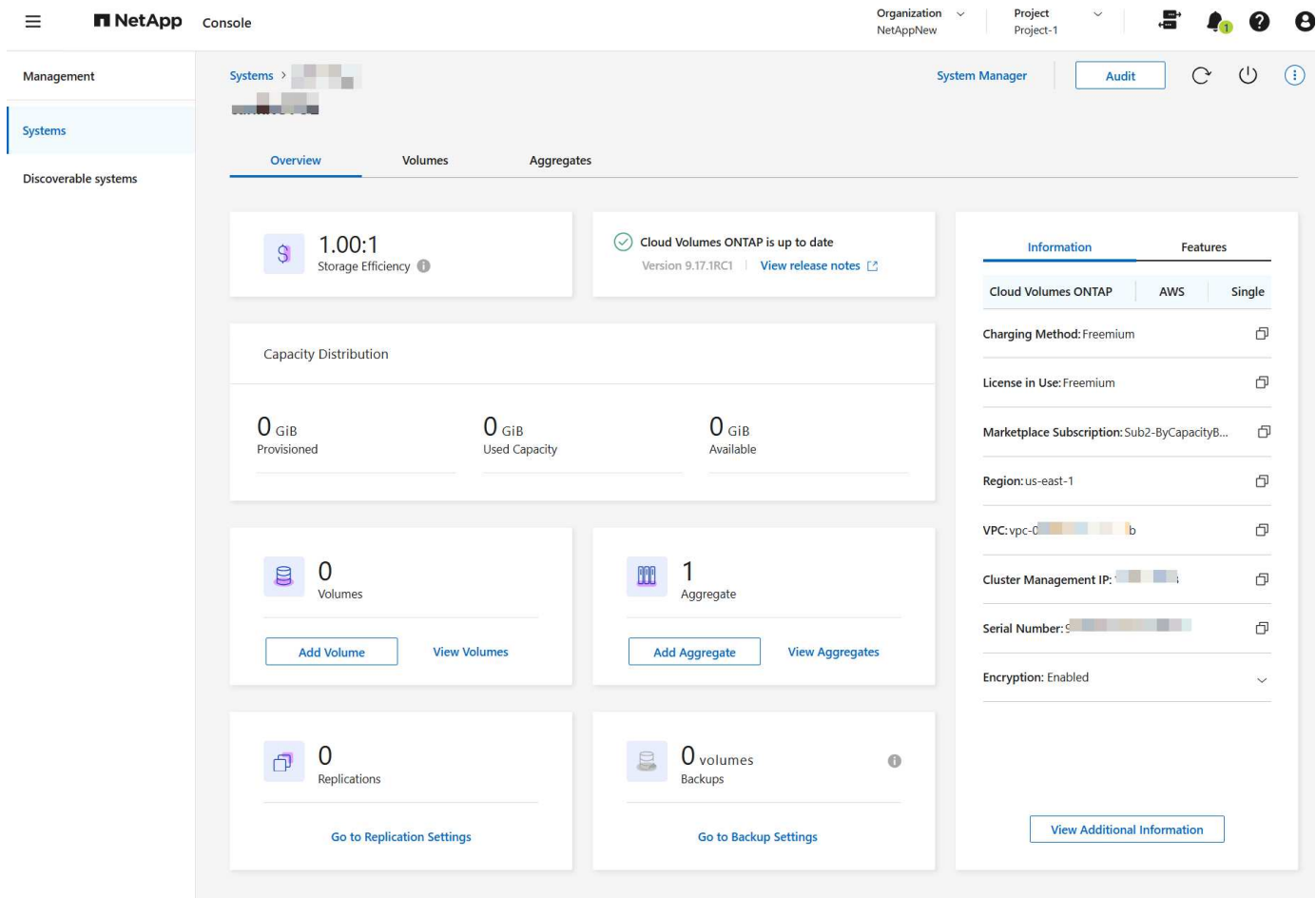
["Aprenda a visualizar a capacidade consumida na sua conta"](#).

Suporte para comentários durante a criação do volume

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

Redesenho da interface do usuário do BlueXP para as páginas Visão geral, Volumes e Agregados do Cloud Volumes ONTAP

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



Volumes FlexGroup visíveis através do Cloud Volumes ONTAP

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



Atualmente, você só pode visualizar volumes FlexGroup existentes no BlueXP. A capacidade de criar volumes FlexGroup no BlueXP não está disponível, mas está planejada para uma versão futura.

FlexGroup Volume



Volume

ONLINE

Manage 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	  		

["Saiba mais sobre como visualizar volumes FlexGroup criados."](#)

13 de março de 2023

Suporte para regiões da China no Azure

A região China Norte 3 agora tem suporte para implantações de nó único do Cloud Volumes ONTAP 9.12.1 GA e 9.13.0 GA no Azure. Somente licenças adquiridas diretamente da NetApp (licenças BYOL) são suportadas nessas regiões.



Novas implantações do Cloud Volumes ONTAP nas regiões da China são suportadas apenas no 9.12.1 GA e 9.13.0 GA. Você pode atualizar essas versões para patches e lançamentos posteriores do Cloud Volumes ONTAP. Se você quiser implantar versões posteriores do Cloud Volumes ONTAP em regiões da China, entre em contato com o Suporte da NetApp .

Para 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 Connector.

Cloud Volumes ONTAP 9.13.0

O BlueXP agora 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"](#) .

Suporte a 16 TiB e 32 TiB no Azure

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

Saiba mais sobre ["tamanhos de disco suportados no Azure"](#) .

Licença MTEKM

A licença Multi-tenant Encryption Key Management (MTEKM) agora está incluída nos sistemas Cloud Volumes ONTAP novos e existentes que executam a versão 9.12.1 GA ou posterior.

O gerenciamento de chaves externas multilocatário permite que VMs de armazenamento individuais (SVMs) mantenham suas próprias chaves por meio de um servidor KMIP ao usar o NetApp Volume Encryption.

["Aprenda a criptografar volumes com soluções de criptografia da 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 suportado nesses ambientes. O licenciamento baseado em capacidade não é suportado. Para começar, instale manualmente o software Connector, faça login no console BlueXP que está em execução no Connector, adicione sua licença BYOL à BlueXP digital wallet e implante o Cloud Volumes ONTAP.

- ["Instale o conector em um local sem acesso à Internet"](#)
- ["Acesse o console BlueXP no Conector"](#)
- ["Adicionar uma licença não atribuída"](#)

Flash Cache e alta velocidade de gravação no Google Cloud

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

Saiba mais sobre ["configurações suportadas pela licença para o Google Cloud"](#) .

5 de fevereiro de 2023

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

Criação de grupo de posicionamento na AWS

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

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

Atualização da configuração da zona DNS privada

Uma nova configuração agora está disponível para que você possa evitar a criação de um link entre uma zona DNS privada e uma rede virtual ao usar os Links Privados do Azure. A criação é ativada por padrão.

["Forneça ao BlueXP detalhes sobre seu DNS privado do Azure"](#)

Armazenamento WORM e hierarquização de dados

Agora você pode habilitar a hierarquização de dados e o armazenamento WORM juntos ao criar um sistema Cloud Volumes ONTAP 9.8 ou posterior. Habilitar o armazenamento em camadas de dados com WORM permite que você organize os dados em camadas em um armazenamento de objetos na nuvem.

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

1 de janeiro de 2023

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

Pacotes de licenciamento disponíveis no Google Cloud

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

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

Configuração padrão para Cloud Volumes ONTAP

A licença do Multi-tenant Encryption Key Management (MTEKM) não está mais incluída nas novas implantações do Cloud Volumes ONTAP .

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

15 de dezembro de 2022

Cloud Volumes ONTAP 9.12.0

O BlueXP agora 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

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

["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 Connector.

WORM + Cloud Backup agora disponível durante a criação do Cloud Volumes ONTAP

A capacidade de ativar os recursos WORM (gravar uma vez, ler várias vezes) e Cloud Backup agora está disponível durante o processo de criação do Cloud Volumes ONTAP .

Região de Israel agora com suporte no Google Cloud

A região de Israel agora tem suporte no Google Cloud para Cloud Volumes ONTAP e no Connector for Cloud Volumes ONTAP 9.11.1 P3 e posteriores.

15 de novembro de 2022

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

Licença ONTAP S3 no Google Cloud

Uma licença 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.

["Documentação do ONTAP : Aprenda a configurar e gerenciar serviços de armazenamento de objetos do S3"](#)

6 de novembro de 2022

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

Movendo 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 dentro da mesma assinatura do Azure.

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

Certificação de cópia NDMP

O NDMP-copy agora é certificado para uso com o Cloud Volume ONTAP.

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

Suporte de criptografia de disco gerenciado para Azure

Uma nova permissão do Azure foi adicionada e agora permite criptografar todos os discos gerenciados na criação.

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

18 de setembro de 2022

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

Melhorias na Carteira Digital

- A Carteira Digital agora mostra um resumo do pacote de licenciamento de E/S otimizado e a capacidade WORM provisionada para sistemas Cloud Volumes ONTAP em sua conta.

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

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

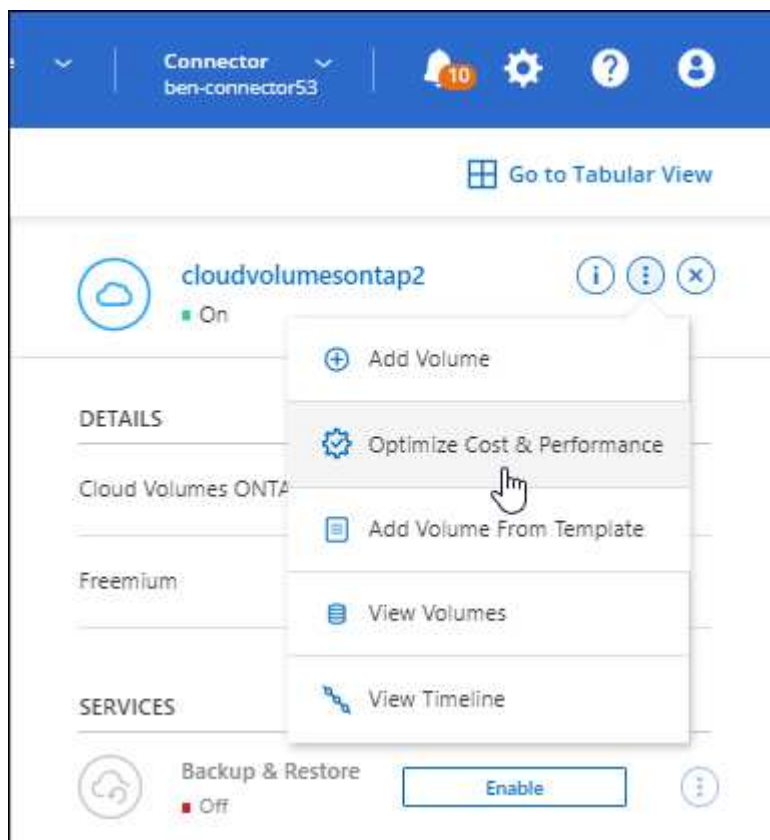
- Agora você pode mudar de um método de carregamento para o método de carregamento otimizado.

["Aprenda como alterar os métodos de cobrança"](#) .

Otimizar custos e desempenho

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

Depois de selecionar um ambiente de trabalho, você pode escolher a opção **Otimizar Custo e Desempenho** para alterar o tipo de instância do Cloud Volumes ONTAP. Escolher uma instância de tamanho menor pode ajudar a reduzir custos, enquanto mudar para uma instância de tamanho maior pode ajudar a otimizar o desempenho.



Notificações do AutoSupport

O BlueXP agora gerará uma notificação se um sistema Cloud Volumes ONTAP não conseguir enviar mensagens de 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 Connector.

Licença MTEKM

A licença Multi-tenant Encryption Key Management (MTEKM) agora está incluída nos sistemas Cloud Volumes ONTAP novos e existentes que executam a versão 9.11.1 ou posterior.

O gerenciamento de chaves externas multilocatário permite que VMs de armazenamento individuais (SVMs) mantenham suas próprias chaves por meio de um servidor KMIP ao usar o NetApp Volume Encryption.

["Aprenda a criptografar volumes com soluções de criptografia da NetApp"](#) .

Servidor proxy

O BlueXP agora configura automaticamente seus sistemas Cloud Volumes ONTAP para usar o Connector como um servidor proxy, caso uma conexão de saída com a Internet não esteja disponível para enviar mensagens do AutoSupport .

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

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

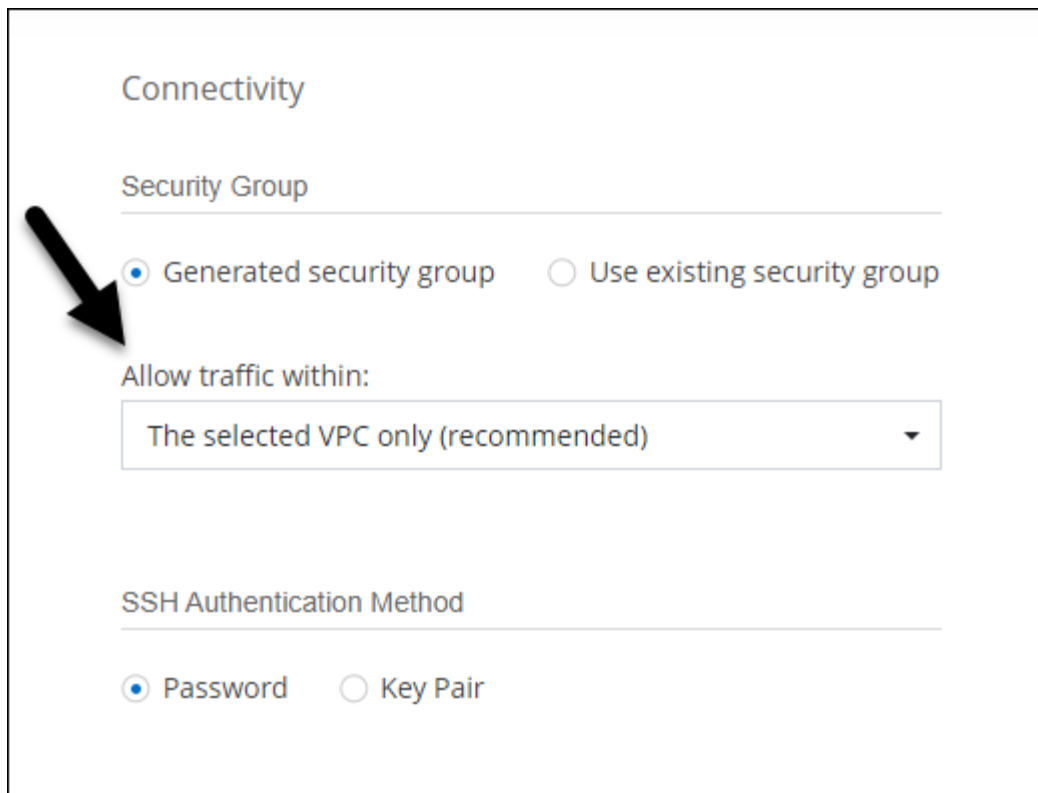
Alterar método de cobrança

Agora você pode alterar o método de cobrança para 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 caso suas necessidades comerciais mudem. Este recurso está disponível na Carteira Digital.

["Aprenda como alterar os métodos de cobrança"](#) .

Aprimoramento do grupo de segurança

Ao criar um ambiente de trabalho do Cloud Volumes ONTAP , a interface do 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 pela capacidade provisionada e pelas operações de E/S separadamente
- **Edge Cache:** Licenciamento para ["Cache de Borda de Volumes em Nuvem"](#)

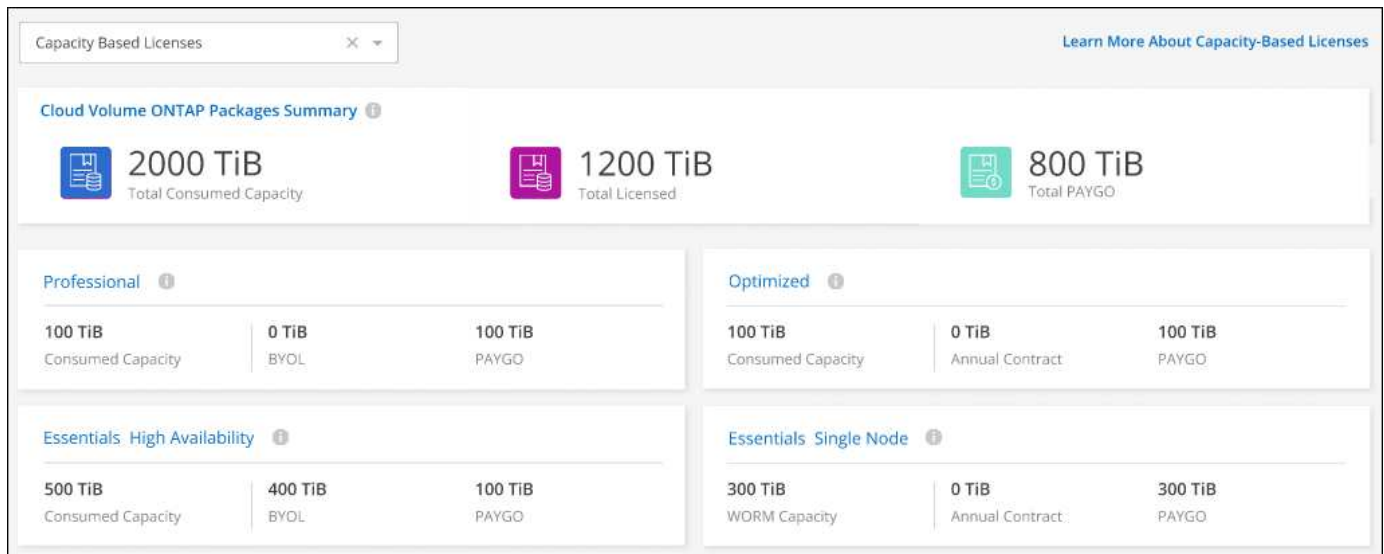
["Saiba mais sobre esses pacotes de licenciamento"](#) .

3 de julho de 2022

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

Carteira Digital

A Carteira Digital agora mostra a capacidade total consumida na sua conta e a capacidade consumida por pacote de licenciamento. Isso pode ajudar você a entender como está sendo cobrado e se precisa comprar capacidade adicional.



Aprimoramento de Volumes Elásticos

O BlueXP agora oferece suporte ao recurso Amazon EBS Elastic Volumes ao criar um ambiente de trabalho do Cloud Volumes ONTAP a partir da interface do usuário. O recurso Elastic Volumes é habilitado por padrão ao usar discos gp3 ou io1. Você pode escolher a capacidade inicial com base em suas necessidades de armazenamento e revisá-la após a implantação do Cloud Volumes ONTAP .

["Saiba mais sobre o suporte para Elastic Volumes na AWS"](#) .

Licença ONTAP S3 na AWS

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

["Documentação do ONTAP : Aprenda a configurar e gerenciar serviços de armazenamento de objetos do S3"](#)

Novo suporte à região do Azure Cloud

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

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

Licença ONTAP S3 no Azure

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

["Documentação do ONTAP : Aprenda a configurar e gerenciar serviços de armazenamento de objetos do S3"](#)

7 de junho de 2022

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

Cloud Volumes ONTAP 9.11.1

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

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

Nova Visualização Avançada

Se precisar executar o gerenciamento avançado do Cloud Volumes ONTAP, você pode fazer isso usando o ONTAP System Manager, que é uma interface de gerenciamento fornecida com um sistema ONTAP . Incluímos a interface do Gerenciador de Sistema diretamente dentro do BlueXP para que você não precise sair do BlueXP para gerenciamento avançado.

Esta Visualização Avançada está disponível como uma prévia com o Cloud Volumes ONTAP 9.10.0 e posteriores. Planejamos refinar essa experiência e adicionar melhorias em versões futuras. Envie-nos seu feedback usando o chat do produto.

["Saiba mais sobre a Visualização Avançada"](#) .

Suporte para Amazon EBS Elastic Volumes

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

O suporte para Elastic Volumes está disponível a partir dos *novos* sistemas Cloud Volumes ONTAP 9.11.0 e com os tipos de disco EBS gp3 e io1.

["Saiba mais sobre o suporte para Elastic Volumes"](#) .

Observe que o suporte para Elastic Volumes requer novas permissões da AWS para o Conector:

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

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

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

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

["Aprenda a implantar um par HA em uma sub-rede compartilhada"](#) .

Acesso limitado à rede ao usar pontos de extremidade de serviço

O BlueXP agora limita o acesso à rede ao usar um ponto de extremidade de serviço VNet para conexões entre o Cloud Volumes ONTAP e contas de armazenamento. O BlueXP usa um ponto de extremidade de serviço se você desabilitar as conexões do Azure Private Link.

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

Suporte para criação de VMs de armazenamento no Google Cloud

Várias VMs de armazenamento agora são compatíveis com o Cloud Volumes ONTAP no Google Cloud, a partir da versão 9.11.1. A partir desta versão do Connector, o BlueXP permite que você crie VMs de

armazenamento em pares de alta disponibilidade do Cloud Volumes ONTAP no Google Cloud usando a API.

O suporte para 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 o ONTAP CLI ou o System Manager para criar uma VM de armazenamento em um sistema de nó único.

- ["Saiba mais sobre os limites de VM de armazenamento no Google Cloud"](#)
- ["Aprenda a criar VMs de armazenamento 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 Connector.

Cloud Volumes ONTAP 9.11.0

O BlueXP agora pode implantar e gerenciar o Cloud Volumes ONTAP 9.11.0.

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

Melhoria nas atualizações do mediador

Quando o BlueXP atualiza o mediador para um par HA, ele agora valida se uma nova imagem do mediador está disponível antes de excluir o disco de inicialização. Essa alteração garante que o mediador possa continuar operando com sucesso caso o processo de atualização não seja bem-sucedido.

A aba K8s foi removida

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

Contrato anual no Azure

Os pacotes Essentials e Professional agora estão disponíveis no Azure por meio 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 a NetApp compartilhar a oferta privada com você, você poderá selecionar o plano anual ao assinar o Azure Marketplace durante a criação do ambiente de trabalho.

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

Recuperação instantânea do S3 Glacier

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

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

Novas permissões da AWS necessárias para o Conector

As seguintes permissões agora são necessárias para criar um grupo de posicionamento de distribuição 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 como o BlueXP cria o grupo de posicionamento.

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

Novo suporte regional do Google Cloud

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

- Delhi (asia-sul2)
- Melbourne (austrália-sudeste2)
- Milão (europe-west8) - apenas um nó
- Santiago (southamerica-west1) - apenas um nó

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

Suporte para n2-standard-16 no Google Cloud

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

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

Melhorias nas políticas de firewall do Google Cloud

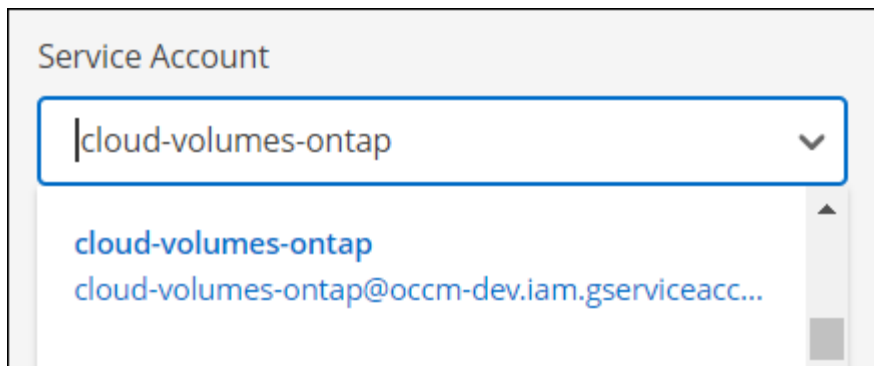
- Ao criar um par de Cloud Volumes ONTAP HA no Google Cloud, o BlueXP agora exibirá todas as políticas de firewall existentes em uma VPC.

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

- Ao criar 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 o tráfego somente na VPC selecionada (recomendado) ou em todas as 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. Visualizar o endereço de e-mail pode facilitar a distinção entre contas de serviço que compartilham o mesmo nome.



3 de abril de 2022

O link do Gerenciador de Sistema foi removido

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

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

Cobrança pelo armazenamento WORM

Agora que a tarifa especial introdutória expirou, você será cobrado pelo uso do 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 preços para armazenamento WORM"](#) .

27 de fevereiro de 2022

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

Assistente de volume redesenhado

O assistente de criação de novo volume que introduzimos recentemente agora está disponível ao criar um volume em um agregado específico na opção **Alocação avançada**.

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

9 de fevereiro de 2022

Atualizações do Marketplace

- Os pacotes Essenciais e Profissional agora 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 marketplace de nuvem, você também será automaticamente

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

Se você for um novo cliente, o BlueXP solicitará que você assine quando 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 cobrança ainda está disponível para clientes existentes que tenham uma assinatura ativa.

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

6 de fevereiro de 2022

Trocar licenças não atribuídas

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

Esta ação revoga a licença do Cloud Volumes ONTAP e cria uma licença equivalente em dólares para o serviço com a mesma data de expiração.

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

30 de janeiro de 2022

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

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 que foram introduzidos em julho de 2021 e dão suporte às próximas ofertas por meio dos mercados de provedores de nuvem.

Atualização da Carteira Digital

Atualizamos a **Carteira Digital** consolidando as licenças do Cloud Volumes ONTAP em uma única aba.

2 de janeiro de 2022

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

Suporte para tipos adicionais de VM do Azure

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

- E4ds_v4
- E8ds_v4
- E32ds_v4

- E48ds_v4

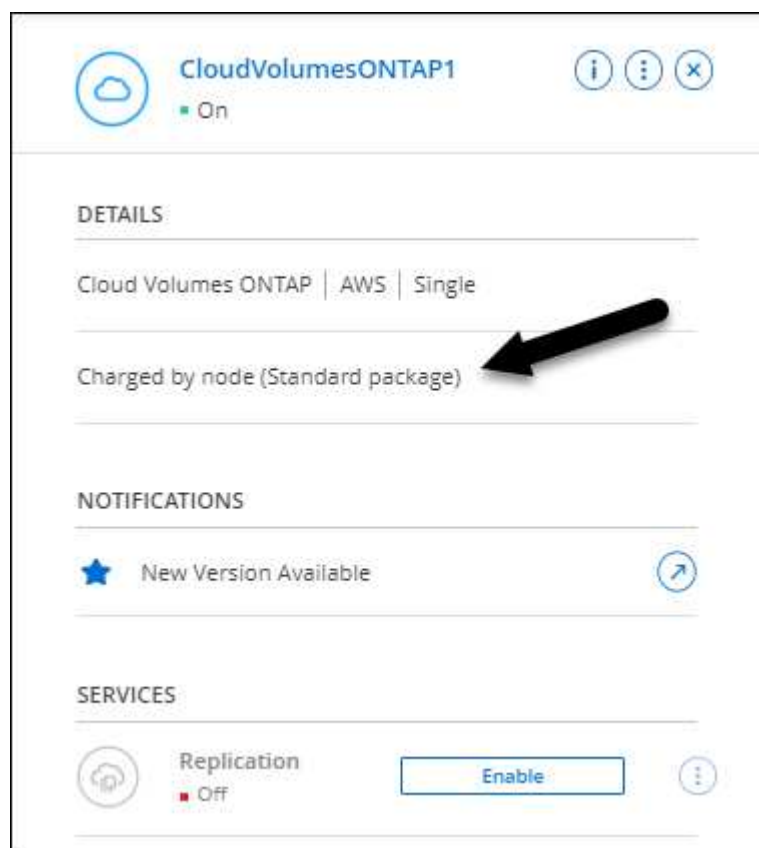
Vá para o ["Notas de versão do Cloud Volumes ONTAP"](#) para mais detalhes sobre as configurações suportadas.

Atualização de carregamento do FlexClone

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

Método de carregamento agora exibido

O BlueXP agora mostra o método de cobrança para cada ambiente de trabalho do Cloud Volumes ONTAP no painel direito do Canvas.



Escolha o seu nome de usuário

Ao criar um ambiente de trabalho do Cloud Volumes ONTAP , agora você tem a opção de inserir seu nome de usuário preferido, em vez do nome de usuário administrador padrão.

Credentials

User Name

customusername

Password

.....

Confirm Password

.....

Melhorias na criação de volume

Fizemos algumas melhorias na criação de volume:

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

✓ 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 Connector.

Cloud Volumes ONTAP 9.10.1

O BlueXP agora 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 Keystone para pagar por pares de Cloud Volumes ONTAP HA.

Uma assinatura Keystone é um serviço baseado em assinatura com pagamento conforme o crescimento que oferece uma experiência de nuvem híbrida perfeita para aqueles que preferem modelos de consumo de OpEx ao CapEx inicial ou leasing.

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

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

Suporte para nova região da AWS

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

Redução de porta

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

Essa alteração se aplica aos *novos* sistemas Cloud Volumes ONTAP a partir da versão 3.9.13 do Connector.

4 de outubro de 2021

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

Cloud Volumes ONTAP 9.10.0

O BlueXP agora 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 agora é, em média, 3 a 4 minutos menor.

2 de setembro de 2021

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

Chave de criptografia gerenciada pelo cliente no Azure

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

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

["Saiba mais sobre essas etapas"](#) .

7 de julho de 2021

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

Novos métodos de cobrança

Novos métodos de cobrança estão disponíveis para o Cloud Volumes ONTAP.

- **BYOL baseado em capacidade:** Uma licença baseada em capacidade permite que você pague pelo Cloud Volumes ONTAP por TiB de capacidade. A licença está associada à sua conta NetApp e permite que você crie vários sistemas Cloud Volumes ONTAP , desde que haja capacidade suficiente disponível por meio da sua licença. O licenciamento baseado em capacidade está disponível na forma de um pacote, *Essentials* ou *Professional*.
- **Oferta Freemium:** O Freemium permite que você use todos os recursos do Cloud Volumes ONTAP gratuitamente da NetApp (as taxas do 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 cobrança 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

Capacity-Based

Package

Professional

☐ Freemium (Up to 500GB)

Armazenamento WORM disponível para uso geral

O armazenamento WORM (grave uma vez e leia muitas vezes) não está mais em versão de visualização e agora está disponível para uso geral com o Cloud Volumes ONTAP. ["Saiba mais sobre o armazenamento WORM"](#) .

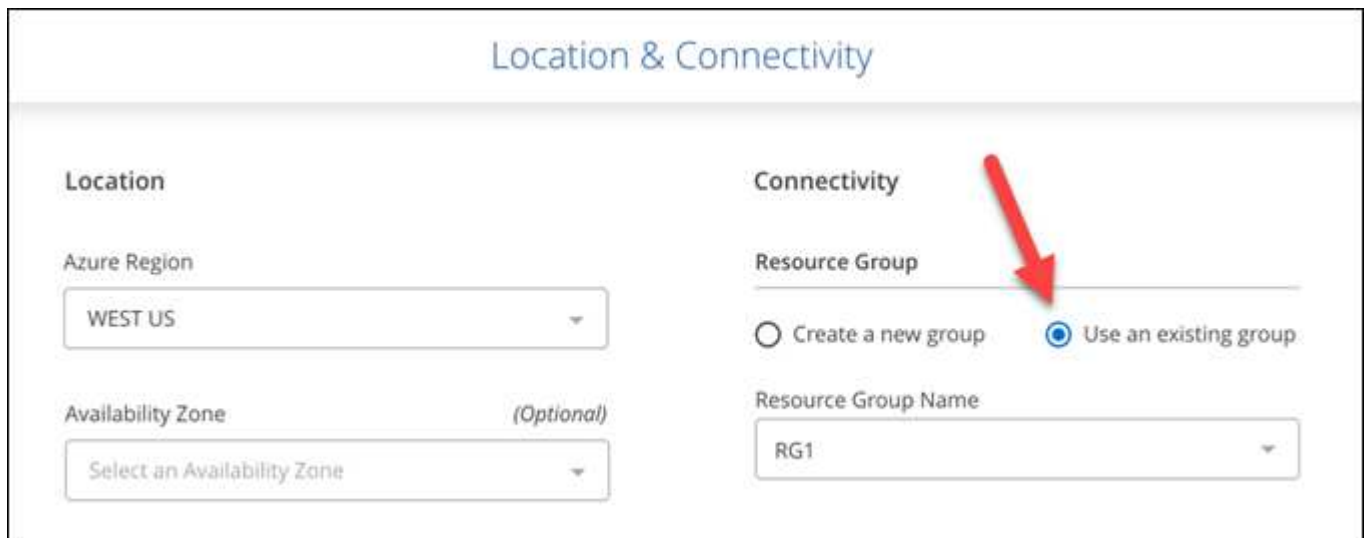
Suporte para m5dn.24xlarge na AWS

A partir da versão 9.9.1, o Cloud Volumes ONTAP agora oferece suporte ao tipo de instância m5dn.24xlarge com os seguintes métodos de cobrança: PAYGO Premium, traga sua própria licença (BYOL) e Freemium.

["Veja as configurações suportadas para o Cloud Volumes ONTAP na AWS"](#) .

Selecionar 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.



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

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

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

O acesso público ao blob agora está desabilitado no Azure

Como um aprimoramento de segurança, o BlueXP agora desabilita o **Acesso público ao 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 do Azure Private Link na conta de armazenamento de diagnóstico de inicialização para novos sistemas Cloud Volumes ONTAP .

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

["Saiba mais sobre como usar um Azure Private Link 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 desempenho e custo ao fornecer IOPS mais baixos por GiB.

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

O tipo de máquina custom-4-16384 não é mais compatível com os novos sistemas Cloud Volumes ONTAP .

Se você tiver um sistema existente em execução neste tipo de máquina, poderá continuar usando-o, mas recomendamos mudar para o tipo de máquina n2-standard-4.

["Ver configurações suportadas para o Cloud Volumes ONTAP no GCP"](#) .

30 de maio de 2021

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

Novo pacote profissional na AWS

Um novo Pacote Profissional permite que você combine o Cloud Volumes ONTAP e o Cloud Backup Service usando um contrato anual do AWS Marketplace. O pagamento é por TiB. Esta assinatura não permite que você faça backup de dados locais.

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

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

Tags em volumes 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 .

Essa alteração pode ajudar se sua organização usar políticas de controle de serviço (SCPs) para gerenciar permissões.

Período mínimo de resfriamento para política de escalonamento automático

Se você habilitou o armazenamento em camadas de dados em um volume usando a política de armazenamento em camadas *auto*, agora você pode ajustar o período mínimo de resfriamento usando a API.

["Aprenda como ajustar o período mínimo de resfriamento."](#)

Aprimoramento de políticas de exportação personalizadas

Ao criar um novo volume NFS, o BlueXP agora exibe políticas de exportação personalizadas em ordem crescente, facilitando a localização da política de exportação necessária.

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. Somente os dois instantâneos mais recentes são retidos para os volumes raiz e de inicialização.

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

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

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

24 de maio de 2021

Cloud Volumes ONTAP 9.9.1

O BlueXP agora 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 de abril de 2021

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

Relatório de espaço lógico

O BlueXP agora habilita relatórios de espaço lógico na VM de armazenamento inicial que ele cria para o Cloud Volumes ONTAP.

Quando o espaço é relatado logicamente, o ONTAP relata o espaço do volume de forma que todo o espaço físico economizado pelos recursos de eficiência de armazenamento também seja relatado como usado.

Suporte para discos gp3 na AWS

O Cloud Volumes ONTAP agora oferece suporte a discos *General Purpose SSD (gp3)*, a partir da versão 9.7. Os discos gp3 são os SSDs de menor custo que equilibram custo e desempenho para uma ampla variedade de cargas de trabalho.

["Dimensione seu sistema na AWS"](#) .

Discos HDD frios não são mais suportados na AWS

O Cloud Volumes ONTAP não oferece mais suporte a discos Cold HDD (sc1).

TLS 1.2 para contas de armazenamento do Azure

Quando o BlueXP cria contas de armazenamento no Azure para o Cloud Volumes ONTAP, a versão do 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 Connector.

Cloud Volumes ONTAP 9.9.0

O BlueXP agora 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 AWS Commercial Cloud Services (C2S).

["Implantar o Cloud Volumes ONTAP no AWS Secret Cloud ou no AWS Top Secret Cloud"](#) .

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 os dados em camadas no S3 serão criptografados se você selecionar uma CMK gerenciada pelo cliente. Anteriormente, apenas os dados do EBS eram criptografados.

Observe que você precisará fornecer à função IAM do Cloud Volumes ONTAP acesso para usar a 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 6 (IL6) do Departamento de Defesa (DoD) do Azure.

Redução de endereço IP no Google Cloud

Reduzimos o número de endereços IP necessários para o Cloud Volumes ONTAP 9.8 e posteriores no Google Cloud. Por padrão, um endereço IP a menos é necessário (unificamos o LIF intercluster com o LIF de gerenciamento de nós). Você também tem a opção de pular a criação do LIF de gerenciamento do 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"](#) .

Suporte a VPC compartilhada no Google Cloud

Ao implantar um par de Cloud Volumes ONTAP HA no Google Cloud, agora você pode escolher VPCs compartilhadas para VPC-1, VPC-2 e VPC-3. Anteriormente, somente a VPC-0 podia ser uma VPC compartilhada. Essa alteração é compatível com o Cloud Volumes ONTAP 9.8 e posteriores.

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

4 de janeiro de 2021

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

Postos avançados da AWS

Há alguns meses, anunciamos que o Cloud Volumes ONTAP alcançou a designação Amazon Web Services (AWS) Outposts Ready. 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, poderá implantar o Cloud Volumes ONTAP nesse Outpost selecionando a VPC do Outpost no assistente do ambiente de trabalho. A experiência é a mesma de qualquer outra VPC que reside na AWS. Observe que você precisará primeiro implantar um conector no seu AWS Outpost.

Há algumas limitações a serem apontadas:

- Somente sistemas Cloud Volumes ONTAP de nó único são suportados no momento
- As instâncias do EC2 que você pode usar com o Cloud Volumes ONTAP são limitadas ao que está disponível no seu Outpost
- Somente SSDs de uso geral (gp2) são suportados no momento

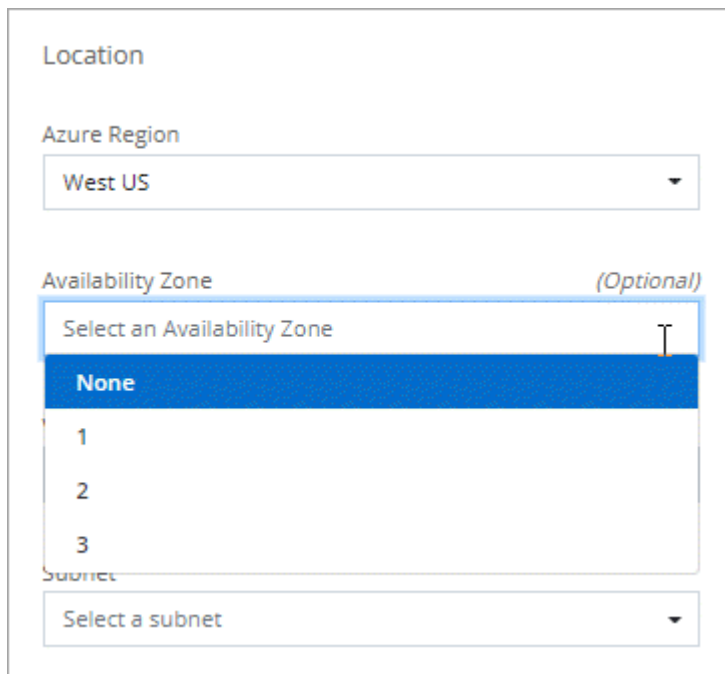
Ultra SSD VNVRAM em regiões do Azure com suporte

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

A VNVRAM oferece 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.



Location

Azure Region

West US

Availability Zone (Optional)

Select an Availability Zone

None

1

2

3

Subnet

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 máquinas no Google Cloud

O Cloud Volumes ONTAP agora oferece suporte aos seguintes tipos de máquinas:

- 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 de novembro de 2020

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

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 pontos de extremidade no Azure.

- ["Saiba mais sobre os Links Privados do Azure"](#)
- ["Saiba mais sobre como usar um Azure Private Link com o Cloud Volumes ONTAP"](#)

Limitações conhecidas

Limitações conhecidas identificam plataformas, dispositivos ou funções que não são suportados por esta versão do produto ou que não interoperam corretamente com ele. Revise essas limitações cuidadosamente.

Essas limitações são específicas do gerenciamento do Cloud Volumes ONTAP no NetApp Console. Para visualizar as limitações do próprio software Cloud Volumes ONTAP, ["acesse as Notas de versão do Cloud Volumes ONTAP"](#).

O console não oferece suporte à criação de volumes FlexGroup

Embora o Cloud Volumes ONTAP ofereça suporte a volumes FlexGroup, o Console atualmente não oferece suporte à criação de volumes FlexGroup. Se você criar um volume FlexGroup do ONTAP System Manager ou do ONTAP CLI, deverá definir o modo de Gerenciamento de Capacidade no Console como `Manual`. `Automatic` O modo pode não funcionar corretamente com volumes FlexGroup.



A capacidade de criar volumes FlexGroup no Console está planejada para uma versão futura.

O console não oferece suporte ao S3 com o Cloud Volumes ONTAP

Embora o Cloud Volumes ONTAP ofereça suporte ao S3 como uma opção para armazenamento escalável, o

Console não fornece nenhum recurso de gerenciamento para esse recurso. Usar a CLI é a prática recomendada para configurar o acesso do cliente S3 do Cloud Volumes ONTAP. Para mais detalhes, consulte o ["Guia de configuração do S3"](#) .

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

O console não oferece suporte à recuperação de desastres para VMs de armazenamento

O Console não fornece nenhum suporte de configuração ou orquestração para recuperação de desastres de VM de armazenamento (SVM). Você deve usar o ONTAP System Manager ou o ONTAP CLI.

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

Notas de versão do Cloud Volumes ONTAP

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

["Acesse as notas de versão do Cloud Volumes ONTAP"](#)

Começar

Saiba mais sobre o Cloud Volumes ONTAP

O Cloud Volumes ONTAP permite que você otimize seus custos e desempenho de armazenamento em nuvem, ao mesmo tempo em que melhora a proteção, a segurança e a conformidade dos dados.

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

- Eficiências de armazenamento

Aproveite a deduplicação de dados, a compactação de dados, o provisionamento fino e a clonagem integrados para minimizar os custos de armazenamento.

- Alta disponibilidade

Garanta a confiabilidade empresarial e operações contínuas em caso de falhas no seu ambiente de nuvem.

- Proteção de dados

O Cloud Volumes ONTAP utiliza o SnapMirror, a tecnologia de replicação líder do setor da NetApp, para replicar dados locais para a nuvem, facilitando a disponibilidade de cópias secundárias para vários casos de uso.

O Cloud Volumes ONTAP também se integra ao NetApp Backup and Recovery para fornecer recursos de backup e restauração para proteção e arquivamento de longo prazo dos seus dados na nuvem.

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

- Camadas de dados

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

- Consistência da aplicação

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

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

- Segurança de dados

O Cloud Volumes ONTAP oferece suporte à criptografia de dados e proteção contra vírus e ransomware.

- Controles de conformidade de privacidade

A integração com a Classificação de Dados da NetApp ajuda você a entender o contexto dos dados e identificar dados confidenciais.

["Saiba mais sobre Classificação de Dados"](#)



Licenças para recursos do ONTAP estão incluídas no Cloud Volumes ONTAP.

["Ver configurações Cloud Volumes ONTAP suportadas"](#)

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

Versões ONTAP suportadas para implantações do Cloud Volumes ONTAP

O NetApp Console permite que você escolha entre várias versões diferentes do ONTAP ao adicionar um sistema Cloud Volumes ONTAP .

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

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 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

Azul

Nó único

- 9.17.1 RC1
- 9.16.1 GA
- 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 HA

- 9.17.1 RC1
- 9.16.1 GA
- 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

- 9.17.1 RC1
- 9.16.1 GA
- 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 HA

- 9.17.1 RC1
- 9.16.1 GA
- 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 na Amazon Web Services

Início rápido para Cloud Volumes ONTAP na AWS

Comece a usar o Cloud Volumes ONTAP na AWS em poucas etapas.

1

Criar um agente de console

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

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

2

Planeje sua configuração

O Console oferece pacotes pré-configurados que correspondem aos seus requisitos de carga de trabalho, ou você pode criar sua própria configuração. Se você escolher sua própria configuração, deverá entender as opções disponíveis. ["Saber mais"](#) .

3

Configure sua rede

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

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

3. Configure um endpoint VPC para o serviço S3.

Um endpoint VPC é necessário se você quiser hierarquizar dados frios do Cloud Volumes ONTAP para armazenamento de objetos de baixo custo.

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

4

Configurar o AWS KMS

Se você quiser usar a criptografia da Amazon com o Cloud Volumes ONTAP, precisará garantir que exista 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 agente do Console como um *usuário de chave*. ["Saber mais"](#) .

5

Inicie o Cloud Volumes ONTAP usando o Console

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

Links relacionados

- ["Crie um agente de console para AWS"](#)
- ["Crie um agente de console no AWS Marketplace"](#)
- ["Instalar e configurar um agente do Console no local"](#)
- ["Permissões da AWS para o agente do Console"](#)

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 seus requisitos de carga de trabalho ou pode criar sua própria configuração. Se você escolher sua própria configuração, deverá entender as opções disponíveis.

Escolha uma licença do Cloud Volumes ONTAP

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

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

Escolha uma região com suporte

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

Regiões mais recentes da AWS devem ser habilitadas antes que você possa criar e gerenciar recursos nessas regiões. ["Documentação da AWS: Aprenda como habilitar uma região"](#) .

Escolha uma Zona Local com suporte

Selecionar uma Zona Local é opcional. O Cloud Volumes ONTAP é suportado em algumas zonas locais da AWS, incluindo Cingapura. O Cloud Volumes ONTAP na AWS oferece suporte apenas ao modo de alta disponibilidade (HA) em uma única zona de disponibilidade. Implantações de nó único não são suportadas.



O Cloud Volumes ONTAP não oferece suporte para camadas de dados e camadas de nuvem em zonas locais da AWS. Além disso, zonas locais com instâncias que não foram qualificadas para o Cloud Volumes ONTAP não são suportadas. Um exemplo disso é Miami, que não está disponível como uma Zona Local, porque tem apenas instâncias Gen6 que não são suportadas e não qualificadas.

["Documentação da AWS: Veja a lista completa de Zonas Locais"](#) . As Zonas Locais devem ser habilitadas antes que você possa criar e gerenciar recursos nessas zonas.

["Documentação da AWS: Introdução às Zonas Locais da AWS"](#) .

Escolha uma instância suportada

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

["Configurações com suporte para Cloud Volumes ONTAP na AWS"](#)

Entenda os limites de armazenamento

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

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

Dimensione seu sistema na AWS

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

Tipo de instância

- Adapte seus requisitos de carga de trabalho ao rendimento máximo e IOPS para cada tipo de instância 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 lido com frequência, escolha um sistema com RAM suficiente.
 - ["Documentação da AWS: Tipos de instância do Amazon EC2"](#)
 - ["Documentação da AWS: Instâncias otimizadas para Amazon EBS"](#)

Tipo de disco EBS

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

- Os discos *SSD de uso geral (gp3)* são os SSDs de menor custo que equilibram custo e desempenho para uma ampla gama de cargas de trabalho. O desempenho é definido em termos de IOPS e taxa de transferência. Os discos gp3 são suportados com o Cloud Volumes ONTAP 9.7 e posteriores.

Quando você seleciona um disco gp3, o NetApp Console preenche os valores padrão de IOPS e taxa de transferência que fornecem desempenho equivalente a um disco gp2 com base no tamanho do disco selecionado. Você pode aumentar os valores para obter melhor desempenho a um custo mais alto, mas não oferecemos suporte a valores menores porque isso pode resultar em desempenho inferior. Resumindo, mantenha os valores padrões ou aumente-os. Não os abaixe. ["Documentação da AWS: Saiba mais sobre discos gp3 e seu desempenho"](#) .

Observe que o Cloud Volumes ONTAP oferece suporte ao recurso Amazon EBS Elastic Volumes com discos gp3. ["Saiba mais sobre o suporte do Elastic Volumes"](#) .

- Os discos *SSD de uso geral (gp2)* equilibram custo e desempenho para uma ampla gama de cargas de trabalho. O desempenho é definido em termos de IOPS.
- Os discos *Provisioned IOPS SSD (io1)* são para aplicativos críticos que exigem o mais alto desempenho a um custo mais alto.

Observe que o Cloud Volumes ONTAP oferece suporte ao recurso Amazon EBS Elastic Volumes com discos io1. ["Saiba mais sobre o suporte do Elastic Volumes"](#) .

- Os discos *Throughput Optimized HDD (st1)* são para cargas de trabalho acessadas com frequência que exigem throughput rápido e consistente a um preço mais baixo.



A hierarquização de dados 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"](#) , então você precisa escolher um tamanho de disco inicial ao iniciar um sistema Cloud Volumes ONTAP . Depois disso, você pode ["deixe o Console gerenciar a capacidade de um sistema para você"](#) , mas se você quiser ["crie agregados você mesmo"](#) , esteja ciente do seguinte:

- Todos os discos em um agregado devem ter o mesmo tamanho.
- O desempenho dos discos EBS está vinculado ao tamanho do disco. O tamanho determina o IOPS de base e a duração máxima de burst para discos SSD e a taxa de transferência de base e burst para discos HDD.
- No final das contas, você deve escolher o tamanho do disco que lhe dará o *desempenho sustentado* que você precisa.
- Mesmo se você escolher discos maiores (por exemplo, seis discos de 4 TiB), talvez não obtenha todos os IOPS porque a instância EC2 pode atingir seu limite de largura de banda.

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

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

Exibir discos de sistema padrão

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

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



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

Preparar para implantar o Cloud Volumes ONTAP em um AWS Outpost

Se você tiver um AWS Outpost, poderá implantar o Cloud Volumes ONTAP nesse Outpost selecionando a VPC do Outpost durante o processo de implantação. A experiência é a mesma de qualquer outra VPC que

reside na AWS. Observe que você precisará primeiro implantar um agente de console no seu AWS Outpost.

Há algumas limitações a serem apontadas:

- Somente sistemas Cloud Volumes ONTAP de nó único são suportados no momento
- As instâncias do EC2 que você pode usar com o Cloud Volumes ONTAP são limitadas ao que está disponível no seu Outpost
- Somente SSDs de uso geral (gp2) são suportados no momento

Coletar 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 informações do seu administrador.

Nó único ou par HA em uma única AZ

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

Par HA em múltiplas AZs

Informações da AWS	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	

Informações da AWS	Seu valor
Endereço IP flutuante para dados no nó 2	
Tabelas de rotas para endereços IP flutuantes	

Escolha uma velocidade de gravação

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

Escolha um perfil de uso de volume

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

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

Provisionamento fino

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

Desduplicação

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

Compressão

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

Configure sua rede

Configurar a rede AWS para o Cloud Volumes ONTAP

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

Requisitos gerais

Certifique-se de ter atendido aos seguintes requisitos na AWS.

Acesso de saída à Internet para nós do Cloud Volumes ONTAP

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

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

Pontos de extremidade Cloud Volumes ONTAP

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

Pontos finais	Aplicável para	Propósito	Modos de implantação	Impacto se o ponto final não estiver disponível
\ https://netapp-cloud-account.auth0.com	Autenticação	Usado para autenticação no Console.	Modos padrão e restrito.	A autenticação do usuário falha e os seguintes serviços permanecem indisponíveis: • Serviços Cloud Volumes ONTAP • Serviços ONTAP • Protocolos e serviços de proxy
\ https://api.bluexp.net/app.com/tenancy	Arrendamento	Usado para recuperar o recurso Cloud Volumes ONTAP do Console para autorizar recursos e usuários.	Modos padrão e restrito.	Os recursos do Cloud Volumes ONTAP e os usuários não estão autorizados.
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Usado para enviar dados de telemetria do AutoSupport para o suporte da NetApp.	Modos padrão e restrito.	As informações do AutoSupport continuam não entregues.

Pontos finais	Aplicável para	Propósito	Modos de implantação	Impacto se o ponto final não estiver disponível
O ponto final comercial exato para o serviço AWS (com sufixo <code>amazonaws.com</code>) depende da região da AWS que você está usando. Consulte o "Documentação da AWS para detalhes" .	• CloudFormation • Nuvem de Computação Elástica (EC2) • Gerenciamento de Identidade e Acesso (IAM) • Serviço de Gerenciamento de Chaves (KMS) • Serviço de Token de Segurança (STS) • Serviço de Armazenamento Simples (S3)	Comunicação com serviços da AWS.	Modos padrão e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço da AWS para executar operações específicas na AWS.
O ponto de extremidade governamental exato para o serviço da AWS depende da região da AWS que você está usando. Os pontos finais são sufixados com <code>amazonaws.com</code> e <code>ec2s.ic.gov</code> . Consulte "SDK da AWS" e "Documentação da AWS" para maiores informações.	• CloudFormation • Nuvem de Computação Elástica (EC2) • Gerenciamento de Identidade e Acesso (IAM) • Serviço de Gerenciamento de Chaves (KMS) • Serviço de Token de Segurança (STS) • Serviço de Armazenamento Simples (S3)	Comunicação com serviços da AWS.	Modo restrito.	O Cloud Volumes ONTAP não pode se comunicar com o serviço da AWS para executar operações específicas na AWS.

Acesso de saída à Internet para o mediador HA

A instância do mediador HA deve ter uma conexão de saída com o serviço AWS EC2 para que possa auxiliar no failover de armazenamento. 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 VPC de interface da sub-rede de destino para o serviço AWS EC2. Para obter detalhes sobre os endpoints VPC, consulte o ["Documentação da AWS: Interface VPC Endpoints \(AWS PrivateLink\)"](#).

Configuração de proxy de rede do agente do NetApp Console

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

- **Proxy explícito:** O tráfego de saída do Cloud Volumes ONTAP usa o endereço HTTP do servidor proxy especificado durante a configuração de proxy do agente do Console. O administrador também pode ter configurado credenciais de usuário e certificados de CA raiz para autenticação adicional. Se um certificado de CA raiz estiver disponível para o proxy explícito, certifique-se de obter e carregar o mesmo certificado para o seu sistema Cloud Volumes ONTAP usando o ["ONTAP CLI: instalação do certificado de segurança"](#) comando.
- **Proxy transparente:** A rede está configurada para rotear automaticamente o tráfego de saída do Cloud Volumes ONTAP por meio do proxy para o agente do Console. Ao configurar um proxy transparente, o administrador precisa fornecer apenas um certificado de CA raiz para conectividade do Cloud Volumes ONTAP, não o endereço HTTP do servidor proxy. Certifique-se de obter e carregar o mesmo certificado de CA raiz para o seu sistema Cloud Volumes ONTAP usando o ["ONTAP CLI: instalação do certificado de segurança"](#) comando.

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

Endereços IP privados

O Console aloca automaticamente o número necessário de endereços IP privados para o Cloud Volumes ONTAP. Você precisa garantir que sua rede tenha endereços IP privados suficientes disponíveis.

O número de LIFs que o Console aloca para o Cloud Volumes ONTAP depende se você implanta um sistema de nó único ou um par de HA. Um LIF é um endereço IP associado a uma porta física.

Endereços IP para um sistema de nó único

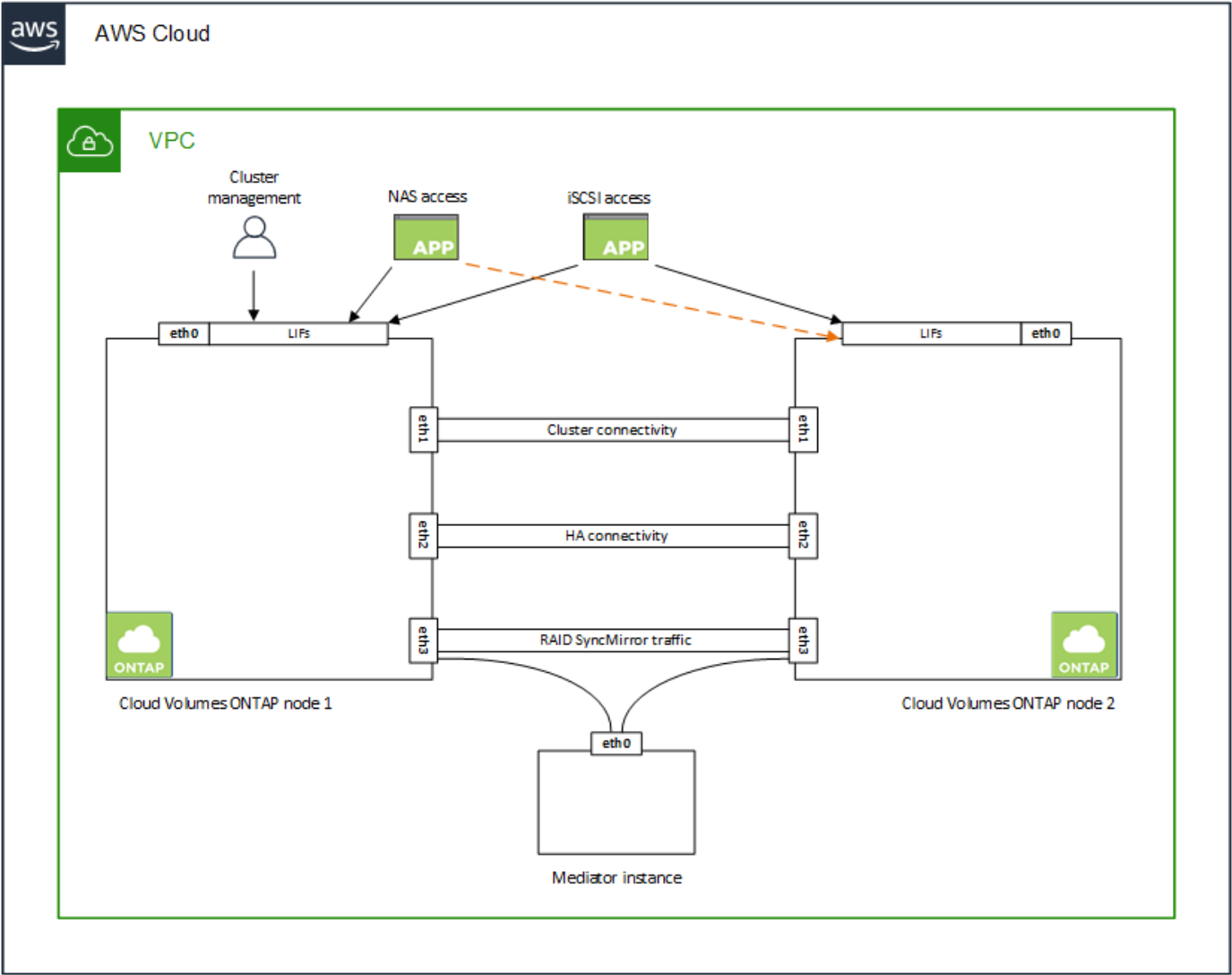
O Console aloca 6 endereços IP para um único sistema de nó.

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

LIF	Propósito
Gerenciamento de cluster	Gerenciamento administrativo de todo o cluster (par HA).
Gerenciamento de nós	Gerenciamento administrativo de um nó.
Interaglomerado	Comunicação entre clusters, backup e replicação.
Dados NAS	Acesso do cliente por meio de protocolos NAS.
Dados iSCSI	Acesso do 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 excluído.
Gerenciamento de VM de armazenamento	Um LIF de gerenciamento de VM de armazenamento é usado com ferramentas de gerenciamento como o SnapCenter.

Endereços IP para pares HA

Os pares HA exigem mais endereços IP do que um sistema de nó único. Esses endereços IP estão distribuídos por diferentes interfaces Ethernet, conforme 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 *única* Zona de Disponibilidade (AZ) da AWS requer 15 endereços IP privados, enquanto um par de HA implantado em *várias* AZs requer 13 endereços IP privados.

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

LIF	Interface	Nó	Propósito
Gerenciamento de cluster	eth0	nó 1	Gerenciamento administrativo de todo o cluster (par HA).
Gerenciamento de nós	eth0	nó 1 e nó 2	Gerenciamento administrativo de um nó.
Interaglomerado	eth0	nó 1 e nó 2	Comunicação entre clusters, backup e replicação.

LIF	Interface	Nó	Propósito
Dados NAS	eth0	nó 1	Acesso do cliente por meio de protocolos NAS.
Dados iSCSI	eth0	nó 1 e nó 2	Acesso do cliente através do protocolo iSCSI. Também usado pelo sistema para outros fluxos de trabalho de rede importantes. Esses 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 RSM iSCSI	eth3	nó 1 e nó 2	Tráfego RAID SyncMirror iSCSI, bem como 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 auxiliar nos processos de aquisição e devolução de armazenamento.

LIF	Interface	Nó	Propósito
Gerenciamento de nós	eth0	nó 1 e nó 2	Gerenciamento administrativo de um nó.
Interaglomerado	eth0	nó 1 e nó 2	Comunicação entre clusters, backup e replicação.
Dados iSCSI	eth0	nó 1 e nó 2	Acesso do cliente através do protocolo iSCSI. Esses LIFs também gerenciam a migração de endereços IP flutuantes entre nós. Esses 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 RSM iSCSI	eth3	nó 1 e nó 2	Tráfego RAID SyncMirror iSCSI, bem como 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 auxiliar nos processos de aquisição e devolução de armazenamento.



Quando implantados em várias Zonas de Disponibilidade, vários LIFs são associados a "[endereços IP flutuantes](#)", que não contam para o limite de IP privado da AWS.

Grupos de segurança

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



Procurando informações sobre o agente do Console? ["Exibir regras de grupo de segurança para o agente do Console"](#)

Conexão para hierarquização de dados

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

Ao criar o VPC Endpoint, certifique-se de selecionar a região, a VPC e a tabela de rotas que correspondem à instância do Cloud Volumes ONTAP . Você também deve modificar o grupo de segurança para adicionar uma regra HTTPS de saída que habilite o tráfego para o ponto de extremidade S3. Caso contrário, o Cloud Volumes ONTAP não poderá se conectar ao serviço S3.

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

Conexões com sistemas ONTAP

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

DNS e Active Directory para CIFS

Se você quiser provisionar armazenamento CIFS, deverá configurar o DNS e o Active Directory na AWS ou estender 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 EC2 padrão, que não deve ser o servidor DNS usado pelo ambiente do Active Directory.

Para obter instruções, consulte o ["Documentação da AWS: Serviços de Domínio do Active Directory na Nuvem AWS: Implantação de Referência de Início Rápido"](#) .

Compartilhamento de VPC

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

["Aprenda a implantar um par HA em uma sub-rede compartilhada"](#) .

Requisitos para pares de HA em várias AZs

Requisitos adicionais de rede da AWS se aplicam às configurações de alta disponibilidade do Cloud Volumes ONTAP que usam várias zonas de disponibilidade (AZs). Você deve revisar esses requisitos antes de iniciar

um par de HA porque deve inserir os detalhes de rede no Console ao adicionar um sistema Cloud Volumes ONTAP .

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

Zonas de disponibilidade

Este modelo de implantação de HA usa várias AZs para garantir alta disponibilidade dos 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 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 várias AZs usam endereços IP flutuantes que migram entre nós se ocorrerem falhas. Eles não são nativamente acessíveis de fora do VPC, a menos que você "[configure um gateway de trânsito da AWS](#)" .

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



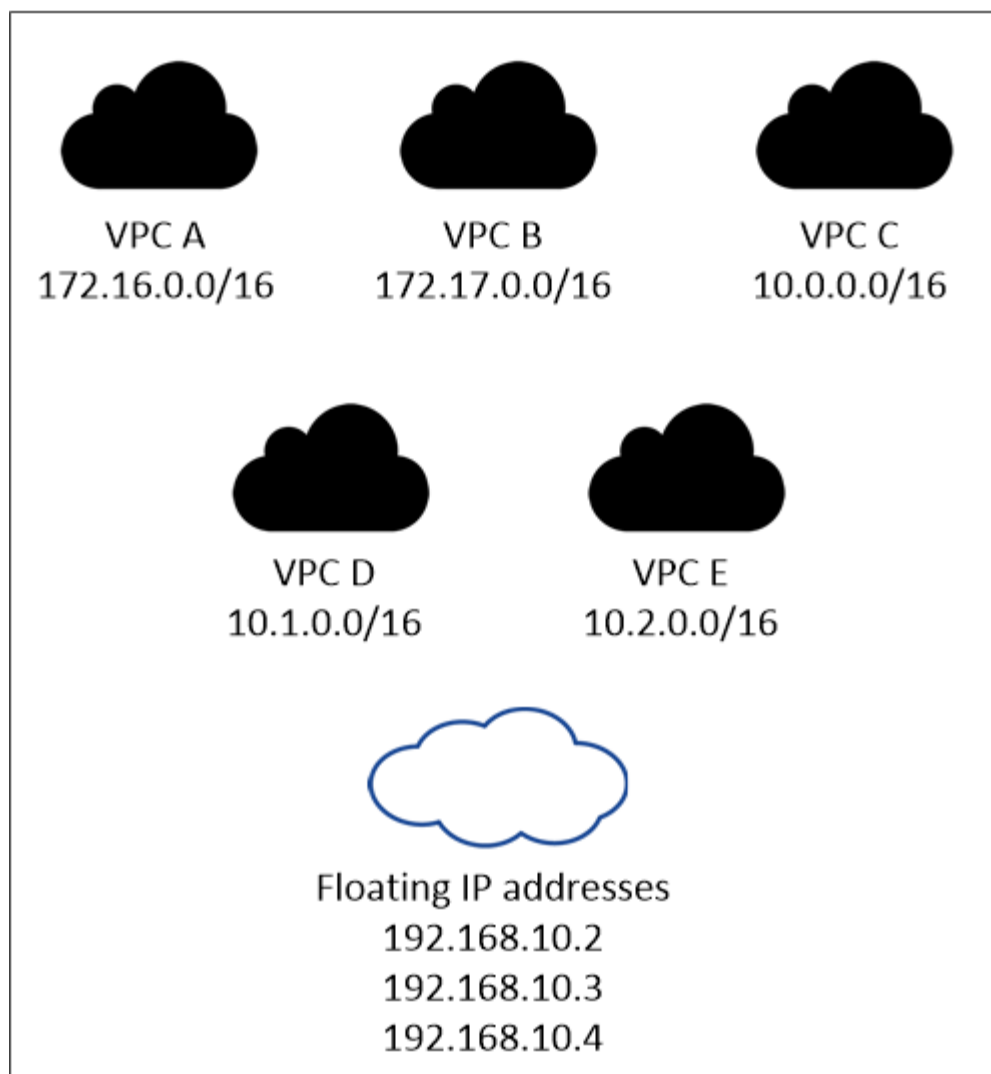
Um endereço IP flutuante é necessário para o LIF de gerenciamento do SVM se você usar o SnapDrive para Windows ou o SnapCenter com o par HA.

Você precisa inserir os endereços IP flutuantes ao adicionar um sistema Cloud Volumes ONTAP HA. O Console aloca os endereços IP ao par HA quando inicia o sistema.

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

O exemplo a seguir mostra a relação entre endereços IP flutuantes e as VPCs em uma região da AWS. Embora os endereços IP flutuantes estejam fora dos blocos CIDR para todas as VPCs, eles podem ser roteados para sub-redes por meio de tabelas de rotas.

AWS region



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

Gateway de trânsito para permitir acesso IP flutuante de fora da VPC

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

Tabelas de rotas

Depois de especificar os endereços IP flutuantes, você será solicitado a selecionar as tabelas de rotas que devem incluir rotas para os endereços IP flutuantes. Isso permite o acesso do cliente ao par HA.

Se você tiver apenas uma tabela de rotas para as sub-redes na sua VPC (a tabela de rotas principal), o Console adicionará automaticamente os endereços IP flutuantes a essa tabela de rotas. Se você tiver mais de uma tabela de rotas, é muito importante selecionar as tabelas de rotas 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 diferentes tabelas de rotas. Se você selecionar a tabela de rotas A, mas não a tabela de rotas B, os clientes na sub-rede associada à tabela de rotas A

poderão acessar o par HA, mas os clientes na sub-rede associada à tabela de rotas B não poderão.

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

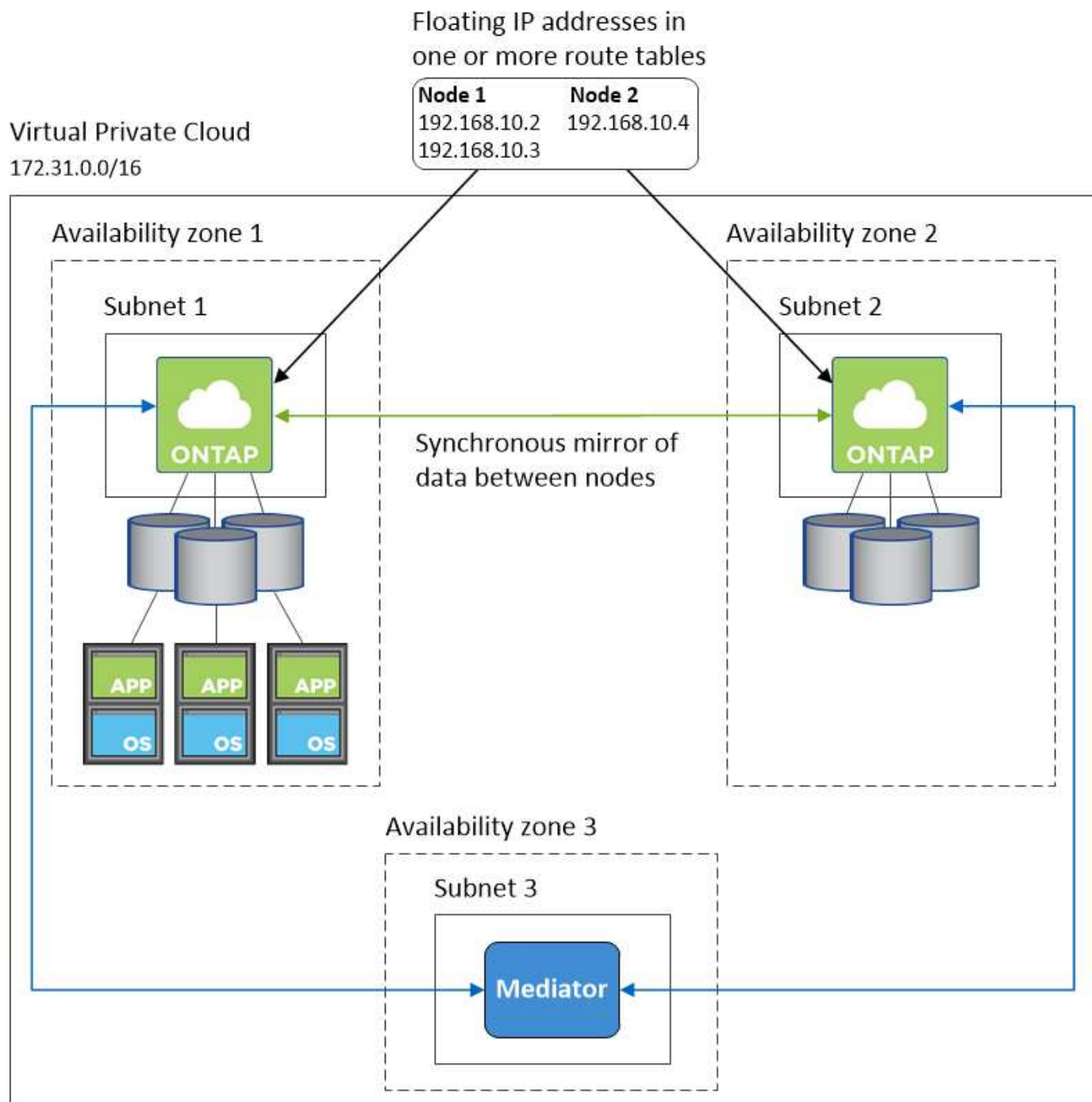
Conexão com ferramentas de gerenciamento da NetApp

Para usar ferramentas de gerenciamento do NetApp com configurações de HA que estão em várias AZs, você tem duas opções de conexão:

1. Implante as ferramentas de gerenciamento do NetApp em uma VPC diferente e ["configurar um gateway de trânsito da AWS"](#) . O gateway permite o acesso ao endereço IP flutuante para a interface de gerenciamento do cluster de fora da VPC.
2. Implante as ferramentas de gerenciamento do NetApp na mesma VPC com uma configuração de roteamento semelhante à dos clientes NAS.

Exemplo de configuração de HA

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



Requisitos para o agente do console

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

- ["Exibir requisitos de rede para o agente do Console"](#)
- ["Regras de grupo de segurança na AWS"](#)

Tópicos relacionados

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

Configurar um gateway de trânsito da AWS para pares de alta disponibilidade do Cloud Volumes ONTAP

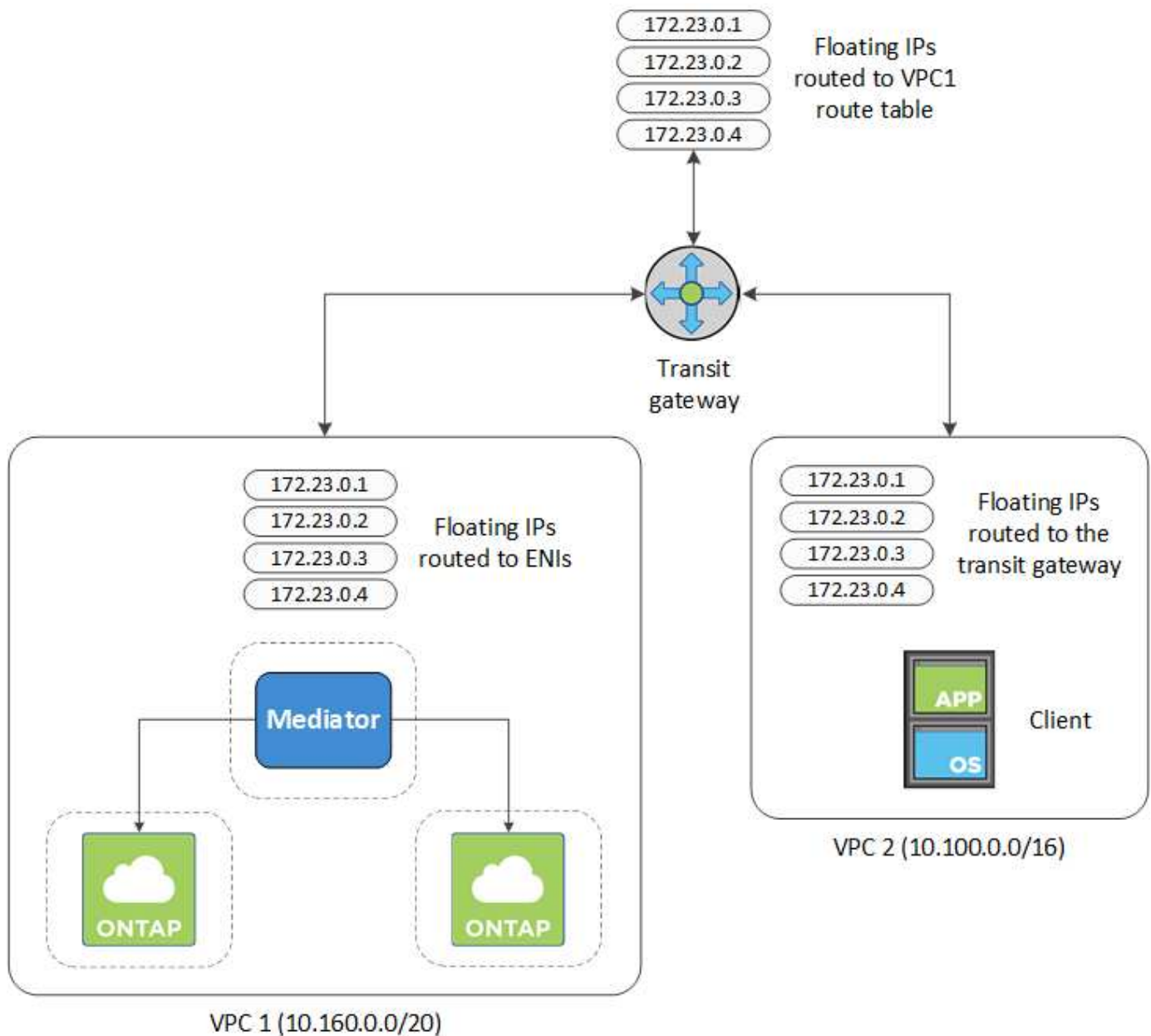
Configure um gateway de trânsito da AWS para permitir o acesso a um par de HA "endereços IP flutuantes" de fora da VPC onde o par HA reside.

Quando uma configuração do Cloud Volumes ONTAP HA é distribuída em várias zonas de disponibilidade da AWS, endereços IP flutuantes são necessários para acesso a dados do NAS de dentro da VPC. Esses endereços IP flutuantes podem migrar entre nós quando ocorrem falhas, mas não são nativamente 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 SVM opcional.

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

Aqui está um exemplo que mostra duas VPCs conectadas por um gateway de trânsito. Um sistema HA reside em uma VPC, enquanto um cliente reside na outra. Você pode então 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 anexe as VPCs ao gateway" .
2. Associe as VPCs à tabela de rotas do gateway de trânsito.
 - a. No serviço **VPC**, clique em **Tabelas de rotas do gateway de trânsito**.
 - b. Selecione a tabela de rotas.
 - c. Clique em **Associações** e depois selecione **Criar associação**.
 - d. Escolha os anexos (VPCs) a serem associados 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 de informações do sistema no NetApp Console. 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. Inclui rotas para os blocos CIDR das duas 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

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

Floating IP Addresses

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

- Adicione entradas de rota aos endereços IP flutuantes.
- Adicione uma entrada de rota ao bloco CIDR da VPC onde o par 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	lgw-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 rotas para a VPC do par HA adicionando uma rota à VPC que precisa de acesso aos endereços IP flutuantes.

Esta etapa é importante porque conclui o roteamento entre as VPCs.

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

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

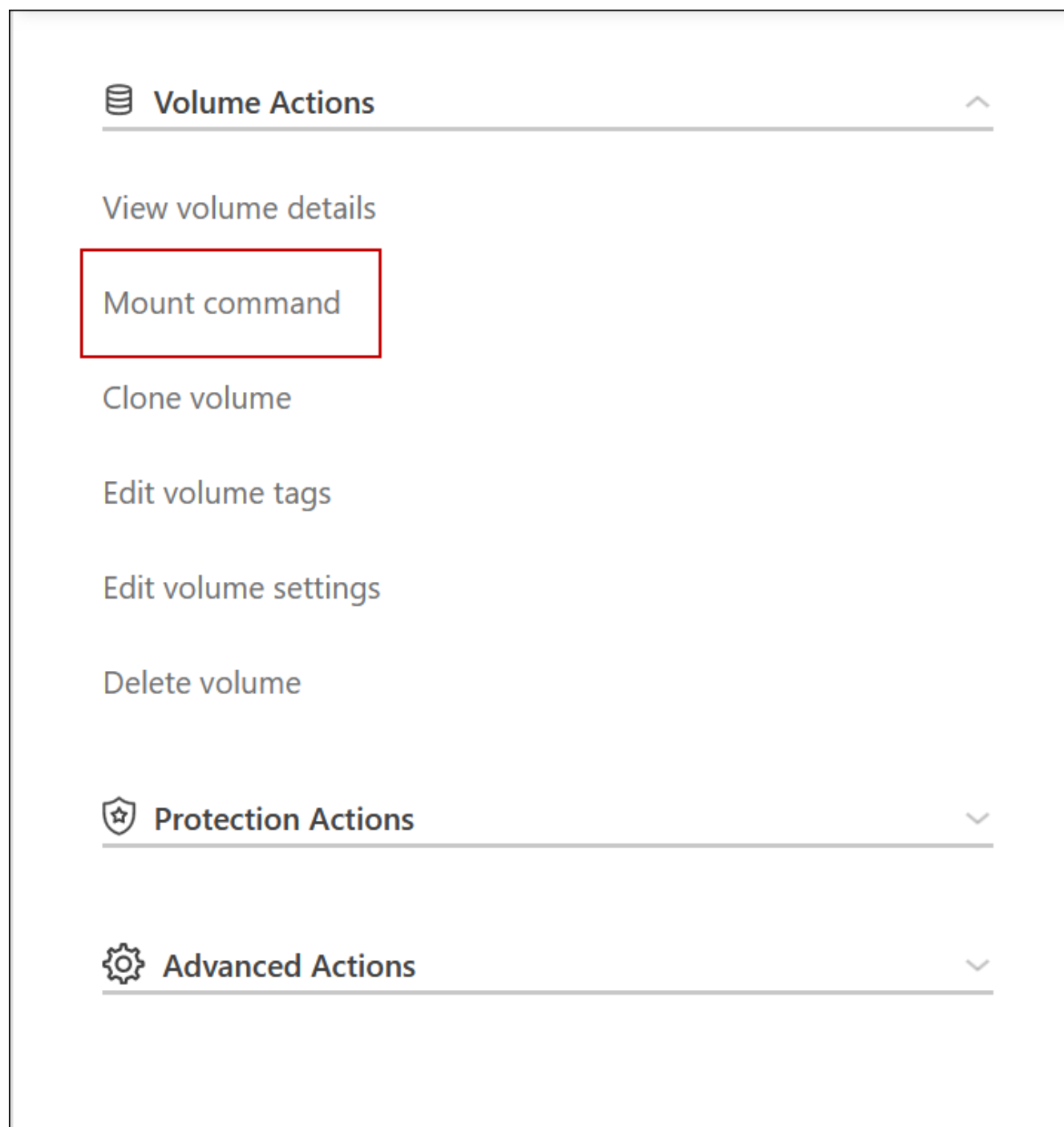
Destination	Target	Status
10.160.0.0/20	local	active
pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22)	vpce-cb51a0a2	active
0.0.0.0/0	lgw-b2182dd7	active
10.60.29.0/25	pcx-589c3331	active
10.100.0.0/16	tgw-015b7c249661ac279	active
10.129.0.0/20	pcx-ff7e1396	active
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 para a VPC.
- Em Nuvem Privada Virtual, clique em **Sub-redes**.
 - Clique na aba **Tabela de rotas**, selecione o ambiente desejado para um dos endereços IP flutuantes para um par HA.
 - Clique em **Grupos de segurança**.
 - Selecione **Editar regras de entrada**.
 - Clique em **Adicionar regra**.
 - Em Tipo, selecione **Todo o tráfego** e, em seguida, selecione o endereço IP da VPC.
 - 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 Console por meio da opção **Comando de montagem** no

painel Gerenciar volumes no Console.



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

["Aprenda a editar um volume"](#) .

Links relacionados

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

Implantar pares de Cloud Volumes ONTAP HA em uma sub-rede compartilhada da AWS

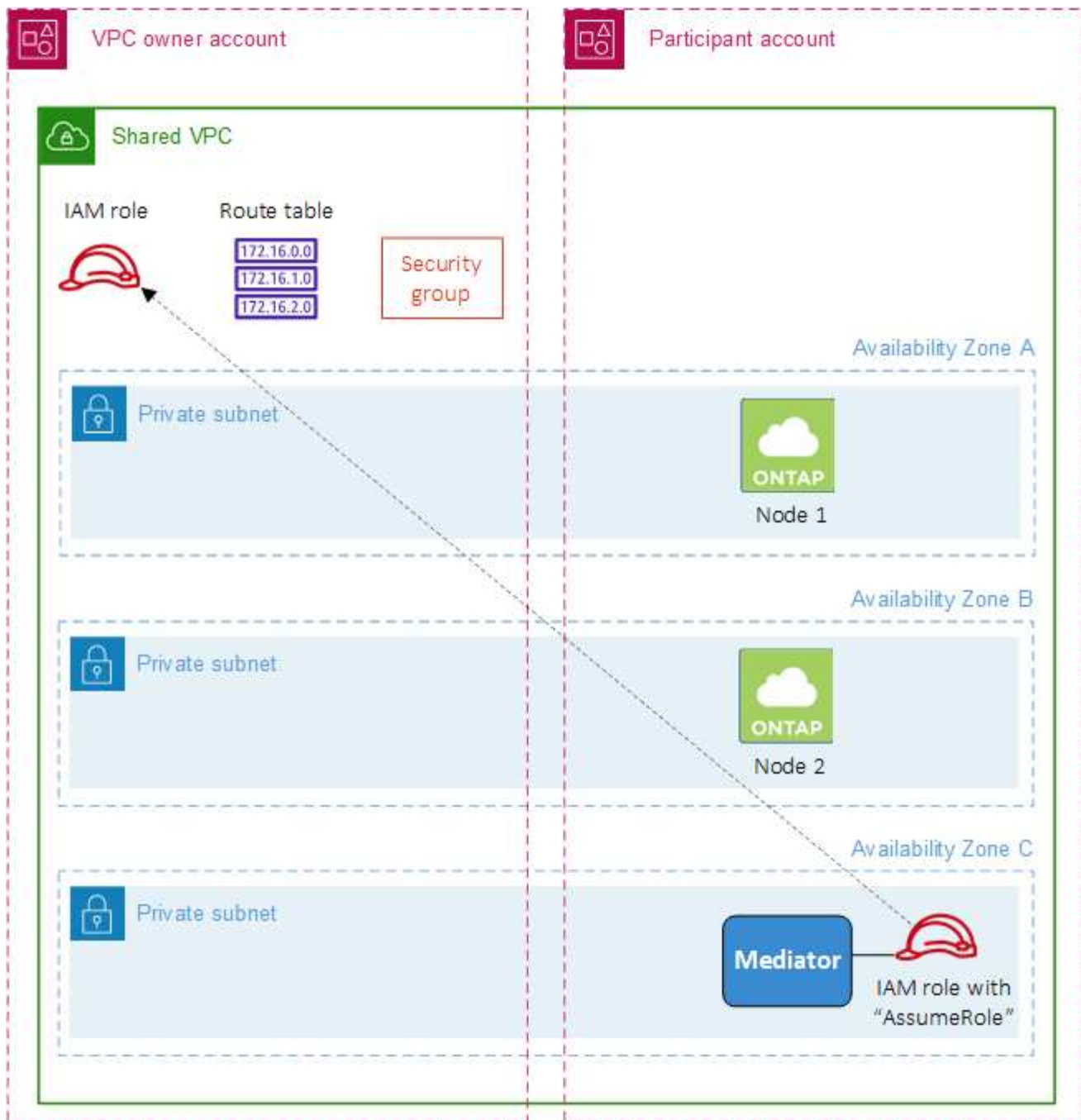
A partir da versão 9.11.1, os pares de HA do Cloud Volumes ONTAP são suportados na AWS com compartilhamento de VPC. O compartilhamento de VPC permite que sua organização compartilhe sub-redes com outras contas da AWS. Para usar esta configuração, você deve configurar seu ambiente AWS e então implantar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

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

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

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

A imagem a seguir mostra os componentes envolvidos nesta implantação:



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

Quando você cria o sistema Cloud Volumes ONTAP, o NetApp Console cria e anexa automaticamente uma função do IAM ao mediador. Esta função assume a função do IAM que você criou na conta do proprietário da VPC para fazer alterações nas tabelas de rotas associadas ao par HA.

Passos

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

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

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

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

["Consulte as regras do grupo de segurança para o Cloud Volumes ONTAP"](#) . Observe que você não precisa criar um grupo de segurança para o mediador HA. O Console faz isso por você.

3. Na conta do 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 para criar um novo sistema Cloud Volumes ONTAP .

Observe que você deve especificar os seguintes campos:

- "ID do Grupo de Segurança"

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

- "assumeRoleArn" no objeto "haParams"

O campo "assumeRoleArn" deve incluir o ARN da função do IAM que você criou na conta do proprietário da VPC (consulte 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"](#)

Configurar a criação de grupos de posicionamento para pares de alta disponibilidade do Cloud Volumes ONTAP em AZs únicas da AWS

As implantações de alta disponibilidade (HA) do Cloud Volumes ONTAP na Zona de disponibilidade única (AZ) da AWS podem falhar e ser revertidas se a criação do grupo de posicionamento falhar. A criação do grupo de posicionamento também falha e a implantação é revertida se o nó Cloud Volumes ONTAP e a instância do mediador não

estiverem disponíveis. Para evitar isso, você pode modificar a configuração para permitir que a implantação seja concluída mesmo se a criação do grupo de posicionamento falhar.

Ao ignorar o processo de reversão, o processo de implantação do Cloud Volumes ONTAP é concluído com sucesso e notifica você de que a criação do grupo de posicionamento está incompleta.

Passos

1. Use SSH para se conectar ao host do agente do NetApp Console e efetuar login.
2. Navegar para `/opt/application/netapp/cloudmanager/docker_occm/data`.
3. Editar `app.conf` alterando o valor do `rollback-on-placement-group-failure` parâmetro para `false`. O valor padrão deste parâmetro é `true`.

```
{
  "occm" : {
    "aws" : {
      "rollback-on-placement-group-failure" : false
    }
  }
}
```

4. Salve o arquivo e faça logoff do agente do Console. Não é necessário reiniciar o agente do Console.

Regras de entrada e saída do grupo de segurança da AWS para o Cloud Volumes ONTAP

O NetApp Console cria grupos de segurança da AWS que incluem as regras de entrada e saída que o Cloud Volumes ONTAP precisa para operar com sucesso. Talvez você queira 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 exige regras de entrada e saída.

Regras de entrada

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

- **Somente 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 agente do Console reside. Esta é a opção recomendada.
- **Todas as VPCs:** a origem do tráfego de entrada é o intervalo de IP 0.0.0.0/0.

Protocolo	Porta	Propósito
Todos os ICMP	Todos	Executando ping na instância
HTTP	80	Acesso HTTP ao console da web do ONTAP System Manager usando o endereço IP do LIF de gerenciamento do cluster
HTTPS	443	Conectividade com o agente do Console e acesso HTTPS ao console da Web do ONTAP System Manager usando o endereço IP do LIF de gerenciamento do cluster
SSH	22	Acesso SSH ao endereço IP do LIF de gerenciamento de cluster ou de 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 simples de gerenciamento de rede
TCP	445	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
TCP	635	Montagem NFS
TCP	749	Kerberos
TCP	2049	Daemon do servidor NFS
TCP	3260	Acesso iSCSI através do LIF de dados iSCSI
TCP	4045	Daemon de bloqueio NFS
TCP	4046	Monitor de status de rede para NFS
TCP	10000	Backup usando NDMP
TCP	11104	Gerenciamento de sessões de comunicação entre clusters para SnapMirror
TCP	11105	Transferência de dados do SnapMirror usando LIFs intercluster
UDP	111	Chamada de procedimento remoto para NFS
UDP	161-162	Protocolo simples de gerenciamento de rede
UDP	635	Montagem NFS
UDP	2049	Daemon do servidor NFS
UDP	4045	Daemon de bloqueio NFS
UDP	4046	Monitor de status de rede para NFS
UDP	4049	Protocolo NFS rquotad

Regras de saída

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

Regras básicas de saída

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

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

Regras avançadas de saída

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



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

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

Serviço	Protocolo	Porta	Fonte	Destino	Propósito
AutoSupport	HTTPS	443	Gerenciamento de nós LIF	meusuporte.netapp.com	AutoSupport (HTTPS é o padrão)
	HTTP	80	Gerenciamento de nós LIF	meusuporte.netapp.com	AutoSupport (somente se o protocolo de transporte for alterado de HTTPS para HTTP)
	TCP	3128	Gerenciamento de nós LIF	Agente de console	Envio de mensagens do AutoSupport por meio de um servidor proxy no agente do Console, se uma conexão de saída com a Internet não estiver disponível
Backup para S3	TCP	5010	LIF interaglomerado	Ponto de extremidade de backup ou ponto de extremidade de restauração	Operações de backup e restauração para o recurso Backup para S3
Conjunto	Todo o tráfego	Todo o tráfego	Todos os LIFs em um nó	Todos os LIFs no outro nó	Comunicações entre clusters (somente Cloud Volumes ONTAP HA)
	TCP	3000	Gerenciamento de nós LIF	Mediador HA	Chamadas ZAPI (somente Cloud Volumes ONTAP HA)
	ICMP	1	Gerenciamento de nós LIF	Mediador HA	Mantenha-se ativo (somente Cloud Volumes ONTAP HA)
Backups de configuração	HTTP	80	Gerenciamento de nós LIF	http://<endereço-IP-do-agente-do-console>/occm/offboxconfig	Envie backups de configuração para o agente do Console. "Documentação do ONTAP"
DHCP	UDP	68	Gerenciamento de nós LIF	DHCP	Cliente DHCP para configuração inicial
DHCPs	UDP	67	Gerenciamento de nós LIF	DHCP	Servidor DHCP
DNS	UDP	53	Gerenciamento de nós LIF e dados LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	1860–18699	Gerenciamento de nós LIF	Servidores de destino	Cópia do NDMP
SMTP	TCP	25	Gerenciamento de nós LIF	Servidor de e-mail	Alertas SMTP podem ser usados para AutoSupport

Serviço	Protocolo	Porta	Fonte	Destino	Propósito
SNMP	TCP	161	Gerenciamento de nós LIF	Servidor de monitoramento	Monitoramento por armadilhas SNMP
	UDP	161	Gerenciamento de nós LIF	Servidor de monitoramento	Monitoramento por armadilhas SNMP
	TCP	162	Gerenciamento de nós LIF	Servidor de monitoramento	Monitoramento por armadilhas SNMP
	UDP	162	Gerenciamento de nós LIF	Servidor de monitoramento	Monitoramento por armadilhas SNMP
SnapMirror	TCP	11104	LIF interaglomerado	LIFs interaglomerados ONTAP	Gerenciamento de sessões de comunicação entre clusters para SnapMirror
	TCP	11105	LIF interaglomerado	LIFs interaglomerados ONTAP	Transferência de dados do SnapMirror
Log de sistema	UDP	514	Gerenciamento de nós LIF	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 Cloud Volumes ONTAP HA inclui as seguintes regras de entrada e saída.

Regras de entrada

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

Protocolo	Porta	Fonte	Propósito
TCP	3000	CIDR do agente do console	Acesso à API RESTful a partir do agente do Console

Regras de saída

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

Regras básicas de saída

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

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

Regras avançadas de saída

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

Protocolo	Porta	Destino	Propósito
HTTP	80	Endereço IP do agente do console na instância do AWS EC2	Baixe atualizações para o mediador
HTTPS	443	ec2.amazonaws.com	Auxiliar no failover de armazenamento
UDP	53	ec2.amazonaws.com	Auxiliar no failover de armazenamento



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 do Cloud Volumes ONTAP HA inclui as seguintes regras. Este grupo de segurança permite a comunicação entre os nós HA e entre o mediador e os nós.

O Console 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	Propósito
Todo o tráfego	Todos	Comunicação entre o mediador HA e os nós HA

Regras de saída

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

Protocolo	Porta	Propósito
Todo o tráfego	Todos	Comunicação entre o mediador HA e os nós HA

Regras para o agente do Console

["Exibir regras de grupo de segurança para o agente do Console"](#)

Configurar o Cloud Volumes ONTAP para usar uma chave gerenciada pelo cliente na AWS

Se você quiser usar a criptografia da Amazon com o Cloud Volumes ONTAP, precisará configurar o AWS Key Management Service (KMS).

Passos

1. Certifique-se de que exista uma Chave Mestra do Cliente (CMK) ativa.

A CMK pode ser uma CMK gerenciada pela AWS ou uma CMK gerenciada pelo cliente. Ele pode estar na mesma conta da AWS que o NetApp Console e o Cloud Volumes ONTAP ou em uma conta da AWS diferente.

"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 Console como um *usuário de chave*.

Adicionar a função de Gerenciamento de Identidade e Acesso (IAM) como um usuário-chave concede ao Console permissões para usar a CMK com o Cloud Volumes ONTAP.

"Documentação da AWS: Editando Chaves"

3. Se a CMK estiver em uma conta diferente da AWS, conclua as seguintes etapas:

- a. Acesse o console do KMS a partir da conta onde o CMK reside.
- b. Selecione a chave.
- c. No painel **Configuração geral**, copie o ARN da chave.

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

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

Normalmente, esta é a conta onde o Console é implantado. Se o Console não estiver instalado na AWS, use a conta para a qual você forneceu as chaves de acesso da AWS ao Console.



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

Remove

Add another AWS account

Cancel

Save changes

- e. Agora mude para a conta da AWS que fornece permissões ao Console 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 Console.

A política a seguir fornece as permissões que o Console precisa para usar a CMK da conta externa da AWS. Não se esqueça 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 detalhes adicionais sobre este processo, consulte o ["Documentação da AWS: Permitindo que usuários em outras contas usem uma chave KMS"](#).

4. Se você estiver usando uma CMK gerenciada pelo cliente, modifique a política de chave para a CMK adicionando a função IAM do Cloud Volumes ONTAP como um *usuário de chave*.

Esta etapa é necessária se você habilitou a hierarquização de dados no Cloud Volumes ONTAP e deseja criptografar os dados armazenados no bucket do S3.

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

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

Configurar funções do AWS IAM para nós do Cloud Volumes ONTAP

As funções de gerenciamento de identidade e acesso (IAM) da AWS com as permissões necessárias devem ser anexadas a cada nó do Cloud Volumes ONTAP . O mesmo vale para o mediador HA. É mais fácil deixar que o NetApp Console crie as funções do IAM para você, mas você pode usar suas próprias funções.

Esta tarefa é opcional. Ao criar um sistema Cloud Volumes ONTAP , a opção padrão é deixar o Console criar as funções do IAM para você. Se as políticas de segurança da sua empresa exigirem que você mesmo crie as funções do IAM, siga as etapas abaixo.



É necessário fornecer sua própria função de IAM no AWS Secret Cloud. ["Aprenda a implantar o Cloud Volumes ONTAP no C2S"](#) .

Passos

1. Acesse o console do AWS IAM.
2. Crie políticas do IAM que incluam as seguintes permissões:
 - Política básica para nós 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"
  }]
}

```

Regiões ultrasecretas

```

{
  "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 Cloud Volumes ONTAP

Se você planeja usar o NetApp Backup and Recovery 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"
    }
  ]
}

```

Regiões ultrasecretas

```

{
  "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"
    }
  ]
}

```

- Mediador 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",
      "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 sistema Cloud Volumes ONTAP .

Mais informações

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

Configurar licenciamento para Cloud Volumes ONTAP na AWS

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

Freemium

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

Passos

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

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

Edit Credentials & Add Subscription

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

Select Charging Method

☐ Professional

By capacity

▼

☐ Essential

By capacity

▼

☒ Freemium (Up to 500 GiB)

By capacity

▼

☐ Per Node

By node

▼

"Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP 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)) adquirida da NetApp
- Uma assinatura por hora, paga conforme o uso (PAYGO) do AWS Marketplace
- Um contrato anual do AWS Marketplace

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

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

Traga sua própria bebida

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

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

Passos

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

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

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

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

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

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

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

Select Charging Method



Professional

By capacity



Essential

By capacity



Freemium (Up to 500 GiB)

By capacity



Per Node

By node



"Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP na AWS" .

Assinatura PAYGO

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

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

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas.
 - a. Na página **Detalhes e credenciais**, clique em **Editar credenciais > Adicionar assinatura** e siga as instruções para assinar a oferta de pagamento conforme o uso no 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. Após retornar ao Console, selecione um pacote baseado em capacidade quando chegar à página de métodos de cobrança.

Select Charging Method

☒ Professional

By capacity

▼

☐ Essential

By capacity

▼

☐ Freemium (Up to 500 GiB)

By capacity

▼

☐ Per Node

By node

▼

"Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP na AWS" .



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

Contrato anual

Pague anualmente comprando um contrato anual no marketplace do seu provedor de nuvem.

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

Passos

1. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas.
 - a. Na página **Detalhes e credenciais**, clique em **Editar credenciais > Adicionar assinatura** e siga as instruções para assinar 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. Após retornar ao Console, selecione um pacote baseado em capacidade quando chegar à página de métodos de cobrança.

Select Charging Method

☒ **Professional**

By capacity



☐ **Essential**

By capacity



☐ **Freemium (Up to 500 GiB)**

By capacity



☐ **Per Node**

By node



"Veja instruções passo a passo para iniciar o Cloud Volumes ONTAP na AWS" .

Assinatura Keystone

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

Passos

1. Se você ainda não tem uma assinatura, ["entre em contato com a NetApp"](#)
2. [Entre em contato com a NetApp](#) para autorizar sua conta de usuário com uma ou mais assinaturas Keystone .
3. Depois que a NetApp autorizar sua conta, ["vincule suas assinaturas para uso com o Cloud Volumes ONTAP"](#) .
4. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas.
 - a. Selecione o método de cobrança da Assinatura Keystone quando solicitado a escolher um método de cobrança.

Select Charging Method

☒ **Keystone** By capacity ^

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1 v

☐ **Professional** By capacity v

☐ **Essential** By capacity v

☐ **Freemium (Up to 500 GiB)** By capacity v

☐ **Per Node** By node v

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

Implante o Cloud Volumes ONTAP na AWS usando implantação rápida

Você pode implantar o Cloud Volumes ONTAP na AWS usando um método de implantação rápida para configurações de nó único e de alta disponibilidade (HA). Este processo simplificado reduz as etapas de implantação em comparação ao método avançado. Ele também oferece mais clareza no fluxo de trabalho, definindo

automaticamente valores padrão em uma única página e minimizando a navegação.

Antes de começar

Você precisa do seguinte para adicionar um sistema Cloud Volumes ONTAP na AWS a partir do NetApp Console.

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

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

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

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

- DNS e Active Directory para configurações CIFS.

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

Sobre esta tarefa

Imediatamente após a criação do sistema Cloud Volumes ONTAP , o NetApp Console inicia uma instância de teste na VPC especificada para verificar a conectividade. Se for bem-sucedido, o Console encerra imediatamente a instância e começa a implantar o sistema. Se o Console não puder verificar a conectividade, a criação do sistema falhará. A instância de teste é uma `t2.nano` (para locação VPC padrão) ou um `m3.medium` (para locação de VPC dedicada).

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página Canvas, clique em **Adicionar Sistema** e siga as instruções.
3. Selecione **Amazon Web Services > * Cloud Volumes ONTAP* > Adicionar novo**. A opção **Criação rápida** é selecionada por padrão.



Quick create
Use the recommended and default configuration options. You can change most of these options later.



Advanced create
You set all of the configuration options, including specifying performance, networking, security, backups, and maintenance.

System details

Show API request

Cloud provider account	Instance Profile Account ID: 2	▼
Name	ⓘ Action required	▼
ONTAP Credentials	ⓘ Action required	▼
Tags	0 Tags	▼

Deployment and Configuration

Deployment Type	Single node	▼
Network configuration	US East - N. Virginia VPC name - 172.31.0.0/16 Subnet name -	▼

Charging and Services

Marketplace subscription	Sub2-ByCapacityByNodePYGO_delete_after_1234	▼
License	Freemium (Up to 500 GiB)	▼
Data services and features	Netapp Backup and Recovery	▼
NetApp Support Site account	No existing account	▼

Summary

Overview	▼

Create

Cancel

detalhes do sistema

- Conta do provedor de nuvem:** Os detalhes da conta são preenchidos automaticamente com base no agente do Console selecionado. Se você tiver várias contas, selecione aquela que deseja usar. Se um agente do Console não estiver disponível, você será solicitado a ["criar um agente de console"](#).
- Nome:** O nome do sistema. O Console usa o nome do sistema (cluster) para nomear o sistema Cloud Volumes ONTAP e a instância do Amazon EC2. Ele também usa o nome como prefixo para o grupo de segurança predefinido, se você selecionar essa opção.
- * Credenciais ONTAP *** Estas são as credenciais para a conta de administrador do cluster Cloud Volumes ONTAP. Você pode usar essas credenciais para se conectar ao Cloud Volumes ONTAP por meio do ONTAP System Manager ou do ONTAP CLI. Você pode manter o nome de usuário padrão *admin* ou alterá-lo para um nome de usuário personalizado.
- Tags** As tags da AWS são metadados para seus recursos da AWS. O Console adiciona as tags à instância do Cloud Volumes ONTAP e a cada recurso da AWS associado à instância. Você pode adicionar

até 15 tags da interface do usuário ao criar um sistema Cloud Volumes ONTAP e, depois, adicionar mais depois que ele for criado. Observe que a API não limita você a quatro tags ao criar um sistema. Para obter informações sobre tags, consulte ["Documentação da AWS: Marcando seus recursos do Amazon EC2"](#) .

Implantação e configuração

1. **Tipo de implantação:** selecione o tipo de implantação que você deseja usar: nó único, alta disponibilidade (HA) em uma única zona de disponibilidade (AZ) ou HA em várias AZs.
2. **Configuração de rede:** Insira as informações de rede que você registrou no ["Planilha AWS"](#) .
 - a. **Região da AWS:** Por padrão, a região da conta de nuvem associada que tem VPC com recursos de sub-rede é selecionada.
 - b. **VPC:** insira uma VPC para a região da AWS com uma sub-rede. Se não houver sub-redes, o valor padrão para a VPC será selecionado.
 - c. **Sub-rede:** você pode selecionar uma sub-rede para a VPC somente para uma implantação de nó único ou implantação de HA em uma única AZ.

Alta disponibilidade

Se você selecionou a configuração HA, insira as seguintes informações:

HA em AZ único

1. **Acesso do mediador:** especifique as informações de acesso do mediador. O mediador é uma instância separada que monitora a integridade do par HA e fornece quorum em caso de falha. Forneça o nome do par de chaves para permitir que a instância do mediador se conecte ao serviço AWS EC2 e selecione o método de conexão.

HA em várias AZ

1. **Zonas de disponibilidade e mediador:** selecione as zonas de disponibilidade (AZs) para cada nó, o mediador e as sub-redes correspondentes onde você deseja implantar o par Cloud Volumes ONTAP HA.
2. **IPs flutuantes:** se você escolher várias AZs, especifique os endereços IP flutuantes para os serviços NFS e CIFS e para o gerenciamento de cluster e SVM. Os endereços IP devem estar fora do bloco CIDR para todas as VPCs na região. Para obter detalhes adicionais, consulte ["Requisitos de rede da AWS para Cloud Volumes ONTAP HA em várias AZs"](#) .
3. **Acesso do mediador:** especifique as informações de acesso do mediador. O mediador é uma instância separada que monitora a integridade do par HA e fornece quorum em caso de falha. Forneça o nome do par de chaves para permitir que a instância do mediador se conecte ao serviço AWS EC2 e selecione o método de conexão.
4. **Tabelas de rotas:** se você escolher várias zonas de disponibilidade, selecione as tabelas de rotas que incluem rotas para os endereços IP flutuantes. Se você tiver mais de uma tabela de rotas, é importante selecionar as tabelas de rotas corretas. Caso contrário, alguns clientes podem não ter acesso ao par Cloud Volumes ONTAP HA. Para obter mais informações sobre tabelas de rotas, consulte o ["Documentação da AWS: Tabelas de rotas"](#) .

Cobrança e Serviços

1. **Assinatura do Marketplace:** Selecione a assinatura do marketplace da AWS que você deseja usar com este sistema Cloud Volumes ONTAP .
2. **Licença:** Selecione o tipo de licença que deseja usar com este sistema Cloud Volumes ONTAP . Você pode escolher entre licenças Profissional, Essencial e Premium. Para obter informações sobre diferentes licenças, consulte ["Saiba mais sobre as licenças do Cloud Volumes ONTAP"](#) .

3. **Serviços e recursos de dados:** mantenha os serviços ativados ou desative os serviços que você não deseja usar com o Cloud Volumes ONTAP.

- ["Saiba mais sobre a classificação da NetApp"](#)
- ["Saiba mais sobre o NetApp Backup and Recovery"](#)
- ["Saiba mais sobre o armazenamento WORM no Cloud Volumes ONTAP"](#)



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

- * Conta do site de suporte da NetApp *: se você tiver várias contas, selecione aquela que deseja usar.

Resumo

Verifique ou edite os detalhes inseridos e clique em **Criar**.

Links relacionados

- ["Planejando sua configuração do Cloud Volumes ONTAP"](#)
- ["Implantar o Cloud Volumes ONTAP na AWS usando implantação avançada"](#)

Inicie o Cloud Volumes ONTAP no AWS

Você pode iniciar o Cloud Volumes ONTAP em uma configuração de sistema único ou como um par de HA na AWS. Este método fornece uma experiência de implantação avançada que oferece mais opções de configuração e flexibilidade do que o método de implantação rápida.

Antes de começar

Você precisa do seguinte antes de começar.

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

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

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

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

- DNS e Active Directory para configurações CIFS.

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

Inicie um sistema Cloud Volumes ONTAP de nó único na AWS

Se você quiser iniciar o Cloud Volumes ONTAP na AWS, precisará criar um novo sistema no NetApp Console.

Sobre esta tarefa

Imediatamente após a criação do sistema, o Console inicia uma instância de teste na VPC especificada para verificar a conectividade. Se for bem-sucedido, o Console encerra imediatamente a instância e começa a implantar o sistema Cloud Volumes ONTAP . Se a conectividade não puder ser verificada, a criação do sistema falhará. A instância de teste é uma `t2.nano` (para localização VPC padrão) ou `m3.medium` (para localização de VPC dedicada).

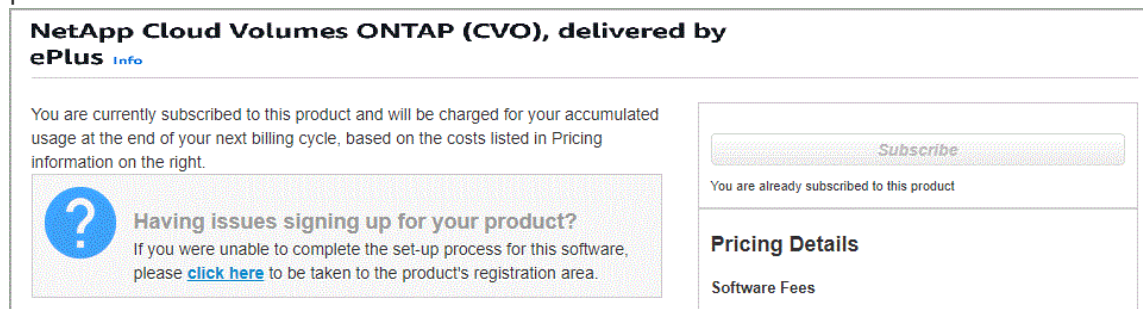
Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as instruções.
3. Selecione **Amazon Web Services** e * Cloud Volumes ONTAP Single Node*.
4. Selecione **Criação avançada**. Como o modo **Criação rápida** é selecionado por padrão, você pode ver uma mensagem para valores padrão. Clique em **Continuar**.
5. Se você for solicitado, "[criar um agente de console](#)".
6. **Detalhes e credenciais**: Opcionalmente, altere as credenciais e a assinatura da AWS, insira um nome de sistema, adicione tags, se necessário, e insira uma senha.

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

Campo	Descrição
Nome do sistema	O Console usa o nome do sistema para nomear o sistema Cloud Volumes ONTAP e a instância do Amazon EC2. Ele também usa o nome como prefixo para o grupo de segurança predefinido, se você selecionar essa opção.
Adicionar tags	As tags da AWS são metadados para seus recursos da AWS. O Console 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 sistema e depois adicionar mais depois que ele for criado. Observe que a API não limita você a quatro tags ao criar um sistema. Para obter informações sobre tags, consulte " Documentação da AWS: Marcando seus recursos do Amazon EC2 ".
Nome de usuário e senha	Estas são as credenciais para a conta de administrador do cluster Cloud Volumes ONTAP . Você pode usar essas credenciais para se conectar ao Cloud Volumes ONTAP por meio do ONTAP System Manager ou do ONTAP CLI. Mantenha o nome de usuário padrão <i>admin</i> ou altere-o para um nome de usuário personalizado.
Editar credenciais	Escolha as credenciais da AWS associadas à conta onde você deseja implantar este sistema. Você também pode associar a assinatura do marketplace da AWS para usar com este sistema Cloud Volumes ONTAP . Clique em Adicionar Assinatura para associar as credenciais selecionadas a uma nova assinatura do marketplace da AWS. A assinatura pode ser para um contrato anual ou para pagar o Cloud Volumes ONTAP por hora. " Aprenda como adicionar credenciais adicionais da AWS ao NetApp Console ".

Se vários usuários do IAM trabalharem na mesma conta da AWS, cada usuário precisará se inscrever. Depois que o primeiro usuário se inscreve, o marketplace da AWS informa os usuários subsequentes que eles já estão inscritos, conforme mostrado na imagem abaixo. Enquanto uma assinatura estiver em vigor para a *conta* da AWS, 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 do Console e concluir o processo.



7. **Serviços:** mantenha os serviços habilitados ou desabilite os serviços individuais que você não deseja usar com o Cloud Volumes ONTAP.

- ["Saiba mais sobre a classificação de dados da NetApp"](#)
- ["Saiba mais sobre o NetApp Backup and Recovery"](#)



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

8. **Localização e conectividade:** insira as informações de rede que você registrou no ["Planilha 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, poderá implantar um sistema Cloud Volumes ONTAP de nó único nesse Outpost selecionando a VPC do Outpost. A experiência é a mesma de qualquer outra VPC que reside na AWS.
Grupo de segurança gerado	Se você deixar o Console gerar o grupo de segurança para você, precisará escolher como permitirá o tráfego: • 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 agente do Console reside. Esta é a opção recomendada. • Se você escolher Todas as VPCs, a origem do tráfego de entrada será o intervalo de IP 0.0.0.0/0.
Usar grupo de segurança existente	Se você usar uma política de firewall existente, certifique-se de que ela inclua as regras necessárias. "Saiba mais sobre as regras de firewall para o Cloud Volumes ONTAP" .

9. **Criptografia de dados:** escolha nenhuma 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 .

["Aprenda a configurar o AWS KMS para Cloud Volumes ONTAP"](#) .

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

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

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

11. * Configuração do Cloud Volumes ONTAP * (somente contrato anual do marketplace da AWS): revise a configuração padrão e clique em **Continuar** ou clique em **Alterar configuração** para selecionar sua própria configuração.

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

12. **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, precisará apenas especificar um volume e depois revisar e aprovar a configuração.

13. **Função do IAM:** É melhor manter a opção padrão para deixar o Console criar a função para você.

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

14. **Licenciamento:** Altere a versão do Cloud Volumes ONTAP conforme necessário e selecione um tipo de instância e a localização da instância.



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

15. **Recursos de armazenamento subjacentes:** escolha um tipo de disco, configure o armazenamento subjacente e escolha se deseja manter a hierarquização 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 gp3 ou io1, o Console usará o recurso Elastic Volumes na AWS para aumentar automaticamente a capacidade do disco de armazenamento subjacente, conforme necessário. Você pode escolher a capacidade inicial com base em suas necessidades de armazenamento e revisá-la após a implantação do Cloud Volumes ONTAP . ["Saiba mais sobre o suporte para Elastic Volumes na AWS"](#) .

- Se você escolher um disco gp2 ou st1, poderá selecionar um tamanho de disco para todos os discos no agregado inicial e para quaisquer agregados adicionais que o Console criar quando você usar a opção de provisionamento simples. Você pode criar agregados que usam um tamanho de disco diferente usando a opção de alocação avançada.
- Você pode escolher uma política específica de níveis de volume ao criar ou editar um volume.
- Se você desabilitar a hierarquização de dados, poderá habilitá-la em agregações subsequentes.

["Aprenda como funciona a hierarquização de dados"](#) .

16. Velocidade de gravação e WORM:

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

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

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

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

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

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

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

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

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

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

Campo	Descrição
Opções avançadas (somente para NFS)	Selecione uma versão do NFS para o volume: NFSv3 ou NFSv4.
Grupo iniciador e IQN (somente para iSCSI)	Os destinos de armazenamento iSCSI são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Os grupos de iniciadores são tabelas de nomes de nós de host iSCSI e controlam quais iniciadores têm acesso a quais LUNs. Os destinos iSCSI se conectam à rede por meio de adaptadores de rede Ethernet padrão (NICs), placas de mecanismo de descarregamento TCP (TOE) com iniciadores de software, adaptadores de rede convergentes (CNAs) ou adaptadores de bust de host dedicados (HBAs) e são identificados por nomes qualificados iSCSI (IQNs). Quando você cria um volume iSCSI, o Console cria automaticamente um LUN para você. Simplificamos criando apenas um LUN por volume, portanto não há gerenciamento envolvido. Depois de criar o volume, "use o IQN para conectar-se ao LUN de seus hosts" .

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

The screenshot shows a form titled "Volume Details & Protection". It has five main input areas:

- Volume Name:** A text box containing "ABDcv5689" with an information icon (i) to its right.
- Storage VM (SVM):** A dropdown menu showing "svm_c...CVO1" with a downward arrow.
- Volume Size:** A text box containing "100".
- Unit:** A dropdown menu showing "GiB" with a downward arrow.
- Snapshot Policy:** A dropdown menu showing "default" with a downward arrow.

 Below the Snapshot Policy dropdown, there is a label "default policy" with an information icon (i).

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

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

Campo	Descrição
Unidade Organizacional	A unidade organizacional dentro do domínio do AD a ser associada ao servidor CIFS. O padrão é CN=Computadores. Se você configurar o AWS Managed Microsoft AD como o servidor AD para o Cloud Volumes ONTAP, deverá inserir OU=Computers,OU=corp neste campo.
Domínio DNS	O domínio DNS para a máquina virtual de armazenamento (SVM) do Cloud Volumes ONTAP . Na maioria dos casos, o domínio é o mesmo que o domínio do AD.
Servidor NTP	Selecione Usar domínio do Active Directory para configurar um servidor NTP usando o DNS do Active Directory. Se você precisar configurar um servidor NTP usando um endereço diferente, use a API. Consulte o "Documentação de automação do NetApp Console" para mais detalhes. Observe que você só pode configurar um servidor NTP ao criar um servidor CIFS. Não é configurável depois de criar o servidor CIFS.

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

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

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

Resultado

O Console inicia a instância do Cloud Volumes ONTAP . Você pode acompanhar o progresso na página **Auditoria**.

Se você tiver problemas para iniciar a instância do Cloud Volumes ONTAP , revise a mensagem de falha. Você também pode selecionar o sistema e clicar em **Recrutar ambiente**.

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

Depois que você terminar

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

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

Inicie um par de Cloud Volumes ONTAP HA na AWS

Se você quiser iniciar um par de HA do Cloud Volumes ONTAP na AWS, precisará criar um sistema de HA no

Console.

Limitação

No momento, os pares HA não são suportados pelo AWS Outposts.

Sobre esta tarefa

Imediatamente após a criação do sistema Cloud Volumes ONTAP , o Console inicia uma instância de teste na VPC especificada para verificar a conectividade. Se for bem-sucedido, o Console encerra imediatamente a instância e começa a implantar o sistema Cloud Volumes ONTAP . Se a conectividade não puder ser verificada, a criação do sistema falhará. A instância de teste é uma `t2.nano` (para locação VPC padrão) ou `m3.medium` (para locação de VPC dedicada).

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as instruções.
3. Selecione **Amazon Web Services** e * Cloud Volumes ONTAP HA*.

Algumas zonas locais da AWS estão disponíveis.

Antes de poder usar as Zonas Locais da AWS, você deve habilitar as Zonas Locais e criar uma sub-rede na Zona Local na sua conta da AWS. Siga as etapas **Optar por uma zona local da AWS** e **Estender sua Amazon VPC para a zona local** no "[Tutorial da AWS "Comece a implantar aplicativos de baixa latência com zonas locais da AWS"](#)".

Se você estiver executando o agente do Console 3.9.36 ou inferior, será necessário adicionar o `DescribeAvailabilityZones` permissão para a função AWS no console AWS EC2.

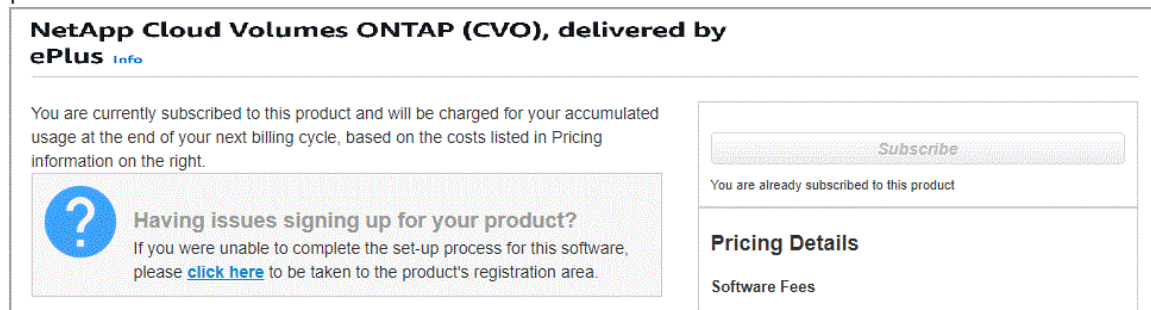
4. **Detalhes e credenciais:** Opcionalmente, altere as credenciais e a assinatura da AWS, insira um nome de sistema, adicione tags, se necessário, e insira uma senha.

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

Campo	Descrição
Nome do sistema	O Console usa o nome do sistema para nomear o sistema Cloud Volumes ONTAP e a instância do Amazon EC2. Ele também usa o nome como prefixo para o grupo de segurança predefinido, se você selecionar essa opção.
Adicionar tags	As tags da AWS são metadados para seus recursos da AWS. O Console 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 sistema e depois adicionar mais depois que ele for criado. Observe que a API não limita você a quatro tags ao criar um sistema. Para obter informações sobre tags, consulte " Documentação da AWS: Marcando seus recursos do Amazon EC2 ".
Nome de usuário e senha	Estas são as credenciais para a conta de administrador do cluster Cloud Volumes ONTAP . Você pode usar essas credenciais para se conectar ao Cloud Volumes ONTAP por meio do ONTAP System Manager ou do ONTAP CLI. Mantenha o nome de usuário padrão <i>admin</i> ou altere-o para um nome de usuário personalizado.

Campo	Descrição
Editar credenciais	Selecione as credenciais da AWS e a assinatura do marketplace para usar com este sistema Cloud Volumes ONTAP . Clique em Adicionar Assinatura para associar as credenciais selecionadas a uma nova assinatura do marketplace da AWS. A assinatura pode ser para um contrato anual ou para pagar o Cloud Volumes ONTAP por hora. Se você adquiriu uma licença diretamente da NetApp (traga sua própria licença (BYOL)), não é necessária uma assinatura da AWS. A NetApp restringiu a compra, extensão e renovação de licenças BYOL. Para obter mais informações, consulte " Disponibilidade restrita de licenciamento BYOL para Cloud Volumes ONTAP " . " Aprenda como adicionar credenciais adicionais da AWS ao Console " .

Se vários usuários do IAM trabalharem na mesma conta da AWS, cada usuário precisará se inscrever. Depois que o primeiro usuário se inscreve, o marketplace da AWS informa os usuários subsequentes que eles já estão inscritos, conforme mostrado na imagem abaixo. Enquanto uma assinatura estiver em vigor para a *conta* da AWS, 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 do Console e concluir o processo.



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 de dados da NetApp](#)"
- "[Saiba mais sobre backup e recuperação](#)"



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

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

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

7. **Localização e conectividade** (zona de disponibilidade única (AZ)) ou **Região e VPC** (várias AZs): insira as informações de rede que você registrou 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 deixar o Console gerar o grupo de segurança para você, precisará escolher como permitirá o tráfego: • 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 agente do Console reside. Esta é a opção recomendada. • Se você escolher Todas as VPCs, a origem do tráfego de entrada será o intervalo de IP 0.0.0.0/0.
Usar grupo de segurança existente	Se você usar uma política de firewall existente, certifique-se de que ela inclua as regras necessárias. "Saiba mais sobre as regras de firewall para o 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 várias AZs, especifique os endereços IP flutuantes.

Os endereços IP devem estar fora do bloco CIDR para todas as VPCs na região. Para obter detalhes adicionais, consulte ["Requisitos de rede da AWS para Cloud Volumes ONTAP HA em várias AZs"](#) .

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

Se você 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 Cloud Volumes ONTAP HA. Para obter mais informações sobre tabelas de rotas, consulte o ["Documentação da AWS: Tabelas de rotas"](#) .

11. **Criptografia de dados:** escolha nenhuma 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 .

["Aprenda a configurar o AWS KMS para Cloud Volumes ONTAP"](#) .

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

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

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

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

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

15. **Função do IAM:** É melhor manter a opção padrão para deixar o Console criar a função para você.

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

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



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

17. **Recursos de armazenamento subjacentes:** escolha um tipo de disco, configure o armazenamento subjacente e escolha se deseja manter a hierarquização 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 gp3 ou io1, o Console usará o recurso Elastic Volumes na AWS para aumentar automaticamente a capacidade do disco de armazenamento subjacente, conforme necessário. Você pode escolher a capacidade inicial com base em suas necessidades de armazenamento e revisá-la após a implantação do Cloud Volumes ONTAP. "[Saiba mais sobre o suporte para Elastic Volumes na AWS](#)".
- Se você escolher um disco gp2 ou st1, poderá selecionar um tamanho de disco para todos os discos no agregado inicial e para quaisquer agregados adicionais que o Console criar quando você usar a opção de provisionamento simples. Você pode criar agregados que usam um tamanho de disco diferente usando a opção de alocação avançada.
- Você pode escolher uma política específica de níveis de volume ao criar ou editar um volume.
- Se você desabilitar a hierarquização de dados, poderá habilitá-la em agregações subsequentes.

["Aprenda como funciona a hierarquização de dados"](#).

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

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

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

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

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

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

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

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

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

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

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

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

Volume Details & Protection

Volume Name i

ABDcv5689

Volume Size i

100

Storage VM (SVM)

svm_...CVO1 ▼

Unit

GiB ▼

Snapshot Policy

default ▼

default policy i

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 ao qual o servidor CIFS se juntará.
Domínio do Active Directory para ingressar	O FQDN do domínio do Active Directory (AD) ao qual você deseja que o servidor CIFS ingresse.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com privilégios suficientes para adicionar computadores à Unidade Organizacional (UO) especificada dentro do domínio do AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio do AD.
Unidade Organizacional	A unidade organizacional dentro do domínio do AD a ser associada ao servidor CIFS. O padrão é CN=Computadores. Se você configurar o AWS Managed Microsoft AD como o servidor AD para o Cloud Volumes ONTAP, deverá inserir OU=Computers,OU=corp neste campo.
Domínio DNS	O domínio DNS para a máquina virtual de armazenamento (SVM) do Cloud Volumes ONTAP . Na maioria dos casos, o domínio é o mesmo que o domínio do AD.
Servidor NTP	Selecione Usar domínio do Active Directory para configurar um servidor NTP usando o DNS do Active Directory. Se você precisar configurar um servidor NTP usando um endereço diferente, use a API. Consulte o "Documentação de automação do NetApp Console" para mais detalhes. Observe que você só pode configurar um servidor NTP ao criar um servidor CIFS. Não é configurável depois de criar o servidor CIFS.

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

Para mais informações, consulte ["Escolha um perfil de uso de volume"](#) e ["Visão geral da hierarquização de dados"](#) .

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

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

Resultado

O Console inicia o par Cloud Volumes ONTAP HA. Você pode acompanhar o progresso na página **Auditoria**.

Se você tiver algum problema ao iniciar o par HA, revise a mensagem de falha. Você também pode selecionar o sistema e clicar em Recriar ambiente.

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

Depois que você terminar

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

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

Links relacionados

- "[Planejando sua configuração do Cloud Volumes ONTAP](#)"
- "[Implante o Cloud Volumes ONTAP na AWS usando implantação rápida](#)"

Implantar o Cloud Volumes ONTAP no AWS Secret Cloud ou no AWS Top Secret Cloud

Semelhante a uma região padrão da AWS, você pode usar o NetApp Console em "[Nuvem secreta da AWS](#)" e em "[Nuvem ultrassecreta da AWS](#)" para implantar o Cloud Volumes ONTAP, que fornece recursos de nível empresarial para seu armazenamento em nuvem. AWS Secret Cloud e Top Secret Cloud são regiões fechadas específicas para a Comunidade de Inteligência dos EUA; as instruções nesta página se aplicam somente aos usuários das regiões AWS Secret Cloud e Top Secret Cloud.

Antes de começar

Antes de começar, revise as versões compatíveis no AWS Secret Cloud e no Top Secret Cloud e saiba mais sobre o modo privado no Console.

- Revise as seguintes versões suportadas no AWS Secret Cloud e Top Secret Cloud:
 - Cloud Volumes ONTAP 9.12.1 P2
 - Versão 3.9.32 do agente do Console

O agente do Console é necessário para implantar e gerenciar o Cloud Volumes ONTAP na AWS. Você fará login no Console a partir do software instalado na instância do agente do Console. O site SaaS do Console não é compatível com o AWS Secret Cloud e o Top Secret Cloud.

- Saiba mais sobre o modo privado

No AWS Secret Cloud e Top Secret Cloud, o Console opera no *modo privado*. No modo privado, não há conectividade com a camada SaaS do Console. Você pode acessar o Console por meio de um aplicativo local baseado na Web que pode acessar o agente do Console.

Para saber mais sobre como funciona o modo privado, consulte "[o modo de implantação privada no Console](#)".

Etapa 1: configure sua rede

Configure sua rede AWS para que o Cloud Volumes ONTAP possa operar corretamente.

Passos

1. Escolha a VPC e as sub-redes nas quais você deseja iniciar a instância do agente do Console e as instâncias do Cloud Volumes ONTAP .
2. Certifique-se de que sua VPC e sub-redes oferecerão suporte à conectividade entre o agente do Console e o Cloud Volumes ONTAP.
3. Configure um endpoint VPC para o serviço S3.

Um endpoint VPC é necessário se você quiser hierarquizar dados frios do Cloud Volumes ONTAP para armazenamento de objetos de baixo custo.

Etapa 2: Configurar permissões

Configure políticas e funções do IAM que forneçam ao agente do Console e ao Cloud Volumes ONTAP as permissões necessárias para executar ações no AWS Secret Cloud ou Top Secret Cloud.

Você precisa de uma política do IAM e uma função do IAM para cada um dos seguintes:

- A instância do agente do Console
- Instâncias Cloud Volumes ONTAP
- Para pares de HA, a instância do mediador de HA do Cloud Volumes ONTAP (se você quiser implantar pares de HA)

Passos

1. Acesse o console do AWS IAM e clique em **Políticas**.
2. Crie uma política para a instância do agente do Console.



Crie essas políticas para dar suporte aos buckets do S3 no seu ambiente AWS. Ao criar os buckets posteriormente, certifique-se de que os nomes dos buckets sejam prefixados com `fabric-pool-` . Este requisito se aplica às regiões AWS Secret Cloud e Top Secret Cloud.

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/*"
    ]
}
]
}

```

Regiões ultrasecretas

```

{
    "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"
  }]
}
```

Regiões ultrasecretas


```

{
  "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 que você criou nas etapas anteriores.

Crie a função:

Semelhante às políticas, você deve ter uma função do IAM para o agente do Console e uma para os nós do Cloud Volumes ONTAP . Para pares de HA: semelhante às políticas, você deve ter uma função do IAM para o agente do Console, uma para os nós do Cloud Volumes ONTAP e uma para o mediador de HA (se quiser implantar pares de HA).

Selecione a função:

Você deve selecionar a função IAM do agente do Console ao iniciar a instância do agente do Console. Você pode selecionar as funções do IAM para o Cloud Volumes ONTAP ao criar um sistema Cloud Volumes ONTAP no Console. Para pares de HA, você pode selecionar as funções do IAM para o Cloud Volumes ONTAP e o mediador de HA ao criar um sistema Cloud Volumes ONTAP .

Etapa 3: configurar o AWS KMS

Se você quiser usar a criptografia da Amazon com o Cloud Volumes ONTAP, certifique-se de que os requisitos sejam atendidos para o AWS Key Management Service (KMS).

Passos

1. Certifique-se de que exista uma Chave Mestra do Cliente (CMK) ativa na sua conta ou em outra conta da AWS.

A CMK pode ser uma CMK gerenciada pela AWS ou uma CMK gerenciada pelo cliente.

2. Se a CMK estiver em uma conta da AWS separada da conta onde você planeja implantar o Cloud Volumes ONTAP, será necessário obter o ARN dessa chave.

Você precisa fornecer o ARN ao Console ao criar o sistema Cloud Volumes ONTAP .

3. Adicione a função do IAM da instância à lista de usuários principais de uma CMK.

Isso dá ao Console permissões para usar o CMK com o Cloud Volumes ONTAP.

Etapa 4: instalar o agente do Console e configurar o Console

Antes de começar a usar o Console para implantar o Cloud Volumes ONTAP na AWS, você deve instalar e configurar o agente do Console. Ele permite que o Console gerencie recursos e processos dentro do 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 em Privacy Enhanced Mail (PEM) Base-64. Consulte as políticas e procedimentos da sua organização para obter o certificado.



Para regiões do AWS Secret Cloud, você deve fazer upload do `NSS Root CA 2` certificado e para Top Secret Cloud, o `Amazon Root CA 4` certificado. Certifique-se de carregar apenas esses certificados e não a cadeia inteira. O arquivo da cadeia de certificados é grande e o upload pode falhar. Se você tiver certificados adicionais, poderá enviá-los mais tarde, conforme descrito na próxima etapa.

Você precisa carregar o certificado durante o processo de configuração. O Console usa o certificado confiável ao enviar solicitações para a AWS via HTTPS.

2. Inicie a instância do agente do Console:
 - a. Acesse a página do AWS Intelligence Community Marketplace para o Console.
 - b. Na guia Inicialização personalizada, escolha a opção para iniciar a instância no console do 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 criou ao configurar as permissões.
- Você deve manter as opções de armazenamento padrão.
- Os métodos de conexão necessários para o agente do Console são os seguintes: SSH, HTTP e HTTPS.

3. Configure o Console a partir de um host que tenha uma conexão com a instância:
 - a. Abra um navegador da web e digite `<a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>` onde `<em>ipaddress</em>` é o endereço IP do host Linux onde você instalou o agente do Console.
 - b. Especifique um servidor proxy para conectividade com serviços da AWS.
 - c. Carregue o certificado que você obteve na etapa 1.
 - d. Siga as instruções para configurar um novo sistema.
 - **Detalhes do sistema:** insira um nome para o agente do Console e o nome da sua empresa.
 - **Criar usuário administrador:** Crie o usuário administrador do sistema.

Esta conta de usuário é executada localmente no sistema. Não há conexão com o serviço auth0

disponível através do Console.

- **Revisar**: 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 agente do Console no console do EC2.

4. Após a reinicialização do agente do Console, efetue login usando a conta de usuário administrador que você criou no assistente de configuração.

Etapa 5: (opcional) Instalar um certificado de modo privado

Esta etapa é opcional para as regiões AWS Secret Cloud e Top Secret Cloud e é necessária somente se você tiver certificados adicionais além dos certificados raiz que instalou na etapa anterior.

Passos

1. Listar certificados instalados existentes.

- a. Para coletar o ID do docker do contêiner occm (nome identificado “ds-occm-1”), execute o seguinte comando:

```
docker ps
```

- b. Para entrar no contêiner 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. Adicionar um certificado.

- a. Para coletar o ID do docker do contêiner occm (nome identificado “ds-occm-1”), execute o seguinte comando:

```
docker ps
```

- b. Para entrar no contêiner 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 truststore, 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 contêiner occm, execute o seguinte comando:

```
exit
```

- g. Para redefinir o contêiner occm, execute o seguinte comando:

```
docker restart <docker-id>
```

Etapa 6: Adicionar uma licença ao Console

Se você comprou uma licença da NetApp, precisará adicioná-la ao Console para poder selecionar a licença ao criar um novo sistema Cloud Volumes ONTAP . Essas licenças permanecem não atribuídas até que você as associe a um novo sistema Cloud Volumes ONTAP .

Passos

1. No menu de navegação à esquerda, selecione **Licenças e assinaturas**.
2. No painel * Cloud Volumes ONTAP*, selecione **Exibir**.
3. Na guia * Cloud Volumes ONTAP*, selecione **Licenças > Licenças baseadas em nós**.
4. Clique em **Não atribuído**.
5. Clique em **Adicionar licenças não atribuídas**.
6. Digite o número de série da licença ou carregue o arquivo de licença.

7. Se você ainda não tiver o arquivo de licença, precisará carregá-lo manualmente em netapp.com.
 - a. Vá para o "[Gerador de arquivo de licença NetApp](#)" e faça login usando suas credenciais do site de suporte da NetApp .
 - b. Digite sua senha, escolha seu produto, insira o número de série, confirme que você leu e aceitou a política de privacidade e clique em **Enviar**.
 - c. Escolha se deseja receber o arquivo JSON `serialnumber.NLF` por e-mail ou download direto.
8. Clique em **Adicionar licença**.

Resultado

O Console adiciona a licença como não atribuída até que você a associe a um novo sistema Cloud Volumes ONTAP . Você pode ver a licença no menu de navegação à esquerda em **Licenças e assinaturas > Cloud Volumes ONTAP > Exibir > Licenças**.

Etapa 7: Inicie o Cloud Volumes ONTAP no console

Você pode iniciar instâncias do Cloud Volumes ONTAP no AWS Secret Cloud e Top Secret Cloud criando novos sistemas no Console.

Antes de começar

Para pares HA, um par de chaves é necessário para habilitar a autenticação SSH baseada em chave para o mediador HA.

Passos

1. Na página **Sistemas**, clique em **Adicionar Sistema**.
2. Em **Criar**, selecione Cloud Volumes ONTAP.

Para HA: em **Criar**, selecione Cloud Volumes ONTAP ou Cloud Volumes ONTAP HA.

3. Conclua as etapas do assistente para iniciar o sistema Cloud Volumes ONTAP .



Ao fazer seleções por meio do assistente, não selecione **Data Sense & Compliance** e **Backup to Cloud** em **Serviços**. Em **Pacotes pré-configurados**, selecione apenas **Alterar configuração** e certifique-se de não ter selecionado nenhuma outra opção. Pacotes pré-configurados não são suportados nas regiões AWS Secret Cloud e Top Secret Cloud e, se selecionados, sua implantação falhará.

Observações para implantação do Cloud Volumes ONTAP HA em várias zonas de disponibilidade

Observe o seguinte ao concluir o assistente para pares HA.

- Você deve configurar um gateway de trânsito ao implantar o Cloud Volumes ONTAP HA em várias Zonas de Disponibilidade (AZs). Para obter instruções, consulte "[Configurar um gateway de trânsito da AWS](#)" .
- Implante a configuração da seguinte forma porque apenas duas AZs estavam disponíveis no AWS Top Secret Cloud no momento da publicação:
 - Nó 1: Zona de disponibilidade A
 - Nó 2: Zona de disponibilidade B
 - Mediador: Zona de disponibilidade A ou B

Observações para implantação do Cloud Volumes ONTAP em nós únicos e de alta disponibilidade

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 sucesso. Se você precisar usar o seu próprio, consulte a seção de grupo de segurança abaixo.

- Você deve escolher a função do IAM que criou ao preparar seu ambiente da AWS.
- O tipo de disco AWS subjacente 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 do disco que lhe dará o desempenho sustentado que você 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 precisar de um tamanho diferente posteriormente, você pode usar a opção Alocação avançada para criar um agregado que use discos de um tamanho específico.

Resultado

A instância do Cloud Volumes ONTAP é iniciada. Você pode acompanhar o progresso na página **Auditoria**.

Etapa 8: instalar certificados de segurança para camadas de dados

Você precisa instalar manualmente os certificados de segurança para habilitar a hierarquização de dados nas regiões AWS Secret Cloud e Top Secret Cloud.

Antes de começar

1. Crie buckets S3.



Certifique-se de que os nomes dos buckets sejam prefixados com `fabric-pool-`. Por exemplo `fabric-pool-testbucket`.

2. Mantenha os certificados raiz que você instalou em `step 4` útil.

Passos

1. Copie o texto dos certificados raiz que você instalou em `step 4`.
2. Conecte-se com segurança ao sistema Cloud Volumes ONTAP usando a CLI.
3. Instale os certificados raiz. Pode ser necessário pressionar o `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. Guarde 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 AWS Secret Cloud e Top Secret Cloud: `set -privilege advanced -confirmations off`
8. Execute este comando para configurar o armazenamento de objetos.



Todos os nomes de recursos da Amazon (ARNs) devem ser sufixados com `-iso-b`, como `arn:aws-iso-b`. Por exemplo, se um recurso requer um ARN com uma região, para Top Secret Cloud, use a convenção de nomenclatura como `us-iso-b` para o `-server` bandeira. Para AWS Secret Cloud, use `us-iso-b-1`.

```
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 no Microsoft Azure

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

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

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

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

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

	Mercado do Azure	Console NetApp
Integração	Mais curto e fácil, com preparação mínima necessária para implantação direta	Processo de integração mais longo, incluindo a instalação do agente do Console
Tipos de máquinas virtuais (VM) suportados	Tipos de instância Eds_v5 e Ls_v3	Gama completa de tipos de VM. https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-azure.html ["Configurações com suporte no Azure"^]
Licença	Licença gratuita	Qualquer licença baseada em capacidade. "Licenciamento do Cloud Volumes ONTAP"
* Suporte NetApp *	Não incluído	Disponível, com base no tipo de licença
Capacidade	Até 500 GiB	Expansível por configuração
Modelo de implantação	Implantação do modo de alta disponibilidade (HA) em zona de disponibilidade única (AZ)	Todas as configurações suportadas, incluindo modos de nó único e HA, implantações de AZ únicas e múltiplas
Tipo de disco suportado	Discos gerenciados SSD v2 premium	Suporte mais amplo. "Configuração padrão para Cloud Volumes ONTAP"
Velocidade de gravação (modo de gravação rápida)	Não suportado	Suportado, com base na sua configuração. "Saiba mais sobre velocidades de gravação no Cloud Volumes ONTAP" .
Capacidade de orquestração	Não disponível	Disponível por meio do NetApp Console, com base no tipo de licença
Número de VMs de armazenamento suportadas	Um por implantação	Várias VMs de armazenamento, com base na sua configuração. "Número suportado de VMs de armazenamento"
Alterando o tipo de instância	Não suportado	Suportado
* Hierarquização do FabricPool *	Não suportado	Suportado

Links relacionados

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

Introdução ao NetApp Console

Início rápido para Cloud Volumes ONTAP no Azure

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

1

Criar um agente de console

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

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

2

Planeje sua configuração

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

3

Configure sua rede

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

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

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

4

Inicie o Cloud Volumes ONTAP

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

Links relacionados

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

Planeje sua configuração do Cloud Volumes ONTAP no Azure

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

opções disponíveis.

Escolha uma licença do Cloud Volumes ONTAP

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

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

Escolha uma região com suporte

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

Escolha um tipo de VM compatível

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

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

Entenda os limites de armazenamento

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

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

Dimensione seu sistema no Azure

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

Tipo de máquina virtual

Veja os tipos de máquinas virtuais suportados no ["Notas de versão do Cloud Volumes ONTAP"](#) e depois 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 máquinas virtuais otimizados para memória"](#)

Tipo de disco do Azure com sistemas de nó único

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

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

- *Discos SSD gerenciados premium* oferecem alto desempenho para cargas de trabalho com uso intensivo de E/S a um custo mais alto.
- *Discos gerenciados SSD v2 Premium* oferecem maior desempenho com menor latência e menor custo, em comparação aos discos gerenciados SSD Premium.

- *Discos gerenciados SSD padrão* fornecem desempenho consistente para cargas de trabalho que exigem IOPS baixo.
- *Discos gerenciados de HDD padrão* são uma boa escolha se você não precisa de IOPS alto e quer reduzir seus custos.

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

Tipo de disco do Azure com pares de alta disponibilidade

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

Tamanho do disco do Azure

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



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

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

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

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

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

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

Exibir discos de sistema padrão

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

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



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

Coletar informações de rede

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

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

Escolha uma velocidade de gravação

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

Escolha um perfil de uso de volume

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

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

Provisionamento fino

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

Desduplicação

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

Compressão

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

Configurar a rede do Azure para o Cloud Volumes ONTAP

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

Requisitos para o Cloud Volumes ONTAP

Os seguintes requisitos de rede devem ser atendidos no Azure.

Acesso de saída à Internet

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

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

Pontos de extremidade Cloud Volumes ONTAP

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

Pontos finais	Aplicável para	Propósito	Modos de implantação	Impacto se indisponível
\ https://netapp-cloud-account.auth0.com	Autenticação	Usado para autenticação no Console.	Modos padrão e restrito.	A autenticação do usuário falha e os seguintes serviços permanecem indisponíveis: • Serviços Cloud Volumes ONTAP • Serviços ONTAP • Protocolos e serviços de proxy
https://vault.azure.net	Cofre de Chaves	Usado para recuperar chaves secretas do cliente do Azure Key Vault ao usar chaves gerenciadas pelo cliente (CMK).	Modos padrão, restrito e privado.	Os serviços do Cloud Volumes ONTAP não estão disponíveis.
\ https://api.bluexp.net/app.com/tenancy	Arrendamento	Usado para recuperar os recursos Cloud Volumes ONTAP do Console para autorizar recursos e usuários.	Modos padrão e restrito.	Os recursos do Cloud Volumes ONTAP e os usuários não estão autorizados.

Pontos finais	Aplicável para	Propósito	Modos de implantação	Impacto se indisponível
\ https://mysupport.net/app.com/aods/asupmessage \ https://mysupport.net/app.com/asupprod/post/1.0/postAsup	AutoSupport	Usado para enviar dados de telemetria do AutoSupport para o suporte da NetApp.	Modos padrão e restrito.	As informações do AutoSupport continuam não entregues.
\ https://management.azure.com \ https://login.microsoftonline.com \ https://bluexpinfraproduct.eastus2.data.azurecr.io \ https://core.windows.net	Regiões públicas	Comunicação com serviços do Azure.	Modos padrão, restrito e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço do Azure para executar operações específicas para o Console no Azure.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Região da China	Comunicação com serviços do Azure.	Modos padrão, restrito e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço do Azure para executar operações específicas para o Console no Azure.
\ https://management.microsoftazure.de \ https://login.microsoftonline.de \ https://blob.core.cloudapi.de \ https://core.cloudapi.de	Região da Alemanha	Comunicação com serviços do Azure.	Modos padrão, restrito e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço do Azure para executar operações específicas para o Console no Azure.
\ https://management.usgovcloudapi.net \ https://login.microsoftonline.us \ https://blob.core.usgovcloudapi.net \ https://core.usgovcloudapi.net	Regiões governamentais	Comunicação com serviços do Azure.	Modos padrão, restrito e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço do Azure para executar operações específicas para o Console no Azure.

Pontos finais	Aplicável para	Propósito	Modos de implantação	Impacto se indisponível
\https://management.azure.microsoft.scloud \ https://login.microsoftonline.microsoft.scloud \ https://blob.core.microsoft.scloud \ https://core.microsoft.scloud	Regiões do DoD do governo	Comunicação com serviços do Azure.	Modos padrão, restrito e privado.	O Cloud Volumes ONTAP não pode se comunicar com o serviço do Azure para executar operações específicas para o Console no Azure.

Configuração de proxy de rede do agente do NetApp Console

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

- **Proxy explícito:** O tráfego de saída do Cloud Volumes ONTAP usa o endereço HTTP do servidor proxy especificado durante a configuração de proxy do agente do Console. O administrador também pode ter configurado credenciais de usuário e certificados de CA raiz para autenticação adicional. Se um certificado de CA raiz estiver disponível para o proxy explícito, certifique-se de obter e carregar o mesmo certificado para o seu sistema Cloud Volumes ONTAP usando o ["ONTAP CLI: instalação do certificado de segurança"](#) comando.
- **Proxy transparente:** A rede está configurada para rotear automaticamente o tráfego de saída do Cloud Volumes ONTAP por meio do proxy para o agente do Console. Ao configurar um proxy transparente, o administrador precisa fornecer apenas um certificado de CA raiz para conectividade do Cloud Volumes ONTAP, não o endereço HTTP do servidor proxy. Certifique-se de obter e carregar o mesmo certificado de CA raiz para o seu sistema Cloud Volumes ONTAP usando o ["ONTAP CLI: instalação do certificado de segurança"](#) comando.

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

Endereços IP

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

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



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

Endereços IP para um sistema de nó único

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

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



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

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

Endereços IP para pares HA

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

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

NIC0

- IP de gerenciamento de nó
- IP intercluster
- IP iSCSI



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

NIC1

- IP de rede de cluster

NIC2

- IP de interconexão de cluster (HA IC)

NIC3

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



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

Os endereços IP acima não migram em eventos de failover.

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

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

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

Conexões seguras com serviços do Azure

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

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

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

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

Conexões com outros sistemas ONTAP

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

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

Porta para a interconexão HA

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

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

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

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

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

Regras do grupo de segurança

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

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

Não recomendamos modificar os grupos de segurança predefinidos ou usar grupos de segurança

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

Regras de entrada para sistemas de nó único

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

- **Somente VNet selecionada:** A origem do tráfego de entrada é o intervalo de sub-redes da VNet para o sistema Cloud Volumes ONTAP e o intervalo de sub-redes da VNet onde o agente do Console reside. Esta é a opção recomendada.
- **Todas as VNets:** A origem do tráfego de entrada é o intervalo de IP 0.0.0.0/0.
- **Desativado:** esta opção restringe o acesso da rede pública à sua conta de armazenamento e desabilita a hierarquização de dados para sistemas Cloud Volumes ONTAP . Esta é uma opção recomendada se seus endereços IP privados não devem ser expostos, mesmo dentro da mesma VNet, devido a regulamentações e políticas de segurança.

Prioridade e nome	Porta e protocolo	Origem e destino	Descrição
1000 entrada_ssh	22 TCP	Qualquer para Qualquer	Acesso SSH ao endereço IP do LIF de gerenciamento de cluster ou de um LIF de gerenciamento de nó
1001 entrada_http	80 TCP	Qualquer para Qualquer	Acesso HTTP ao console da web do ONTAP System Manager usando o endereço IP do LIF de gerenciamento do cluster
1002 entrada_111_tcp	111 TCP	Qualquer para Qualquer	Chamada de procedimento remoto para NFS
1003 entrada_111_udp	111 UDP	Qualquer para Qualquer	Chamada de procedimento remoto para NFS
1004 entrada_139	139 TCP	Qualquer para Qualquer	Sessão de serviço NetBIOS para CIFS
1005 entrada_161-162_tcp	161-162 TCP	Qualquer para Qualquer	Protocolo simples de gerenciamento de rede
1006 entrada_161-162_udp	161-162 UDP	Qualquer para Qualquer	Protocolo simples de gerenciamento de rede

Prioridade e nome	Porta e protocolo	Origem e destino	Descrição
1007 entrada_443	443 TCP	Qualquer para Qualquer	Conectividade com o agente do Console e acesso HTTPS ao console da Web do ONTAP System Manager usando o endereço IP do LIF de gerenciamento do cluster
1008 entrada_445	445 TCP	Qualquer para Qualquer	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
1009 entrada_635_tcp	635 TCP	Qualquer para Qualquer	Montagem NFS
1010 entrada_635_udp	635 UDP	Qualquer para Qualquer	Montagem NFS
1011 entrada_749	749 TCP	Qualquer para Qualquer	Kerberos
1012 entrada_2049_tcp	2049 TCP	Qualquer para Qualquer	Daemon do servidor NFS
1013 entrada_2049_udp	2049 UDP	Qualquer para Qualquer	Daemon do servidor NFS
1014 entrada_3260	3260 TCP	Qualquer para Qualquer	Acesso iSCSI através do LIF de dados iSCSI
1015 entrada_4045-4046_tcp	4045-4046 TCP	Qualquer para Qualquer	Daemon de bloqueio NFS e monitor de status de rede
1016 entrada_4045-4046_udp	4045-4046 UDP	Qualquer para Qualquer	Daemon de bloqueio NFS e monitor de status de rede
1017 entrada_10000	10000 TCP	Qualquer para Qualquer	Backup usando NDMP
1018 entrada_11104-11105	11104-11105 TCP	Qualquer para Qualquer	Transferência de dados do SnapMirror
3000 negação de entrada_todos_tcp	Qualquer porta TCP	Qualquer para Qualquer	Bloquear todo o outro tráfego de entrada TCP
3001 negação de entrada_todos_udp	Qualquer porta UDP	Qualquer para Qualquer	Bloquear todo o outro tráfego de entrada UDP
65000 Permitir entrada de Vnet	Qualquer porta Qualquer protocolo	Rede Virtual para Rede Virtual	Tráfego de entrada de dentro da VNet
65001 Permitir entrada do balanceador de carga do Azure	Qualquer porta Qualquer protocolo	AzureLoadBalancer para qualquer	Tráfego de dados do Azure Standard Load Balancer
65500 NegarAllInBound	Qualquer porta Qualquer protocolo	Qualquer para Qualquer	Bloqueie todo o outro tráfego de entrada

Regras de entrada para sistemas HA

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

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



Os sistemas HA têm menos regras de entrada do que os sistemas de nó único porque o tráfego de dados de entrada passa pelo Balanceador de Carga Padrão do Azure. Por isso, o tráfego do Load Balancer deve estar aberto, conforme mostrado na regra "AllowAzureLoadBalancerInBound".

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

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

Regras de saída

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

Regras básicas de saída

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

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

Regras avançadas de saída

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



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

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

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

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

Requisitos para o agente do console

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

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

Tópicos relacionados

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

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

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

Visão geral da criptografia de dados

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

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

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

Como os dados são criptografados

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

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

Configuração do Cloud Volumes ONTAP	Discos do sistema usados para criptografia de chaves	Discos de dados usados para criptografia de chaves
Nó único	• Bota • Essencial • NVRAM	• Raiz • Dados
Zona de disponibilidade única do Azure HA com blobs de página	• Bota • Essencial • NVRAM	Nenhum
Zona de disponibilidade única do Azure HA com discos gerenciados compartilhados	• Bota • Essencial • NVRAM	• Raiz • Dados
Várias zonas de disponibilidade do Azure HA com discos gerenciados compartilhados	• Bota • Essencial • NVRAM	• Raiz • Dados

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

Rotação de chaves no Cloud Volumes ONTAP

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

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

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



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

Crie uma identidade gerenciada atribuída pelo usuário

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

O recurso tem o seguinte ID: `userassignedidentity` .

Passos

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

Crie um cofre de chaves e gere uma chave

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

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

Passos

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

Observe os seguintes requisitos para o cofre de chaves:

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



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

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

a. Selecione as seguintes permissões:

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

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

c. Revise e crie a política de acesso.

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

Observe os seguintes requisitos para a chave:

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

Crie um sistema que use a chave de criptografia

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

Permissões necessárias

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

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

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

Passos

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

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

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

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

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

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

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

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

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

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

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

- a. Para um par HA:

POST /azure/ha/working-environments

O corpo da solicitação deve incluir os seguintes campos:

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



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

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

- b. Para um sistema de nó único:

POST /azure/vsa/working-environments

O corpo da solicitação deve incluir os seguintes campos:

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



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

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

Resultado

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

para criptografia de dados.

Configurar o licenciamento do Cloud Volumes ONTAP no Azure

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

Freemium

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

Passos

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

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

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

Managed Service Identity ▼

Azure Subscription

OCCM Dev (Default) ▼

Marketplace Subscription

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

+ Add Subscription

Apply Cancel

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

Select Charging Method

☐ Professional

By capacity

▼

☐ Essential

By capacity

▼

☒ Freemium (Up to 500 GiB)

By capacity

▼

☐ Per Node

By node

▼

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

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

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

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

Traga sua própria bebida

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



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

Passos

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

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

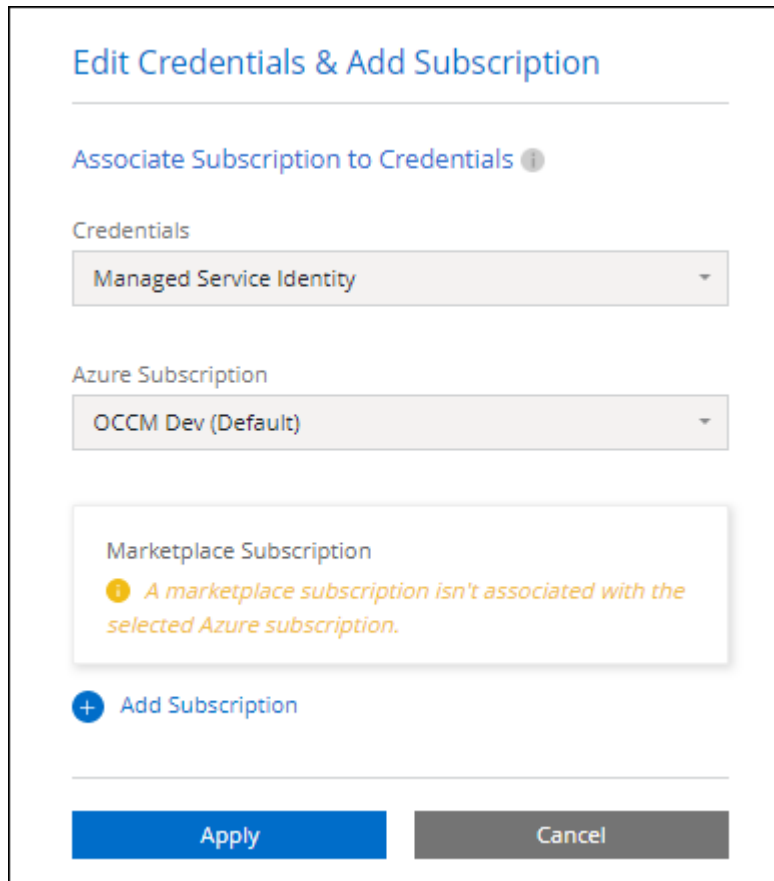
Sua licença deve estar disponível no Console antes que você possa usá-la com o Cloud Volumes ONTAP.

Se necessário, você pode ["adicionar manualmente a licença ao Console"](#) .

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

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

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



The screenshot shows a dialog box titled "Edit Credentials & Add Subscription". It contains two dropdown menus: "Credentials" with "Managed Service Identity" selected, and "Azure Subscription" with "OCCM Dev (Default)" selected. Below these is a "Marketplace Subscription" section with a yellow warning icon and the text "A marketplace subscription isn't associated with the selected Azure subscription." At the bottom left is a blue button with a plus icon and the text "Add Subscription". At the bottom are two buttons: a blue "Apply" button and a grey "Cancel" button.

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

Select Charging Method

☒ Professional

By capacity

▼

☐ Essential

By capacity

▼

☐ Freemium (Up to 500 GiB)

By capacity

▼

☐ Per Node

By node

▼

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

Assinatura PAYGO

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

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

Passos

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

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev (Default)

Marketplace Subscription

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

+ Add Subscription

Apply Cancel

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

Select Charging Method

☒ Professional	By capacity	▼
☐ Essential	By capacity	▼
☐ Freemium (Up to 500 GiB)	By capacity	▼
☐ Per Node	By node	▼

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



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

Contrato anual

Pague pelo Cloud Volumes ONTAP anualmente comprando um contrato anual.

Passos

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

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

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

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

Select Charging Method	
☒ Professional	By capacity
☐ Essential	By capacity
☐ Freemium (Up to 500 GiB)	By capacity
☐ Per Node	By node

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

Assinatura Keystone

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

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

Passos

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

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

Select Charging Method

☒ Keystone By capacity ^

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1 v

☐ Professional By capacity v

☐ Essential By capacity v

☐ Freemium (Up to 500 GiB) By capacity v

☐ Per Node By node v

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

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

O modo de alta disponibilidade (HA) do Microsoft Azure deve ser habilitado para reduzir tempos de failover não planejados e habilitar o suporte NFSv4 para o Cloud Volumes ONTAP. Neste modo, seus nós do Cloud Volumes ONTAP HA podem atingir 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 em execução no Microsoft Azure e adicionamos suporte para NFSv4. Para disponibilizar esses aprimoramentos no Cloud Volumes ONTAP, você precisa habilitar o recurso de alta disponibilidade na sua assinatura do Azure.

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

Observe o seguinte:

- Não há problemas com a alta disponibilidade do seu par Cloud Volumes ONTAP HA. Este recurso do Azure funciona em conjunto com o ONTAP para reduzir o tempo de interrupção do aplicativo observado

pelo cliente para protocolos NFS que resultam de eventos de failover não planejados.

- A ativação desse recurso não causa interrupções nos pares de HA do Cloud Volumes ONTAP .
- Habilitar esse recurso na sua assinatura do Azure não causa problemas para outras VMs.
- O Cloud Volumes ONTAP usa um balanceador de carga interno do Azure durante failovers de LIFs de gerenciamento de cluster e SVM em clientes CIFS e NFS.
- Quando o modo HA está habilitado, o Console verifica o sistema a cada 12 horas para atualizar as regras internas do Balanceador de Carga do Azure.

Um usuário do Azure que tenha privilégios de "Proprietário" pode habilitar o recurso na CLI do Azure.

Passos

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

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

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

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

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

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

Habilitar VMOrchestratorZonalMultiFD para Cloud Volumes ONTAP no Azure

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

implantação de nós em domínios de falhas separados na mesma zona de disponibilidade.

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

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

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

Passos

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

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

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

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

Inicie o Cloud Volumes ONTAP no Azure

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

Antes de começar

Você precisa do seguinte antes de começar.

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

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

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

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

Sobre esta tarefa

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

Potencial de perda de dados

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



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

Inicie um sistema Cloud Volumes ONTAP de nó único no Azure

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

Passos

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

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

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

Campo	Descrição
Editar credenciais	Você pode escolher diferentes credenciais do Azure e uma assinatura diferente do Azure para usar com este sistema Cloud Volumes ONTAP . Você precisa associar uma assinatura do Azure Marketplace à assinatura do Azure selecionada para implantar um sistema Cloud Volumes ONTAP pago conforme o uso. "Aprenda como adicionar credenciais" .

6. **Serviços:** habilite ou desabilite os serviços individuais que você deseja ou não usar com o Cloud Volumes ONTAP.

- ["Saiba mais sobre a classificação de dados da NetApp"](#)
- ["Saiba mais sobre o NetApp Backup and Recovery"](#)



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

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 agente do Console e o local de destino.



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

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

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

Campo	Descrição
Grupo de Recursos	Crie um novo grupo de recursos para o Cloud Volumes ONTAP ou use um grupo de recursos existente. A prática recomendada é usar um novo grupo de recursos dedicado para o Cloud Volumes ONTAP. Embora seja possível implantar o Cloud Volumes ONTAP em um grupo de recursos compartilhados existente, isso não é recomendado devido ao risco de perda de dados. Veja o aviso acima para mais detalhes.  Se a conta do Azure que você está usando tiver o "permissões necessárias" , o Console remove os recursos do Cloud Volumes ONTAP de um grupo de recursos, em caso de falha de implantação ou exclusão.

Campo	Descrição
Grupo de segurança gerado	Se você deixar o Console gerar o grupo de segurança para você, precisará escolher como permitirá o tráfego: • Se você escolher Somente VNet selecionada, a origem do tráfego de entrada será o intervalo de sub-redes da VNet selecionada e o intervalo de sub-redes da VNet onde o agente do Console reside. Esta é a opção recomendada. • Se você escolher Todas as VNets, a origem do tráfego de entrada será o intervalo de IP 0.0.0.0/0.
Use existente	Se você escolher um grupo de segurança existente, ele deverá atender aos requisitos do Cloud Volumes ONTAP . "Exibir o grupo de segurança padrão" .

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

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

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

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

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



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

12. **Inscreva-se no Azure Marketplace:** Você verá esta página se o Console não conseguir habilitar implantações programáticas do Cloud Volumes ONTAP. Siga os passos listados na tela. consulte ["Implantação programática de produtos do Marketplace"](#) para mais informações.

13. **Recursos de armazenamento subjacentes:** escolha as configurações para o agregado inicial: um tipo de disco, um tamanho para cada disco e se a hierarquização de dados para armazenamento de Blobs deve ser habilitada.

Observe o seguinte:

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

que usam um tamanho de disco diferente usando a opção de alocação avançada.

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

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

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

14. Velocidade de gravação e WORM:

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

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

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

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

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

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

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

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

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

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

Campo	Descrição
Tamanho	O tamanho máximo que você pode inserir depende muito se você habilita o provisionamento fino, que permite criar um volume maior que o armazenamento físico disponível atualmente.
Controle de acesso (somente para NFS)	Uma política de exportação define os clientes na sub-rede que podem acessar o volume. Por padrão, o Console insere um valor que fornece acesso a todas as instâncias na sub-rede.
Permissões e usuários/grupos (somente para CIFS)	Esses campos permitem que você controle o nível de acesso a um compartilhamento para usuários e grupos (também chamados de listas de controle de acesso ou ACLs). Você pode especificar usuários ou grupos locais ou de domínio do Windows, ou usuários ou grupos do UNIX. Se você especificar um nome de usuário de domínio do Windows, deverá incluir o domínio do usuário usando o formato domínio\nome de usuário.

Campo	Descrição
Política de Snapshot	Uma política de cópia de instantâneo especifica a frequência e o número de cópias de instantâneo do NetApp criadas automaticamente. Uma cópia do NetApp Snapshot é uma imagem do sistema de arquivos de um momento específico que não tem impacto no desempenho e requer armazenamento mínimo. Você pode escolher a política padrão ou nenhuma. Você pode escolher nenhum para dados transitórios: por exemplo, tempdb para Microsoft SQL Server.
Opções avançadas (somente para NFS)	Selecione uma versão do NFS para o volume: NFSv3 ou NFSv4.
Grupo iniciador e IQN (somente para iSCSI)	Os destinos de armazenamento iSCSI são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Os grupos de iniciadores são tabelas de nomes de nós de host iSCSI e controlam quais iniciadores têm acesso a quais LUNs. Os destinos iSCSI se conectam à rede por meio de adaptadores de rede Ethernet padrão (NICs), placas de mecanismo de descarregamento TCP (TOE) com iniciadores de software, adaptadores de rede convergentes (CNAs) ou adaptadores de bust de host dedicados (HBAs) e são identificados por nomes qualificados iSCSI (IQNs). Quando você cria um volume iSCSI, o Console cria automaticamente um LUN para você. Simplificamos criando apenas um LUN por volume, portanto não há gerenciamento envolvido. Depois de criar o volume, "use o IQN para conectar-se ao LUN de seus hosts" .

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

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

- Volume Name:** A text input field containing 'ABDcv5689'.
- Storage VM (SVM):** A dropdown menu showing 'svm_c...CVO1'.
- Volume Size:** A text input field containing '100'.
- Unit:** A dropdown menu showing 'GiB'.
- Snapshot Policy:** A dropdown menu showing 'default'.
- Below the Snapshot Policy dropdown, there is a link 'default policy' with an information icon.

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

Campo	Descrição
Endereço IP primário e secundário do DNS	Os endereços IP dos servidores DNS que fornecem resolução de nomes para o servidor CIFS. Os servidores DNS listados devem conter os registros de localização de serviço (SRV) necessários para localizar os servidores LDAP do Active Directory e os controladores de domínio para o domínio ao qual o servidor CIFS se juntará.

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

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

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

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

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

Resultado

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

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

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

Depois que você terminar

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

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

Inicie um par de Cloud Volumes ONTAP HA no Azure

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

Passos

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

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

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

5. **Serviços:** habilite ou desabilite os serviços individuais com base na sua vontade de usá-los com o Cloud Volumes ONTAP.
 - ["Saiba mais sobre a classificação de dados da NetApp"](#)
 - ["Saiba mais sobre o NetApp Backup and Recovery"](#)



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

6. Modelos de implantação de HA:

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

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

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

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

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

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

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

Campo	Descrição
Grupo de Recursos	Crie um novo grupo de recursos para o Cloud Volumes ONTAP ou use um grupo de recursos existente. A prática recomendada é usar um novo grupo de recursos dedicado para o Cloud Volumes ONTAP. Embora seja possível implantar o Cloud Volumes ONTAP em um grupo de recursos compartilhados existente, isso não é recomendado devido ao risco de perda de dados. Veja o aviso acima para mais detalhes. Você deve usar um grupo de recursos dedicado para cada par de Cloud Volumes ONTAP HA implantado no Azure. Somente um par de HA é suportado em um grupo de recursos. O Console terá problemas de conexão se você tentar implantar um segundo par de Cloud Volumes ONTAP HA em um grupo de recursos do Azure.  Se a conta do Azure que você está usando tiver o "permissões necessárias", o Console remove os recursos do Cloud Volumes ONTAP de um grupo de recursos, em caso de falha de implantação ou exclusão.

Campo	Descrição
Grupo de segurança gerado	Se você deixar o Console gerar o grupo de segurança para você, precisará escolher como permitirá o tráfego: • Se você escolher Somente VNet selecionada, a origem do tráfego de entrada será o intervalo de sub-redes da VNet selecionada e o intervalo de sub-redes da VNet onde o agente do Console reside. Esta é a opção recomendada. • Se você escolher Todas as VNets, a origem do tráfego de entrada será o intervalo de IP 0.0.0.0/0.
Use existente	Se você escolher um grupo de segurança existente, ele deverá atender aos requisitos do Cloud Volumes ONTAP . "Exibir o grupo de segurança padrão" .

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

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

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

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

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



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

11. **Inscreva-se no Azure Marketplace:** siga as etapas se o Console não conseguir habilitar implantações programáticas do Cloud Volumes ONTAP.

12. **Recursos de armazenamento subjacentes:** escolha as configurações para o agregado inicial: um tipo de disco, um tamanho para cada disco e se a hierarquização de dados para armazenamento de Blobs deve ser habilitada.

Observe o seguinte:

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

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

- Se o acesso público à sua conta de armazenamento estiver desabilitado na VNet, você não poderá habilitar a hierarquização de dados no seu sistema Cloud Volumes ONTAP . Para obter informações, consulte ["Regras do grupo de segurança"](#) .

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

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

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

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

13. Velocidade de gravação e WORM:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Volume Details & Protection

Volume Name i

ABDcv5689

Volume Size i

100

Storage VM (SVM)

svm_...CVO1 ▼

Unit

GiB ▼

Snapshot Policy

default ▼

default policy i

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

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

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

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

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

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

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

Resultado

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

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

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

Depois que você terminar

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

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

Verificar imagem da plataforma Azure

Verificação de imagem do Azure Marketplace para Cloud Volumes ONTAP

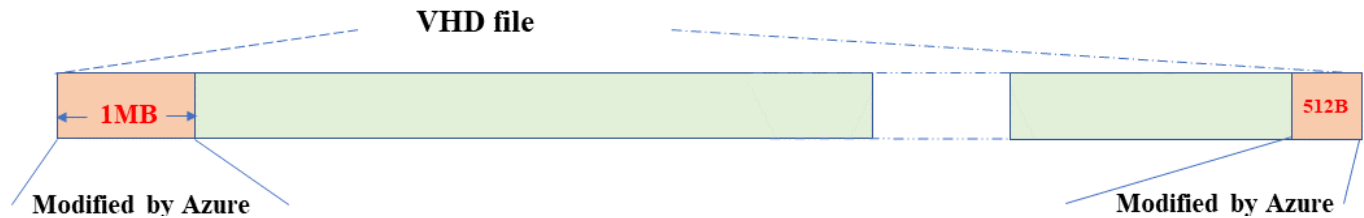
A verificação de imagem do Azure está em conformidade com os requisitos de segurança aprimorados da NetApp . Verificar um arquivo de imagem é um processo simples. No entanto, a verificação da assinatura da imagem do Azure requer considerações específicas para o arquivo de imagem VHD do Azure porque ele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



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

Alteração de arquivos VHD publicados pelo Azure

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



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

Links relacionados

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

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

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

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

Passos

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

Cloud Volumes ONTAP 9.15.0P1

Date Posted : 17-May-2024

Cloud Volumes ONTAP

Non-Restricted Countries

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

DOWNLOAD 9150P1_V_IMAGE.TGZ [2.58 GB]

[View and download checksums](#)

DOWNLOAD 9150P1_V_IMAGE.TGZ.PEM [451 B]

[View and download checksums](#)

DOWNLOAD 9150P1_V_IMAGE.TGZ.SIG [256 B]

[View and download checksums](#)

Cloud Volumes ONTAP

Restricted Countries

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

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ [2.58 GB]

[View and download checksums](#)

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ.PEM [451 B]

[View and download checksums](#)

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ.SIG [256 B]

[View and download checksums](#)

Cloud Volumes ONTAP

DOWNLOAD GCP-9-15-0P1_PKG.TAR.GZ [7.49 KB]

[View and download checksums](#)

DOWNLOAD AZURE-9-15-0P1_PKG.TAR.GZ [7.64 KB]

[View and download checksums](#)

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

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

4. Verifique se o `md5sum` e `sha256sum` os valores correspondem aos da imagem do Azure baixada.

5. No Linux e macOS, extraia o arquivo `tar.gz` usando o `tar -xzf` comando.

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

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

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

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

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

Antes de começar

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

Passos

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

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

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

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

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

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

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

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

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

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

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

Exportar arquivo VHD usando o Azure Cloud Shell no Linux

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

Passos

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

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

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


```

PS /home/user1> $diskName = "9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = "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

```

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

```

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

```

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

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

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

5. Limpe o disco gerenciado

```

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

```


Exportar arquivo VHD usando a CLI do Azure no Linux

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

Passos

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

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

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

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

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

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

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

4. Exporte o arquivo VHD do disco gerenciado.

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

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

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

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

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

5. Verifique o status da cópia do blob.

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

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

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

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

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

7. Limpe o disco gerenciado

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

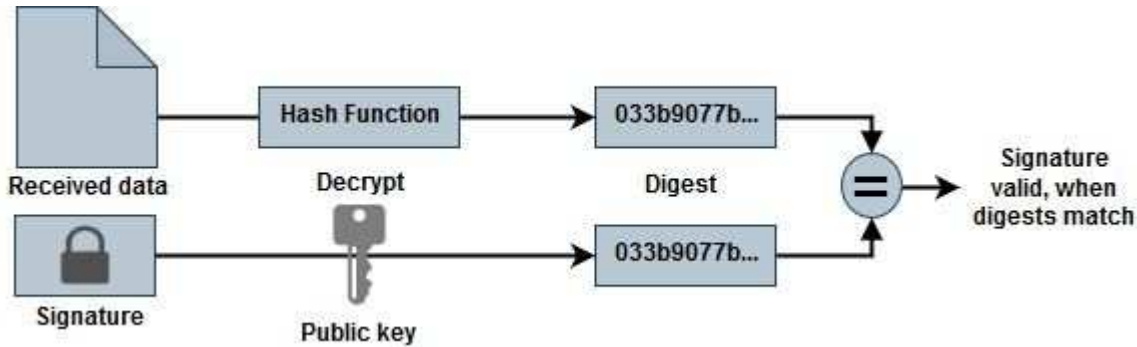
Verificar assinatura do arquivo

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

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

Resumo do fluxo de trabalho de verificação de assinatura de arquivo

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



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

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

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

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

Passos

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

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

2. Verifique a cadeia de confiança.

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

3. Remova 1 MB (1.048.576 bytes) no início e 512 bytes no final do arquivo VHD. Ao usar `tail`, o `-c +K`

opção gera bytes a partir do K-ésimo byte do arquivo. Portanto, ele passa 1048577 para `tail -c`.

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

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

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

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

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

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

5. Limpe o espaço de trabalho.

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

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

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

Passos

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

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

2. Verifique a cadeia de confiança.

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

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

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

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

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

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

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

5. Limpe o espaço de trabalho.

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

Implantar o Cloud Volumes ONTAP no marketplace do Azure

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

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

Sobre esta tarefa

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

- A versão mais recente do Cloud Volumes ONTAP (9.16.1 ou posterior).

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

Antes de começar

- Certifique-se de ter uma assinatura válida do Azure Marketplace.
- Certifique-se de atender aos requisitos de rede para um ["Implantação de HA em uma única AZ"](#) no Azure. Consulte ["Configurar a rede do Azure para o Cloud Volumes ONTAP"](#) .
- Você precisa ter uma destas funções do Azure atribuídas para implantar o Cloud Volumes ONTAP:
 - O `contributor` função com as permissões padrão. Para mais informações, consulte o ["Documentação do Microsoft Azure: funções integradas do Azure"](#) .
 - Uma função RBAC personalizada com as seguintes permissões. Para mais informações, consulte o ["Documentação do Azure: Funções personalizadas do Azure"](#) .

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



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

Passos

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



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

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

Depois que você terminar

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

Uma vez acessível, use o ONTAP System Manager ou o ONTAP CLI para efetuar login na VM de armazenamento com as credenciais de administrador que você definiu. Depois disso, você pode criar

volumes, LUNs ou compartilhamentos e começar a utilizar os recursos de armazenamento do Cloud Volumes ONTAP.

Solucionar problemas de implantação

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

Passos

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

Descubra os sistemas implantados no Console

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

Sobre esta tarefa

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

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

Antes de começar

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

Passos

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

Depois que você terminar

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

Links relacionados

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

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

Comece a usar o Google Cloud

Início rápido para o Cloud Volumes ONTAP no Google Cloud

Comece a usar o Cloud Volumes ONTAP no Google Cloud em poucas etapas.

1

Criar um agente de console

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

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

2

Planeje sua configuração

O Console oferece pacotes pré-configurados que correspondem aos seus requisitos de carga de trabalho, ou você pode criar sua própria configuração. Se você escolher sua própria configuração, deverá entender as opções disponíveis.

["Saiba mais sobre o planejamento de sua configuração"](#).

3

Configure sua rede

1. Certifique-se de que sua VPC e sub-redes oferecerão suporte à conectividade entre o agente do Console e o Cloud Volumes ONTAP.
2. Se você planeja habilitar a hierarquização de dados, ["configurar a sub-rede Cloud Volumes ONTAP para"](#)

[acesso privado do Google](#)" .

3. Se você estiver implantando um par de HA, certifique-se de ter quatro VPCs, cada uma com sua própria sub-rede.
4. Se você estiver usando uma VPC compartilhada, forneça a função *Usuário da rede de computação* à conta de serviço do agente do Console.
5. Habilite o acesso de saída à Internet da VPC de destino para o NetApp AutoSupport.

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

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

4

Configurar uma conta de serviço

O Cloud Volumes ONTAP requer uma conta de serviço do Google Cloud para duas finalidades. A primeira é quando você habilita ["hierarquização de dados"](#) para hierarquizar dados frios para armazenamento de objetos de baixo custo no Google Cloud. A segunda é quando você habilita o ["Backup e recuperação da NetApp"](#) para fazer backup de volumes em armazenamento de objetos de baixo custo.

Você pode configurar uma conta de serviço e usá-la para ambas as finalidades. A conta de serviço deve ter a função **Administrador de armazenamento**.

["Leia as instruções passo a passo"](#) .

5

Habilitar APIs do Google Cloud

["Habilite as seguintes APIs do Google Cloud no seu projeto"](#) . Essas APIs são necessárias para implantar o agente do Console e o Cloud Volumes ONTAP.

- API do Gerenciador de Implantação em Nuvem V2
- API de registro em nuvem
- API do Gerenciador de Recursos de Nuvem
- API do mecanismo de computação
- API de gerenciamento de identidade e acesso (IAM)

6

Inicie o Cloud Volumes ONTAP usando o Console

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

Links relacionados

- ["Criando um agente de console"](#)
- ["Instalando o software do agente do Console em um host Linux"](#)
- ["O que o Console 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 corresponda aos seus requisitos de carga de trabalho ou pode criar sua própria configuração. Se você escolher sua própria configuração, deverá entender as opções disponíveis.

Escolha uma licença do Cloud Volumes ONTAP

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

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

Escolha uma região com suporte

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

Escolha um tipo de máquina compatível

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

["Configurações com suporte para Cloud Volumes ONTAP na GCP"](#)

Entenda os limites de armazenamento

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

["Limites de armazenamento para Cloud Volumes ONTAP na GCP"](#)

Dimensione seu sistema no GCP

Dimensionar seu sistema Cloud Volumes ONTAP pode ajudar você a atender aos requisitos de desempenho 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 máquinas suportados no ["Notas de versão do Cloud Volumes ONTAP"](#) e depois analise os detalhes do Google sobre cada tipo de máquina compatível. Adapte seus requisitos de carga de trabalho ao 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 mais detalhes:

- ["Documentação do Google Cloud: tipos de máquinas padrão N1"](#)
- ["Documentação do Google Cloud: Desempenho"](#)

Tipo de disco GCP

Ao criar volumes para o Cloud Volumes ONTAP, você precisa escolher o armazenamento em nuvem subjacente que o Cloud Volumes ONTAP usa para um disco. O tipo de disco pode ser qualquer um dos seguintes:

- *Discos persistentes SSD zonais*: discos persistentes SSD são melhores para cargas de trabalho que exigem altas taxas de IOPS aleatórios.
- *Discos persistentes zonais balanceados*: Esses SSDs equilibram desempenho e custo ao fornecer IOPS mais baixos por GB.
- *Discos persistentes padrão zonais*: os discos persistentes padrão são econômicos e podem lidar com operações sequenciais de leitura/gravação.

Para mais detalhes, consulte o ["Documentação do Google Cloud: Discos permanentes zonais \(padrão e SSD\)"](#).

Tamanho do disco do GCP

Você precisa escolher um tamanho de disco inicial ao implantar um sistema Cloud Volumes ONTAP. Depois disso, você pode deixar que o NetApp Console gerencie a capacidade de um sistema para você, mas se quiser criar agregados sozinho, esteja ciente do seguinte:

- Todos os discos em um agregado devem ter o mesmo tamanho.
- Determine o espaço 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 mais detalhes:

- ["Documentação do Google Cloud: Discos permanentes zonais \(padrão e SSD\)"](#)
- ["Documentação do Google Cloud: Otimizando o desempenho do disco permanente e do SSD local"](#)

Exibir discos de sistema padrão

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

- ["Visualize os discos padrão para dados do sistema Cloud Volumes ONTAP no Google Cloud"](#).
- ["Documentação do Google Cloud: Cotas de recursos"](#)

O Google Cloud Compute Engine impõe cotas no uso de recursos, portanto, você deve garantir que não atingiu seu limite antes de implantar o Cloud Volumes ONTAP.



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

Coletar informações de rede

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

Informações de rede para um sistema de nó único

Informações da GCP	Seu valor
Região	
Zona	
Rede VPC	
Sub-rede	
Política de firewall (se estiver usando a sua própria)	

Informações de rede para um par HA em várias zonas

Informações da GCP	Seu valor
Região	
Zona para 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 HA em uma única zona

Informações da GCP	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 Console permite que você escolha 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, bem como os riscos e

recomendações ao usar alta velocidade de gravação. ["Saiba mais sobre velocidade de gravação"](#) .

Escolha um perfil de uso de volume

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

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

Provisionamento fino

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

Desduplicação

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

Compressão

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

Configurar a rede do Google Cloud para o Cloud Volumes ONTAP

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

Se você deseja implantar um par HA, você deve ["saiba como os pares de HA funcionam no Google Cloud"](#) .

Requisitos para o Cloud Volumes ONTAP

Os seguintes requisitos 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 Nuvem Privada Virtual (VPC) é necessária para um sistema de nó único.

Endereços IP privados

Para um sistema de nó único no Google Cloud, o Console aloca endereços IP privados para o seguinte:

- Nó

- Conjunto
- VM de armazenamento
- Dados NAS LIF
- Dados iSCSI LIF

Você pode pular a criação do LIF de gerenciamento da VM de armazenamento (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. Um LIF de gerenciamento de VM de armazenamento (SVM) é necessário para ferramentas de gerenciamento como o SnapCenter.

Requisitos específicos para pares HA

Se você quiser implantar um par HA, certifique-se de que sua rede atenda aos seguintes requisitos.

Uma ou várias zonas

Você pode garantir a alta disponibilidade dos seus dados implantando uma configuração de HA em várias zonas ou em uma única zona. O Console solicita que você escolha várias zonas ou uma única zona ao criar o par HA.

- Várias zonas (recomendado)

A implantação de uma configuração de HA em três zonas garante disponibilidade contínua de dados caso ocorra uma falha em uma zona. Observe que o desempenho de gravação é um pouco menor quando comparado ao 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 espalhado. Esta política garante que uma configuração de HA seja protegida de um único ponto de falha dentro da zona, sem precisar usar zonas separadas para obter isolamento de falhas.

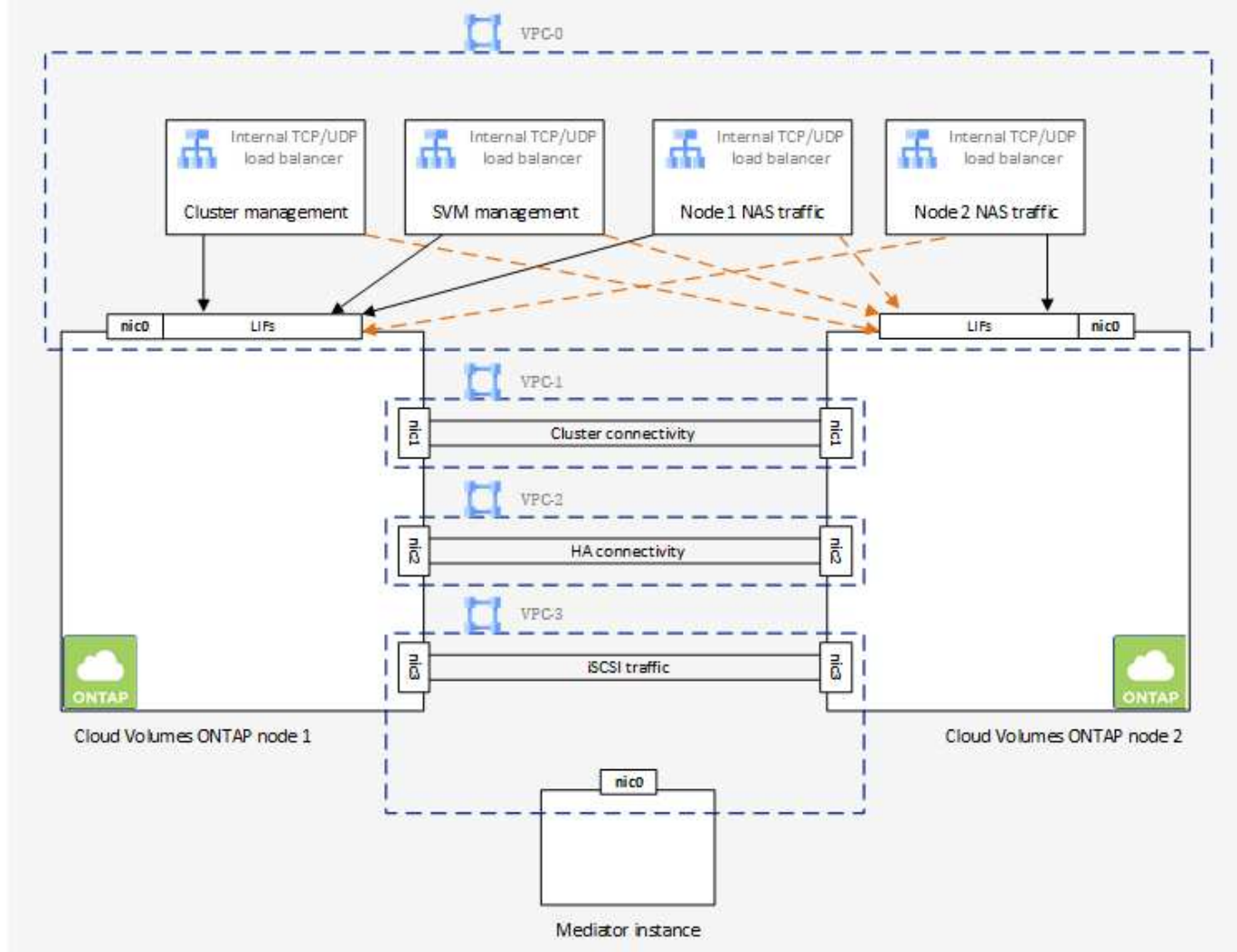
Este modelo de implantação reduz seus custos porque não há cobranças de saída de dados entre zonas.

Quatro Nuvens Privadas Virtuais

Quatro Nuvens Privadas Virtuais (VPCs) são necessárias para uma configuração de HA. Quatro VPCs são necessárias porque o Google Cloud exige que cada interface de rede resida em uma rede VPC separada.

O Console solicita que você escolha quatro VPCs ao criar o par HA:

- VPC-0 para conexões de entrada aos dados e nós
- VPC-1, VPC-2 e VPC-3 para comunicação interna entre os nós e o mediador HA



Sub-redes

Uma sub-rede privada é necessária para cada VPC.

Se você colocar o agente do Console no VPC-0, precisará habilitar o Private Google Access na sub-rede para acessar as APIs e habilitar a hierarquização de dados.

As sub-redes nessas VPCs devem ter intervalos CIDR distintos. Eles não podem ter intervalos CIDR sobrepostos.

Endereços IP privados

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

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

- **Nó único** O Console aloca 4 endereços IP para um sistema de nó único:

- Gerenciamento de nós LIF
- Gerenciamento de cluster LIF
- Dados iSCSI LIF



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

- NAS LIF

Você pode pular a criação do LIF de gerenciamento da VM de armazenamento (SVM) se implantar o Cloud Volumes ONTAP usando a API e especificar o seguinte sinalizador:

```
skipSvmManagementLif: true
```

- **Par HA** O Console aloca 12-13 endereços IP para um par HA:

- 2 LIFs de gerenciamento de nós (e0a)
- 1 Gerenciamento de cluster LIF (e0a)
- 2 iSCSI LIFs (e0a)



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

- 1 ou 2 NAS LIFs (e0a)
- 2 LIFs de cluster (e0b)
- 2 endereços IP de interconexão HA (e0c)
- 2 endereços IP iSCSI RSM (e0d)

Você pode pular a criação do LIF de gerenciamento da VM de armazenamento (SVM) se implantar o Cloud Volumes ONTAP usando a API e especificar o seguinte sinalizador:

```
skipSvmManagementLif: true
```

Balancedores de carga internos

O Console cria quatro balanceadores de carga internos do Google Cloud (TCP/UDP) que gerenciam o tráfego de entrada para o par Cloud Volumes ONTAP HA. Nenhuma configuração é necessária da sua parte. Listamos isso como um requisito simplesmente para informá-lo sobre o tráfego de rede e para atenuar quaisquer preocupações de segurança.

Um balanceador de carga é para gerenciamento de cluster, um é para gerenciamento de VM de armazenamento (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
- Um exame de saúde global

Por padrão, as portas usadas pela verificação de integridade são 63001, 63002 e 63003.

- Um serviço regional de backend TCP
- Um serviço regional de backend UDP
- Uma regra de encaminhamento TCP
- Uma regra de encaminhamento UDP
- O acesso global está desabilitado

Embora o acesso global esteja desabilitado por padrão, há suporte para habilitá-lo após a implantação. Nós o desabilitamos porque o tráfego entre regiões terá latências significativamente maiores. Queríamos garantir que você não tivesse uma experiência negativa devido a montagens acidentais entre regiões. A ativação desta opção é específica para as necessidades do seu negócio.

VPCs compartilhadas

O Cloud Volumes ONTAP e o agente do Console são suportados em uma VPC compartilhada do Google Cloud e também em VPCs autônomas.

Para um sistema de nó único, a VPC pode ser uma VPC compartilhada ou uma VPC autônoma.

Para um par HA, são necessárias quatro VPCs. Cada uma dessas VPCs pode ser compartilhada ou independente. Por exemplo, VPC-0 pode ser uma VPC compartilhada, enquanto VPC-1, VPC-2 e VPC-3 podem ser VPCs independentes.

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 o agente do Console e as instâncias da máquina virtual Cloud Volumes ONTAP em um *projeto de serviço*.

["Documentação do Google Cloud: Visão geral da VPC compartilhada"](#) .

["Revise as permissões de VPC compartilhadas necessárias abordadas na implantação do agente do Console"](#)

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

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

Pontos de extremidade Cloud Volumes ONTAP

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

Pontos finais	Aplicável para	Propósito	Modo de implantação	Impacto se o ponto final não estiver disponível
\ https://netapp-cloud-account.auth0.com	Autenticação	Usado para autenticação no Console.	Modos padrão e restrito.	A autenticação do usuário falha e os seguintes serviços permanecem indisponíveis: • Serviços Cloud Volumes ONTAP • Serviços ONTAP • Protocolos e serviços de proxy
\ https://api.bluexp.net/app.com/tenancy	Arrendamento	Usado para recuperar o recurso Cloud Volumes ONTAP do Console para autorizar recursos e usuários.	Modos padrão e restrito.	Os recursos do Cloud Volumes ONTAP e os usuários não estão autorizados.
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Usado para enviar dados de telemetria do AutoSupport para o suporte da NetApp.	Modos padrão e restrito.	As informações do AutoSupport continuam não entregues.

Pontos finais	Aplicável para	Propósito	Modo de implantação	Impacto se o ponto final não estiver disponível
https://www.googleapis.com/compute/v1/projects/ \ https://cloudresource-manager.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 para o Console no Google Cloud.

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 deve ter uma conexão VPN entre a VPC e a outra rede, por exemplo, sua rede corporativa.

["Documentação do Google Cloud: Visão geral do Cloud VPN"](#) .

Regras de firewall

O Console 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. Talvez você queira 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, estas são as regras de firewall para o Cloud Volumes ONTAP no VPC-0.

Observe que dois conjuntos de regras de firewall são necessários para uma configuração de HA:

- Um conjunto de regras para componentes HA no VPC-0. Essas regras permitem o acesso aos dados do Cloud Volumes ONTAP.
- Outro conjunto de regras para componentes HA em VPC-1, VPC-2 e VPC-3. Essas regras estão abertas para comunicação de entrada e saída entre os componentes do HA. [Saber mais](#) .



Procurando informações sobre o agente do Console? ["Exibir regras de firewall para o agente do Console"](#)

Regras de entrada

Ao adicionar um sistema Cloud Volumes ONTAP , você pode escolher o filtro de origem para a política de firewall predefinida durante a implantação:

- **Somente VPC selecionada:** o filtro de origem para 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 agente do Console reside. Esta é a opção recomendada.
- **Todas as VPCs:** o filtro de origem para tráfego de entrada é o intervalo de 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 mais informações, consulte o ["Documentação do Google Cloud: Regras de firewall do balanceador de carga"](#) .

Protocolo	Porta	Propósito
Todos os ICMP	Todos	Executando ping na instância
HTTP	80	Acesso HTTP ao console da web do ONTAP System Manager usando o endereço IP do LIF de gerenciamento do cluster
HTTPS	443	Conectividade com o agente do Console e acesso HTTPS ao console da Web do ONTAP System Manager usando o endereço IP do LIF de gerenciamento do cluster
SSH	22	Acesso SSH ao endereço IP do LIF de gerenciamento de cluster ou de 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 simples de gerenciamento de rede
TCP	445	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
TCP	635	Montagem NFS
TCP	749	Kerberos
TCP	2049	Daemon do servidor NFS
TCP	3260	Acesso iSCSI através do LIF de dados iSCSI
TCP	4045	Daemon de bloqueio NFS
TCP	4046	Monitor de status de rede para NFS
TCP	10000	Backup usando NDMP
TCP	11104	Gerenciamento de sessões de comunicação entre clusters para SnapMirror
TCP	11105	Transferência de dados do SnapMirror usando LIFs intercluster

Protocolo	Porta	Propósito
TCP	63001-63050	Portas de sondagem de balanceamento de carga para determinar qual nó está íntegro (necessário apenas para pares de HA)
UDP	111	Chamada de procedimento remoto para NFS
UDP	161-162	Protocolo simples de gerenciamento de rede
UDP	635	Montagem NFS
UDP	2049	Daemon do servidor NFS
UDP	4045	Daemon de bloqueio NFS
UDP	4046	Monitor de status de rede para NFS
UDP	4049	Protocolo NFS rquotad

Regras de saída

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

Regras básicas de saída

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

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

Regras avançadas de saída

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



A origem é a interface (endereço IP) do sistema Cloud Volumes ONTAP .

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

Serviço	Protocolo	Porta	Fonte	Destino	Propósito
AutoSupport	HTTPS	443	Gerenciamento de nós LIF	meusupporte.netapp.com	AutoSupport (HTTPS é o padrão)
	HTTP	80	Gerenciamento de nós LIF	meusupporte.netapp.com	AutoSupport (somente se o protocolo de transporte for alterado de HTTPS para HTTP)
	TCP	3128	Gerenciamento de nós LIF	Agente de console	Envio de mensagens do AutoSupport por meio de um servidor proxy no agente do Console, se uma conexão de saída com a Internet não estiver disponível
Backups de configuração	HTTP	80	Gerenciamento de nós LIF	http://<endereço-IP-do-agente-do-console>/occm/offboxconfig	Envie backups de configuração para o agente do Console. "Documentação do ONTAP"
DHCP	UDP	68	Gerenciamento de nós LIF	DHCP	Cliente DHCP para configuração inicial
DHCPs	UDP	67	Gerenciamento de nós LIF	DHCP	Servidor DHCP
DNS	UDP	53	Gerenciamento de nós LIF e dados LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	1860–18699	Gerenciamento de nós LIF	Servidores de destino	Cópia do NDMP
SMTP	TCP	25	Gerenciamento de nós LIF	Servidor de e-mail	Alertas SMTP podem ser usados para AutoSupport
SNMP	TCP	161	Gerenciamento de nós LIF	Servidor de monitoramento	Monitoramento por armadilhas SNMP
	UDP	161	Gerenciamento de nós LIF	Servidor de monitoramento	Monitoramento por armadilhas SNMP
	TCP	162	Gerenciamento de nós LIF	Servidor de monitoramento	Monitoramento por armadilhas SNMP
	UDP	162	Gerenciamento de nós LIF	Servidor de monitoramento	Monitoramento por armadilhas SNMP
SnapMirror	TCP	11104	LIF interaglomerado	LIFs interaglomerados ONTAP	Gerenciamento de sessões de comunicação entre clusters para SnapMirror
	TCP	11105	LIF interaglomerado	LIFs interaglomerados ONTAP	Transferência de dados do SnapMirror

Serviço	Protocolo	Porta	Fonte	Destino	Propósito
Log de sistema	UDP	514	Gerenciamento de nós LIF	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 no VPC-0 são [listado acima para Cloud Volumes ONTAP](#).

Enquanto isso, as regras de firewall predefinidas criadas para as instâncias em VPC-1, VPC-2 e VPC-3 permitem a comunicação de entrada em *todos* os protocolos e portas. Essas regras permitem a comunicação entre nós de HA.

A comunicação dos nós HA com o mediador HA ocorre pela porta 3260 (iSCSI).



Para habilitar alta velocidade de gravação para novas implantações de pares de HA do Google Cloud, uma unidade máxima de transmissão (MTU) de pelo menos 8.896 bytes é necessária para VPC-1, VPC-2 e VPC-3. Se você optar por atualizar as VPC-1, VPC-2 e VPC-3 existentes para uma MTU de 8.896 bytes, deverá desligar todos os sistemas HA existentes que usam essas VPCs durante o processo de configuração.

Requisitos para o agente do console

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

- ["Exibir requisitos de rede para o agente do Console"](#)
- ["Regras de firewall no Google Cloud"](#)

Configurações de rede para oferecer suporte ao proxy do agente do console

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

- **Proxy explícito:** O tráfego de saída do Cloud Volumes ONTAP usa o endereço HTTP do servidor proxy especificado durante a configuração do proxy do agente do Console. O administrador do agente do Console também pode ter configurado credenciais de usuário e certificados de CA raiz para autenticação adicional. Se um certificado de CA raiz estiver disponível para o proxy explícito, certifique-se de obter e carregar o mesmo certificado para o seu sistema Cloud Volumes ONTAP usando o ["ONTAP CLI: instalação do certificado de segurança"](#) comando.
- **Proxy transparente:** A rede está configurada para rotear automaticamente o tráfego de saída do Cloud Volumes ONTAP por meio do proxy do agente do Console. Ao configurar um proxy transparente, o administrador do agente do Console precisa fornecer apenas um certificado de CA raiz para conectividade do Cloud Volumes ONTAP, não o endereço HTTP do servidor proxy. Certifique-se de obter e carregar o mesmo certificado de CA raiz para o seu sistema Cloud Volumes ONTAP usando o ["ONTAP CLI: instalação do certificado de segurança"](#) comando.

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

Configurar tags de rede para o Cloud Volumes ONTAP no Google Cloud

Durante a configuração do proxy transparente do agente do Console, o administrador adiciona uma tag de

rede para o Google Cloud. Você precisa obter e adicionar manualmente a mesma tag de rede para sua configuração do Cloud Volumes ONTAP . Esta tag é necessária para que o servidor proxy funcione corretamente.

1. No console do Google Cloud, localize seu sistema Cloud Volumes ONTAP .
2. Vá para **Detalhes > Rede > Tags de rede**.
3. Adicione a tag usada para o agente do Console e salve a configuração.

Tópicos relacionados

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

Configurar o VPC Service Controls para implantar o Cloud Volumes ONTAP no Google Cloud

Ao escolher bloquear seu ambiente do Google Cloud com o VPC Service Controls, você deve entender como o NetApp Console e o Cloud Volumes ONTAP interagem com as APIs do Google Cloud, bem como configurar seu perímetro de serviço para implantar o Console e o Cloud Volumes ONTAP.

Os Controles de Serviço VPC permitem que você controle o acesso a serviços gerenciados pelo Google fora de um perímetro confiável, bloqueie o acesso a dados de locais não confiáveis e mitigue riscos de transferência de dados não autorizada. ["Saiba mais sobre os controles de serviço VPC do Google Cloud"](#) .

Como os serviços NetApp se comunicam com os VPC Service Controls

O Console se comunica diretamente com as APIs do Google Cloud. Isso é acionado por 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 agente do Console.

Dependendo do estilo de implantação do agente do Console, certas exceções podem ter que ser feitas para seu perímetro de serviço.

Imagens

Tanto o Cloud Volumes ONTAP quanto o Console usam imagens de um projeto dentro do GCP que é gerenciado pelo NetApp. Isso pode afetar a implantação do agente do Console 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 agente do Console 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 agente do Console e o Cloud Volumes ONTAP.

Implantando um agente de console

O usuário que implanta um agente do Console precisa ser capaz de referenciar uma imagem hospedada no projectId `netapp-cloudmanager` e no número do projeto `14190056516`.

Implantando o Cloud Volumes ONTAP

- A conta de serviço do Console precisa fazer referência a uma imagem hospedada no projectId `netapp-`

cloudmanager e ao número do projeto *14190056516* do projeto de serviço.

- A conta de serviço do Agente de Serviço de APIs padrão do Google precisa fazer referência a uma imagem hospedada no projectId *netapp-cloudmanager* e ao número do projeto *14190056516* do projeto de serviço.

Exemplos das regras necessárias para extrair essas imagens com o VPC Service Controls são definidos abaixo.

Políticas de perímetro do VPC Service Controls

As políticas permitem exceções aos conjuntos de regras do VPC Service Controls. Para mais informações sobre políticas, visite o ["Documentação da política de controles de serviço do GCP VPC"](#).

Para definir as políticas exigidas pelo Console, 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 do VPC Service Controls. Observe também que **todas** as regras são obrigatórias 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 pela NetApp para armazenar imagens para o agente do Console e para o Cloud Volumes ONTAP.

Crie uma conta de serviço do Google Cloud para o Cloud Volumes ONTAP

O Cloud Volumes ONTAP requer uma conta de serviço do Google Cloud para duas finalidades. A primeira é quando você habilita "[hierarquização de dados](#)" para hierarquizar dados frios para armazenamento de objetos de baixo custo no Google Cloud. A segunda é quando você habilita o "[Backup e recuperação da NetApp](#)" para fazer backup de volumes em armazenamento de objetos de baixo custo.

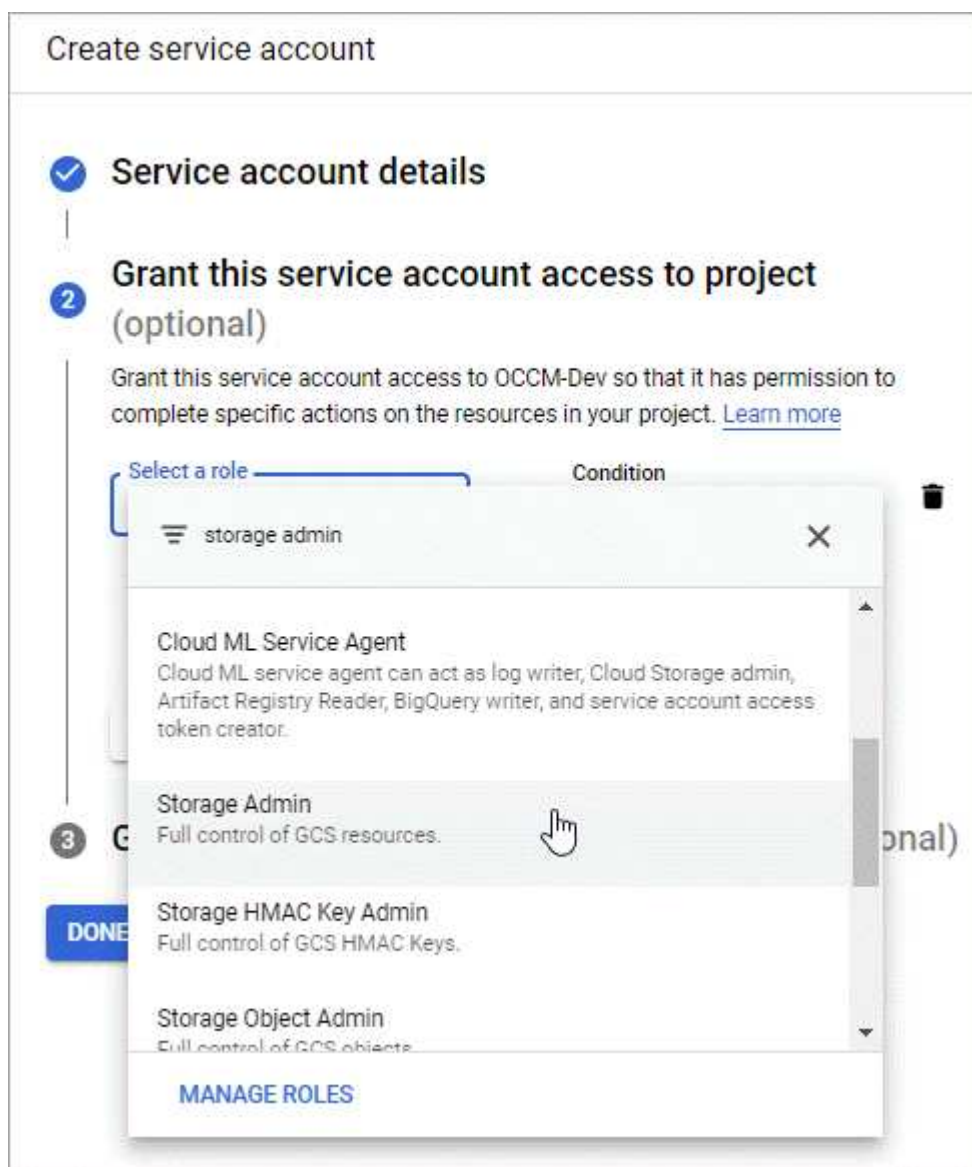
O Cloud Volumes ONTAP usa a conta de serviço para acessar e gerenciar um bucket para dados em camadas e outro bucket para backups.

Você pode configurar uma conta de serviço e usá-la para ambas as finalidades. A conta de serviço deve ter a função **Administrador de armazenamento**.

Passos

1. No console do Google Cloud, "[vá para a página de 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 a esta conta de serviço acesso ao projeto:** Selecione a função **Administrador de armazenamento**.



- c. **Conceder aos usuários acesso a esta conta de serviço:** adicione a conta de serviço do agente do Console como um *Usuário da conta de serviço* a esta nova conta de serviço.

Esta etapa é necessária somente para a hierarquização de dados. Não é necessário para backup e recuperação.

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 vem a seguir?

Você precisará selecionar a conta de serviço mais tarde ao criar um sistema Cloud Volumes ONTAP .

Details and Credentials

default-project

Google Cloud Project

gcp-sub2

Marketplace Subscription

Edit Project

Details

Working Environment Name (Cluster Name)

cloudvolumesontap

Service Account

Service Account Name

account1

+ Add Labels

Optional Field | Up to four labels

Credentials

User Name

admin

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 gravá-los no disco, você pode usar as APIs para criar um sistema Cloud Volumes ONTAP que usa *chaves de criptografia gerenciadas pelo cliente*. Essas são 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 agente do Console tenha as permissões corretas no nível do projeto, no projeto onde a chave está armazenada.

As permissões são fornecidas no "[as permissões da conta de serviço por padrão](#)", mas pode não ser aplicado 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 para o "[Agente de serviço do Google Compute Engine](#)" tem permissões do Cloud KMS Encrypter/Decrypter 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 /gcp/vsa/metadata/gcp-encryption-keys Chamada de API ou escolhendo "Copiar nome do recurso" na chave no console do GCP.
4. Se estiver usando chaves de criptografia gerenciadas pelo cliente e hierarquizando dados para armazenamento de objetos, o NetApp Console tentará utilizar as mesmas chaves usadas para criptografar os discos persistentes. Mas primeiro você precisa habilitar os buckets do Google Cloud Storage para usar as chaves:
 - a. Encontre 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 permissões de Criptografador/Descritografador do Cloud KMS.

Para 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 sistema.

Exemplo

```
"gcpEncryptionParameters": {  
  "key": "projects/project-1/locations/us-east4/keyRings/keyring-  
1/cryptoKeys/generatedkey1"  
}
```

Consulte o ["Documentação de automação do NetApp Console"](#) para mais detalhes sobre o uso do parâmetro "GcpEncryption".

Configurar o licenciamento do Cloud Volumes ONTAP no Google Cloud

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

Freemium

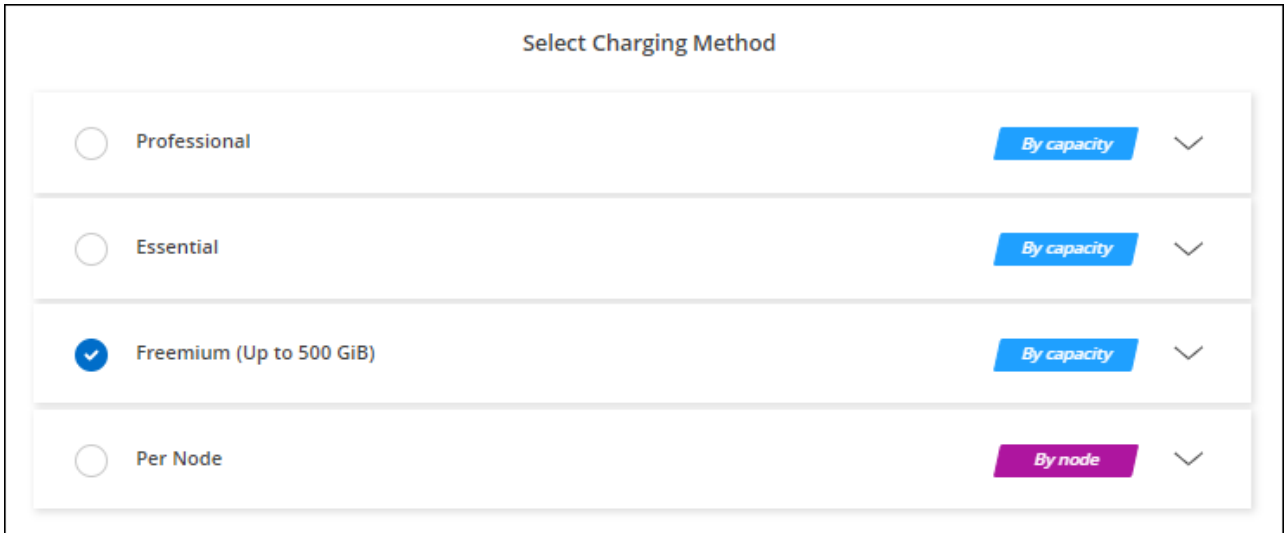
Selecione a oferta Freemium para usar o Cloud Volumes ONTAP gratuitamente com até 500 GiB de capacidade provisionada. ["Saiba mais sobre a oferta Freemium"](#) .

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas no Console NetApp .
 - 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 pela assinatura do marketplace, a menos que exceda 500 GiB de capacidade provisionada, momento em que o sistema será automaticamente convertido para o ["Pacote Essentials"](#).

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



The screenshot shows a 'Select Charging Method' dialog box with four radio button options. The 'Freemium (Up to 500 GiB)' option is selected, indicated by a blue checkmark. To the right of each option is a button labeled 'By capacity' (for Professional, Essential, and Freemium) or 'By node' (for Per Node), followed by a downward arrow. The buttons for 'By capacity' are blue, while the button for 'By node' is purple.

["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 ou Professional.

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

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

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

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

Traga sua própria bebida

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



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

Passos

1. ["Entre em contato com a equipe de vendas da NetApp para obter uma licença"](#)

2. "Adicione sua conta do site de suporte da NetApp ao console da NetApp"

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

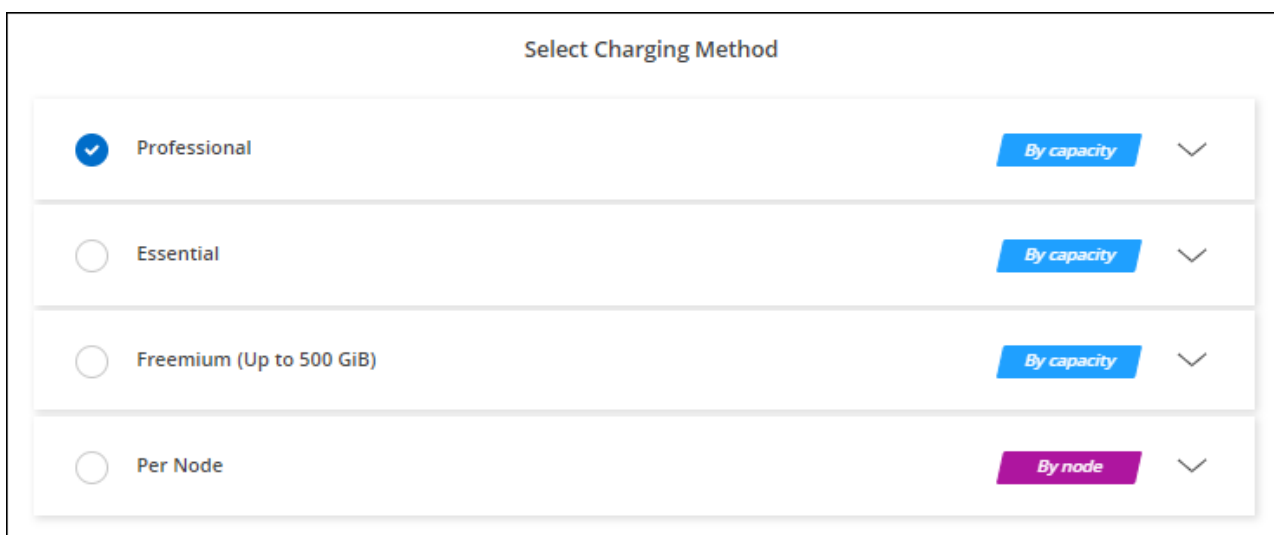
Sua licença deve estar disponível no Console antes que você possa usá-la com o Cloud Volumes ONTAP. Se necessário, você pode [adicionar manualmente a licença ao Console](#) .

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

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

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



The screenshot shows a 'Select Charging Method' dialog box with four options:

- Professional** (selected with a blue checkmark): **By capacity** (blue button) and a dropdown arrow.
- Essential**: **By capacity** (blue button) and a dropdown arrow.
- Freemium (Up to 500 GiB)**: **By capacity** (blue button) and a dropdown arrow.
- Per Node**: **By node** (purple button) and a dropdown arrow.

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

Assinatura PAYGO

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

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

Passos

- No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
- Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas.
 - 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.
 - Após retornar ao Console, selecione um pacote baseado em capacidade quando chegar à página de métodos de cobrança.

Select Charging Method

☒ Professional

By capacity

☐ Essential

By capacity

☐ Freemium (Up to 500 GiB)

By capacity

☐ Per Node

By node

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



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

Contrato anual

Pague pelo Cloud Volumes ONTAP anualmente comprando um contrato anual.

Passos

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

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

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

2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas.
 - a. Na página **Detalhes e credenciais**, clique em **Editar credenciais > Adicionar assinatura** 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 **Assinar**.
 - c. Após retornar ao Console, selecione um pacote baseado em capacidade quando chegar à página de métodos de cobrança.

Select Charging Method

☒ Professional

By capacity

▼

☐ Essential

By capacity

▼

☐ Freemium (Up to 500 GiB)

By capacity

▼

☐ Per Node

By node

▼

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

Assinatura Keystone

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

Passos

1. Se você ainda não tem uma assinatura, ["entre em contato com a NetApp"](#)
2. [Entre em contato com a NetApp](#) para autorizar sua conta de usuário do Console com uma ou mais assinaturas do Keystone .
3. Depois que a NetApp autorizar sua conta, ["vincule suas assinaturas para uso com o Cloud Volumes ONTAP"](#) .
4. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as etapas.
 - a. Selecione o método de cobrança da Assinatura Keystone quando solicitado a escolher um método de cobrança.

[illegible]

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

Inicie o Cloud Volumes ONTAP no Google Cloud

Você pode iniciar o Cloud Volumes ONTAP em uma configuração de nó único ou como um par de HA no Google Cloud.

Antes de começar

Você precisa do seguinte antes de começar.

- Um agente do Console que está ativo e em execução.
 - Você deveria ter um "Agente de console associado ao seu sistema" .
 - "Você deve estar preparado para deixar o agente do Console em execução o tempo todo" .
 - A conta de serviço associada ao agente do Console "deve ter as permissões necessárias"
- Uma compreensão da configuração que você deseja usar.

Você deve ter se preparado escolhendo uma configuração e obtendo informações de rede do Google Cloud com seu administrador. Para mais detalhes, consulte "[Planejando sua configuração do Cloud Volumes ONTAP](#)".

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

"Aprenda como configurar o licenciamento".

- As APIs do Google Cloud devem ser "[habilitado em seu projeto](#)" :
 - API do Gerenciador de Implantação em Nuvem V2
 - API de registro em nuvem
 - API do Gerenciador de Recursos de Nuvem
 - API do mecanismo de computação
 - API de gerenciamento de identidade e acesso (IAM)

Inicie um sistema de nó único no Google Cloud

Crie um sistema no NetApp Console para iniciar o Cloud Volumes ONTAP no Google Cloud.

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique em **Adicionar Sistema** e siga as instruções.
3. **Escolha um local**: Selecione **Google Cloud** e * Cloud Volumes ONTAP*.
4. Se você for solicitado, "[criar um agente de console](#)".
5. **Detalhes e credenciais**: selecione um projeto, especifique um nome de cluster, opcionalmente selecione uma conta de serviço, opcionalmente adicione rótulos e, em seguida, especifique as credenciais.

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

Campo	Descrição
Nome do sistema	O Console usa o nome do sistema para nomear o sistema Cloud Volumes ONTAP e a instância da 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 " hierarquização de dados " ou " Backup e recuperação da NetApp " com o Cloud Volumes ONTAP, você precisa habilitar Conta de serviço e selecionar uma conta de serviço que tenha a função de administrador de armazenamento predefinida. " Aprenda a criar uma conta de serviço ".
Adicionar rótulos	Os rótulos são metadados para seus recursos do Google Cloud. O Console adiciona os rótulos ao sistema Cloud Volumes ONTAP e aos recursos do Google Cloud associados ao sistema. Você pode adicionar até quatro rótulos na interface do usuário ao criar um sistema e depois adicionar mais depois que ele for criado. Observe que a API não limita você a quatro rótulos ao criar um sistema. Para obter informações sobre rótulos, consulte o " Documentação do Google Cloud: Rotulagem de recursos ".
Nome de usuário e senha	Estas são as credenciais para a conta de administrador do cluster Cloud Volumes ONTAP. Você pode usar essas credenciais para se conectar ao Cloud Volumes ONTAP por meio do ONTAP System Manager ou do ONTAP CLI. Mantenha o nome de usuário padrão <i>admin</i> ou altere-o para um nome de usuário personalizado.

Campo	Descrição
Editar Projeto	Selecione o projeto onde você deseja que o Cloud Volumes ONTAP resida. O projeto padrão é o projeto onde o Console está localizado. Se você não vir nenhum projeto adicional na lista suspensa, significa que você ainda não associou a conta de serviço a outros projetos. Acesse o console do Google Cloud, abra o serviço IAM e selecione o projeto. Adicione a conta de serviço com a função que você usa para o Console nesse projeto. Você precisará repetir esta etapa para cada projeto.  Esta é a conta de serviço que você configurou para o Console, "conforme descrito nesta página". Clique em Adicionar assinatura para associar as credenciais selecionadas a uma assinatura. Para criar um sistema Cloud Volumes ONTAP com pagamento conforme o uso, você precisa selecionar um projeto do Google Cloud associado a uma assinatura do Cloud Volumes ONTAP no marketplace do Google Cloud. Consulte "Associando uma assinatura do marketplace às credenciais do Google Cloud".

6. **Serviços:** Selecione os serviços que você deseja usar neste sistema. Para selecionar Backup e Recuperação ou usar o NetApp Cloud Tiering, você deve ter especificado a Conta de Serviço na etapa 3.



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

7. **Localização e conectividade:** selecione um local, escolha uma política de firewall e confirme a conectividade de rede com o armazenamento do Google Cloud para hierarquização de dados.

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

Campo	Descrição
Verificação de conectividade	Para hierarquizar dados frios em um bucket do Google Cloud Storage, a sub-rede na qual o Cloud Volumes ONTAP reside deve ser configurada para o Private Google Access. Para obter instruções, consulte "Documentação do Google Cloud: Configurando o acesso privado do Google" .
Política de firewall gerada	Se você deixar o Console gerar a política de firewall para você, precisará escolher como permitirá o tráfego: - Se você escolher Somente VPC selecionada, o filtro de origem para tráfego de entrada será o intervalo de sub-rede da VPC selecionada e o intervalo de sub-rede da VPC onde o agente do Console reside. Esta é a opção recomendada. - Se você escolher Todas as VPCs, o filtro de origem para o tráfego de entrada será o intervalo de IP 0.0.0.0/0.

Campo	Descrição
Usar política de firewall existente	Se você usar uma política de firewall existente, certifique-se de que ela inclua as regras necessárias: "Saiba mais sobre as regras de firewall para o Cloud Volumes ONTAP"

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

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

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

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

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



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

11. **Recursos de armazenamento subjacentes:** escolha as 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 que o Console cria quando você usa a opção de provisionamento simples. Você pode criar agregados que usam um tamanho de disco diferente usando a opção de alocação avançada.

Para obter ajuda na escolha do tipo e tamanho do disco, consulte ["Dimensione seu sistema no Google Cloud"](#).

12. **Flash Cache, Velocidade de Gravação e WORM:**

a. Habilite **Flash Cache**, se desejar.



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 desabilitar o Flash Cache após a implantação.

b. Escolha a velocidade de gravação **Normal** ou **Alta**, se desejar.

["Saiba mais sobre velocidade de gravação"](#).



Alta velocidade de gravação e uma unidade máxima de transmissão (MTU) maior de 8.896 bytes estão disponíveis por meio da opção de velocidade de gravação **Alta**. Além disso, a MTU mais alta de 8.896 exige 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, consulte ["Regras para VPC-1, VPC-2 e VPC-3"](#).

c. Ative o armazenamento WORM (escreva uma vez e leia muitas vezes), se desejar.

O WORM não pode ser habilitado se a hierarquização de dados estiver habilitada para as versões 9.7 e anteriores do Cloud Volumes ONTAP. A reversão ou o downgrade para o Cloud Volumes ONTAP 9.8 é bloqueado após a ativação do WORM e da hierarquização.

["Saiba mais sobre o armazenamento WORM"](#).

a. Se você ativar o armazenamento WORM, selecione o período de retenção.

13. **Classificação de dados em camadas no Google Cloud Platform:** escolha se deseja habilitar a classificação de dados em camadas no agregado inicial, escolha 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 (necessária para o Cloud Volumes ONTAP 9.7 ou posterior) ou selecione uma conta do Google Cloud (necessária para o Cloud Volumes ONTAP 9.6).

Observe o seguinte:

- O Console define a conta de serviço na instância do Cloud Volumes ONTAP. Esta conta de serviço fornece permissões para hierarquização de dados para um bucket do Google Cloud Storage. Certifique-se de adicionar a conta de serviço do agente do Console como um usuário da conta de serviço em camadas; caso contrário, você não poderá selecioná-la no Console.
- Para obter ajuda na adição de uma conta do Google Cloud, consulte ["Configurando e adicionando contas do Google Cloud para camadas de dados com 9.6"](#).
- Você pode escolher uma política específica de níveis de volume ao criar ou editar um volume.
- Se você desabilitar a hierarquização de dados, poderá habilitá-la em agregações subsequentes, mas precisará desligar o sistema e adicionar uma conta de serviço no console do Google Cloud.

["Saiba mais sobre camadas de dados"](#).

14. **Criar volume:** insira detalhes para o novo volume ou clique em **Ignorar**.

["Saiba mais sobre os protocolos e versões de clientes suportados"](#).

Alguns campos nesta página são autoexplicativos. A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Tamanho	O tamanho máximo que você pode inserir depende muito se você habilita o provisionamento fino, que permite criar um volume maior que o armazenamento físico disponível atualmente.
Controle de acesso (somente para NFS)	Uma política de exportação define os clientes na sub-rede que podem acessar o volume. Por padrão, o Console insere um valor que fornece acesso a todas as instâncias na sub-rede.

Campo	Descrição
Permissões e usuários/grupos (somente para CIFS)	Esses campos permitem que você controle o nível de acesso a um compartilhamento para usuários e grupos (também chamados de listas de controle de acesso ou ACLs). Você pode especificar usuários ou grupos locais ou de domínio do Windows, ou usuários ou grupos do UNIX. Se você especificar um nome de usuário de domínio do Windows, deverá incluir o domínio do usuário usando o formato domínio\nome de usuário.
Política de Snapshot	Uma política de cópia de instantâneo especifica a frequência e o número de cópias de instantâneo do NetApp criadas automaticamente. Uma cópia do NetApp Snapshot é uma imagem do sistema de arquivos de um momento específico que não tem impacto no desempenho e requer armazenamento mínimo. Você pode escolher a política padrão ou nenhuma. Você pode escolher nenhum para dados transitórios: por exemplo, tempdb para Microsoft SQL Server.
Opções avançadas (somente para NFS)	Selecione uma versão do NFS para o volume: NFSv3 ou NFSv4.
Grupo iniciador e IQN (somente para iSCSI)	Os destinos de armazenamento iSCSI são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Os grupos de iniciadores são tabelas de nomes de nós de host iSCSI e controlam quais iniciadores têm acesso a quais LUNs. Os destinos iSCSI se conectam à rede por meio de adaptadores de rede Ethernet padrão (NICs), placas de mecanismo de descarregamento TCP (TOE) com iniciadores de software, adaptadores de rede convergentes (CNAs) ou adaptadores de bust de host dedicados (HBAs) e são identificados por nomes qualificados iSCSI (IQNs). Quando você cria um volume iSCSI, o Console cria automaticamente um LUN para você. Simplificamos criando apenas um LUN por volume, portanto não há gerenciamento envolvido. Depois de criar o volume, "use o IQN para conectar-se ao LUN de seus hosts" .

A imagem a seguir mostra a primeira página do assistente de criação de volume:

Volume Details & Protection

Volume Name: ABDcv5689

Storage VM (SVM): svm_c...CVO1

Volume Size: 100

Unit: GiB

Snapshot Policy: default

default policy

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 ao qual o servidor CIFS se juntará. Se você estiver configurando o Google Managed Active Directory, o AD poderá ser acessado por padrão com o endereço IP 169.254.169.254.
Domínio do Active Directory para ingressar	O FQDN do domínio do Active Directory (AD) ao qual você deseja que o servidor CIFS ingresse.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com privilégios suficientes para adicionar computadores à Unidade Organizacional (UO) especificada dentro do domínio do AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio do AD.
Unidade Organizacional	A unidade organizacional dentro do domínio do AD a ser associada ao servidor CIFS. O padrão é CN=Computadores. Para configurar o Google Managed Microsoft AD como o servidor AD para o Cloud Volumes ONTAP, insira OU=Computers,OU=Cloud neste campo. https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units ["Documentação do Google Cloud: Unidades organizacionais no Google Managed Microsoft AD"]
Domínio DNS	O domínio DNS para a máquina virtual de armazenamento (SVM) do Cloud Volumes ONTAP . Na maioria dos casos, o domínio é o mesmo que o domínio do AD.
Servidor NTP	Selecione Usar domínio do Active Directory para configurar um servidor NTP usando o DNS do Active Directory. Se você precisar configurar um servidor NTP usando um endereço diferente, use a API. Para obter informações, consulte o " Documentação de automação do NetApp Console " para mais detalhes. Observe que você só pode configurar um servidor NTP ao criar um servidor CIFS. Não é configurável depois de criar o servidor CIFS.

16. **Perfil de uso, tipo de disco e política de camadas:** escolha se deseja habilitar recursos de eficiência de armazenamento e alterar a política de camadas de volume, se necessário.

Para mais informações, consulte "[Escolha um perfil de uso de volume](#)" , "[Visão geral da hierarquização de dados](#)" , e "[KB: Quais recursos de eficiência de armazenamento em linha são suportados pelo CVO?](#)"

17. **Revisar e aprovar:** revise e confirme suas seleções.
- Revise os detalhes sobre a configuração.
 - Clique em **Mais informações** para revisar detalhes sobre o suporte e os recursos do Google Cloud que o Console comprará.
 - Selecione as caixas de seleção **Eu entendo...**
 - Clique em **Ir**.

Resultado

O Console implanta o sistema Cloud Volumes ONTAP . Você pode acompanhar o progresso na página **Auditoria**.

Se você tiver algum problema ao implantar o sistema Cloud Volumes ONTAP , revise a mensagem de falha. Você também pode selecionar o sistema e clicar em **Recriar ambiente**.

Para obter ajuda adicional, acesse "[Suporte NetApp Cloud Volumes ONTAP](#)".

Depois que você terminar

- Se você provisionou um compartilhamento CIFS, conceda aos usuários ou grupos permissões para os arquivos e pastas e verifique se esses usuários podem acessar o compartilhamento e criar um arquivo.
- Se você quiser aplicar cotas aos volumes, use o ONTAP System Manager ou o ONTAP CLI.

As cotas permitem que você restrinja ou rastreie o espaço em disco e o número de arquivos usados por um usuário, grupo ou qtree.

Inicie um par de HA no Google Cloud

Crie um sistema no Console para iniciar o Cloud Volumes ONTAP no Google Cloud.

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique em **Armazenamento > Sistema** 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, opcionalmente selecione uma conta de serviço, opcionalmente adicione rótulos e, em seguida, especifique as credenciais.

A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Nome do sistema	O Console usa o nome do sistema para nomear o sistema Cloud Volumes ONTAP e a instância da 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 o " Camadas de nuvem da NetApp " ou " Backup e Recuperação " serviços, você precisa habilitar a opção Conta de serviço e então selecionar a Conta de serviço que tem a função de administrador de armazenamento predefinida.
Adicionar rótulos	Os rótulos são metadados para seus recursos do Google Cloud. O Console adiciona os rótulos ao sistema Cloud Volumes ONTAP e aos recursos do Google Cloud associados ao sistema. Você pode adicionar até quatro rótulos na interface do usuário ao criar um sistema e depois adicionar mais depois que ele for criado. Observe que a API não limita você a quatro rótulos ao criar um sistema. Para obter informações sobre rótulos, consulte " Documentação do Google Cloud: Rotulagem de recursos ".
Nome de usuário e senha	Estas são as credenciais para a conta de administrador do cluster Cloud Volumes ONTAP . Você pode usar essas credenciais para se conectar ao Cloud Volumes ONTAP por meio do ONTAP System Manager ou do ONTAP CLI. Mantenha o nome de usuário padrão <i>admin</i> ou altere-o para um nome de usuário personalizado.

Campo	Descrição
Editar Projeto	Selecione o projeto onde você deseja que o Cloud Volumes ONTAP resida. O projeto padrão é o projeto do Console. Se você não vir nenhum projeto adicional na lista suspensa, significa que você ainda não associou a conta de serviço a outros projetos. Acesse o console do Google Cloud, abra o serviço IAM e selecione o projeto. Adicione a conta de serviço com a função que você usa para o Console nesse projeto. Você precisará repetir esta etapa para cada projeto.  Esta é a conta de serviço que você configurou para o Console, "conforme descrito nesta página". Clique em Adicionar assinatura para associar as credenciais selecionadas a uma assinatura. Para criar um sistema Cloud Volumes ONTAP com pagamento conforme o uso, você precisa selecionar um projeto do Google Cloud associado a uma assinatura do Cloud Volumes ONTAP no Google Cloud Marketplace. Consulte "Associando uma assinatura do marketplace às credenciais do Google Cloud".

5. **Serviços:** Selecione os serviços que você deseja usar neste sistema. Para selecionar Backup e Recuperação ou usar o NetApp Cloud Tiering, você deve ter especificado a Conta de Serviço na etapa 3.



Se você quiser utilizar WORM e camadas de dados, desabilite o Backup e Recuperação e implante um sistema Cloud Volumes ONTAP com versão 9.8 ou superior.

6. **Modelos de implantação de HA:** escolha várias zonas (recomendado) ou uma única zona para a configuração de HA. Em seguida, selecione uma região e zonas.

["Saiba mais sobre modelos de implantação de HA"](#).

7. **Conectividade:** 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 deixar o Console gerar a política de firewall para você, precisará escolher como permitirá o tráfego: - Se você escolher Somente VPC selecionada, o filtro de origem para tráfego de entrada será o intervalo de sub-rede da VPC selecionada e o intervalo de sub-rede da VPC onde o agente do Console reside. Esta é a opção recomendada. - Se você escolher Todas as VPCs, o filtro de origem para o tráfego de entrada será o intervalo de IP 0.0.0.0/0.

Campo	Descrição
Use existente	Se você usar uma política de firewall existente, certifique-se de que ela inclua as regras necessárias. "Saiba mais sobre as regras de firewall para o Cloud Volumes ONTAP" .

8. **Métodos de cobrança e conta NSS:** especifique qual opção de cobrança você gostaria de usar com este sistema e, em seguida, especifique uma conta do site de suporte da NetApp .

- ["Saiba mais sobre as opções de licenciamento do Cloud Volumes ONTAP"](#) .
- ["Aprenda como configurar o licenciamento"](#) .

9. **Pacotes pré-configurados:** selecione um dos pacotes para implantar rapidamente um sistema Cloud Volumes ONTAP ou clique em **Criar minha própria configuração**.

Se você escolher um dos pacotes, precisará apenas especificar um volume e depois revisar e aprovar a configuração.

10. **Licenciamento:** Altere a versão do Cloud Volumes ONTAP conforme necessário e selecione um tipo de máquina.



Se uma versão mais recente de Release Candidate, Disponibilidade Geral ou patch estiver disponível para a versão selecionada, o Console atualizará o sistema para essa versão ao criá-la. Por exemplo, a atualização ocorre se você selecionar Cloud Volumes ONTAP 9.13.1 e 9.13.1 P4 estiver disponível. A atualização não ocorre de uma versão para outra, por exemplo, da 9.13 para a 9.14.

11. **Recursos de armazenamento subjacentes:** escolha as 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 que o Console cria quando você usa a opção de provisionamento simples. Você pode criar agregados que usam um tamanho de disco diferente usando a opção de alocação avançada.

Para obter ajuda na escolha do tipo e tamanho do disco, consulte ["Dimensione seu sistema no Google Cloud"](#) .

12. **Flash Cache, Velocidade de Gravação e WORM:**

a. Habilite **Flash Cache**, se desejar.



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 desabilitar o Flash Cache após a implantação.

b. Escolha a velocidade de gravação **Normal** ou **Alta**, se desejar.

["Saiba mais sobre velocidade de gravação"](#) .



Alta velocidade de gravação e uma unidade máxima de transmissão (MTU) maior de 8.896 bytes estão disponíveis por meio da opção de velocidade de gravação **Alta** com os tipos de instância n2-standard-16, n2-standard-32, n2-standard-48 e n2-standard-64. Além disso, a MTU mais alta de 8.896 exige a seleção de VPC-1, VPC-2 e VPC-3 para a implantação. Alta velocidade de gravação e uma MTU de 8.896 dependem do recurso e não podem ser desabilitadas individualmente em uma instância configurada. Para obter mais informações sobre VPC-1, VPC-2 e VPC-3, consulte ["Regras para VPC-1, VPC-2 e VPC-3"](#) .

c. Ative o armazenamento WORM (escreva uma vez e leia muitas vezes), se desejar.

O WORM não pode ser habilitado se a hierarquização de dados estiver habilitada para as versões 9.7 e anteriores do Cloud Volumes ONTAP . A reversão ou o downgrade para o Cloud Volumes ONTAP 9.8 é bloqueado após a ativação do WORM e da hierarquização.

["Saiba mais sobre o armazenamento WORM"](#) .

a. Se você ativar o armazenamento WORM, selecione o período de retenção.

13. **Classificação de dados no Google Cloud:** escolha se deseja habilitar a classificação de dados no agregado inicial, escolha uma classe de armazenamento para os dados em camadas e, em seguida, selecione uma conta de serviço que tenha a função predefinida de Administrador de armazenamento.

Observe o seguinte:

- O Console define a conta de serviço na instância do Cloud Volumes ONTAP . Esta conta de serviço fornece permissões para hierarquização de dados para um bucket do Google Cloud Storage. Certifique-se de adicionar a conta de serviço do agente do Console como um usuário da conta de serviço em camadas; caso contrário, você não poderá selecioná-la no Console.
- Você pode escolher uma política específica de níveis de volume ao criar ou editar um volume.
- Se você desabilitar a hierarquização de dados, poderá habilitá-la em agregações subsequentes, mas precisará desligar o sistema e adicionar uma conta de serviço no console do Google Cloud.

["Saiba mais sobre camadas de dados"](#) .

14. **Criar volume:** insira detalhes para o novo volume ou clique em **Ignorar**.

["Saiba mais sobre os protocolos e versões de clientes suportados"](#) .

Alguns campos nesta página são autoexplicativos. A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Tamanho	O tamanho máximo que você pode inserir depende muito se você habilita o provisionamento fino, que permite criar um volume maior que o armazenamento físico disponível atualmente.
Controle de acesso (somente para NFS)	Uma política de exportação define os clientes na sub-rede que podem acessar o volume. Por padrão, o Console insere um valor que fornece acesso a todas as instâncias na sub-rede.

Campo	Descrição
Permissões e usuários/grupos (somente para CIFS)	Esses campos permitem que você controle o nível de acesso a um compartilhamento para usuários e grupos (também chamados de listas de controle de acesso ou ACLs). Você pode especificar usuários ou grupos locais ou de domínio do Windows, ou usuários ou grupos do UNIX. Se você especificar um nome de usuário de domínio do Windows, deverá incluir o domínio do usuário usando o formato domínio\nome de usuário.
Política de Snapshot	Uma política de cópia de instantâneo especifica a frequência e o número de cópias de instantâneo do NetApp criadas automaticamente. Uma cópia do NetApp Snapshot é uma imagem do sistema de arquivos de um momento específico que não tem impacto no desempenho e requer armazenamento mínimo. Você pode escolher a política padrão ou nenhuma. Você pode escolher nenhum para dados transitórios: por exemplo, tempdb para Microsoft SQL Server.
Opções avançadas (somente para NFS)	Selecione uma versão do NFS para o volume: NFSv3 ou NFSv4.
Grupo iniciador e IQN (somente para iSCSI)	Os destinos de armazenamento iSCSI são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Os grupos de iniciadores são tabelas de nomes de nós de host iSCSI e controlam quais iniciadores têm acesso a quais LUNs. Os destinos iSCSI se conectam à rede por meio de adaptadores de rede Ethernet padrão (NICs), placas de mecanismo de descarregamento TCP (TOE) com iniciadores de software, adaptadores de rede convergentes (CNAs) ou adaptadores de bust de host dedicados (HBAs) e são identificados por nomes qualificados iSCSI (IQNs). Quando você cria um volume iSCSI, o Console cria automaticamente um LUN para você. Simplificamos criando apenas um LUN por volume, portanto não há gerenciamento envolvido. Depois de criar o volume, "use o IQN para conectar-se ao LUN de seus hosts" .

A imagem a seguir mostra a primeira página do assistente de criação de volume:

The screenshot displays the 'Volume Details & Protection' configuration interface. It includes the following fields and options:

- Volume Name:** A text input field containing 'ABDcv5689'.
- Storage VM (SVM):** A dropdown menu showing 'svm_c...CVO1'.
- Volume Size:** A text input field containing '100'.
- Unit:** A dropdown menu showing 'GiB'.
- Snapshot Policy:** A dropdown menu showing 'default'.
- default policy:** A label with an information icon (i) located below the Snapshot Policy dropdown.

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 ao qual o servidor CIFS se juntará. Se você estiver configurando o Google Managed Active Directory, o AD poderá ser acessado por padrão com o endereço IP 169.254.169.254.
Domínio do Active Directory para ingressar	O FQDN do domínio do Active Directory (AD) ao qual você deseja que o servidor CIFS ingresse.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com privilégios suficientes para adicionar computadores à Unidade Organizacional (UO) especificada dentro do domínio do AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio do AD.
Unidade Organizacional	A unidade organizacional dentro do domínio do AD a ser associada ao servidor CIFS. O padrão é CN=Computadores. Para configurar o Google Managed Microsoft AD como o servidor AD para o Cloud Volumes ONTAP, insira OU=Computers,OU=Cloud neste campo. https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units ["Documentação do Google Cloud: Unidades organizacionais no Google Managed Microsoft AD"^]
Domínio DNS	O domínio DNS para a máquina virtual de armazenamento (SVM) do Cloud Volumes ONTAP . Na maioria dos casos, o domínio é o mesmo que o domínio do AD.
Servidor NTP	Selecione Usar domínio do Active Directory para configurar um servidor NTP usando o DNS do Active Directory. Se você precisar configurar um servidor NTP usando um endereço diferente, use a API. Consulte o "Documentação de automação do NetApp Console" para mais detalhes. Observe que você só pode configurar um servidor NTP ao criar um servidor CIFS. Não é configurável depois de criar o servidor CIFS.

16. **Perfil de uso, tipo de disco e política de camadas:** escolha se deseja habilitar recursos de eficiência de armazenamento e alterar a política de camadas de volume, se necessário.

Para mais informações, consulte ["Escolha um perfil de uso de volume"](#) , ["Visão geral da hierarquização de dados"](#) , e ["KB: Quais recursos de eficiência de armazenamento em linha são suportados pelo CVO?"](#)

17. **Revisar e aprovar:** revise e confirme suas seleções.
- Revise os detalhes sobre a configuração.
 - Clique em **Mais informações** para revisar detalhes sobre o suporte e os recursos do Google Cloud que o Console comprará.
 - Selecione as caixas de seleção **Eu entendo...**
 - Clique em **Ir**.

Resultado

O Console implanta o sistema Cloud Volumes ONTAP . Você pode acompanhar o progresso na página **Auditoria**.

Se você tiver algum problema ao implantar o sistema Cloud Volumes ONTAP , revise a mensagem de falha. Você também pode selecionar o sistema e clicar em **Recriar ambiente**.

Para obter ajuda adicional, acesse "[Suporte NetApp Cloud Volumes ONTAP](#)".

Depois que você terminar

- Se você provisionou um compartilhamento CIFS, conceda aos usuários ou grupos permissões para os arquivos e pastas e verifique se esses usuários podem acessar o compartilhamento e criar um arquivo.
- Se você quiser aplicar cotas aos volumes, use o ONTAP System Manager ou o ONTAP CLI.

As cotas permitem que você restrinja ou rastreie o espaço em disco e o número de arquivos usados por um usuário, grupo ou qtree.

Verificação de imagem da plataforma Google Cloud

Saiba como a imagem do Google Cloud é verificada no Cloud Volumes ONTAP

A verificação de imagem do Google Cloud está em conformidade com os requisitos de segurança aprimorados da NetApp . Foram feitas alterações no script que gera as imagens para assiná-las ao longo do caminho usando chaves privadas geradas especificamente para essa tarefa. Você pode verificar a integridade da imagem do Google Cloud usando o resumo assinado e o certificado público do Google Cloud, que podem ser baixados via "[NSS](#)" para um lançamento específico.



A verificação de imagens do Google Cloud é compatível com o software Cloud Volumes ONTAP versão 9.13.0 ou superior.

Converter imagem do Google Cloud para formato bruto para Cloud Volumes ONTAP

A imagem que está sendo usada para implantar novas instâncias, atualizações ou que está sendo usada em imagens existentes será compartilhada com os clientes por meio de "[o site de suporte da NetApp \(NSS\)](#)". O resumo assinado e os certificados estarão disponíveis para download no portal do NSS. Certifique-se de que você está baixando o resumo e os certificados para a versão correta correspondente à imagem compartilhada pelo Suporte da NetApp . Por exemplo, imagens 9.13.0 terão um resumo assinado 9.13.0 e certificados disponíveis no NSS.

Por que essa etapa é necessária?

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 para o formato disk.raw e salvar os resultados em um bucket de armazenamento no Google Cloud. O arquivo disk.raw é compactado em tar e gzip no processo.

A conta de usuário/serviço precisará de privilégios para executar o seguinte:

- Acesso ao bucket de armazenamento do Google
- Gravar no bucket do Google Storage

- Criar trabalhos de criação de nuvem (usados durante o processo de exportação)
- Acesso à imagem desejada
- Criar tarefas de exportação de imagem

Para verificar a imagem, ela deve ser convertida para o formato disk.raw e depois 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 gcloud compute images export](#)". Este comando pega a imagem fornecida e a converte em um arquivo disk.raw, que é tarado e compactado em gzip. O arquivo gerado é salvo na URL de destino e pode ser baixado para verificação.

O usuário/conta deve ter privilégios 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

```
$ 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 os arquivos compactados

```
# Extracting files from the digest  
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```



Para obter mais informações sobre como exportar uma imagem por meio do Google Cloud, consulte o ["Documento do Google Cloud sobre como exportar uma imagem"](#).

Verificação de assinatura de imagem

Verificação de assinatura de imagem do Google Cloud para Cloud Volumes ONTAP

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

A seguir, uma visão geral do processo de fluxo de trabalho de verificação de imagem assinada do Google Cloud.

- Do ["NSS"](#), baixe o arquivo do Google Cloud contendo 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

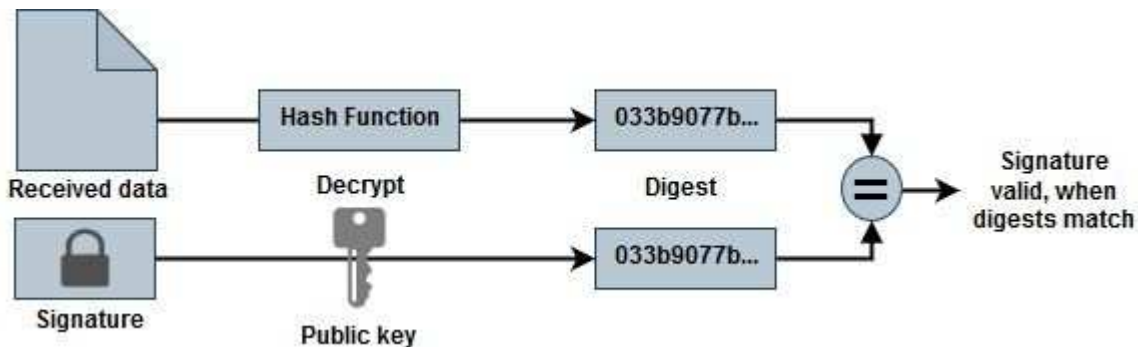
DOWNLOAD GCP-9-15-0P1_PKG.TAR.GZ [7.49 KB]

[View and download checksums](#)

DOWNLOAD AZURE-9-15-0P1_PKG.TAR.GZ [7.64 KB]

[View and download checksums](#)

- Baixe o arquivo disk.raw convertido
- Validar o certificado usando a cadeia de certificados
- Valide o resumo assinado usando o certificado que contém a chave pública
 - Descriptografe 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



Verifique o arquivo disk.raw da imagem do Google Cloud para o Cloud Volumes ONTAP usando OpenSSL

Você pode verificar o arquivo disk.raw baixado pelo Google Cloud em relação ao conteúdo do arquivo de resumo disponível por meio do "NSS" usando OpenSSL.



Os comandos OpenSSL para validar a imagem são compatíveis com máquinas Linux, macOS e Windows.

Passos

1. Verifique o certificado usando OpenSSL.

```
# 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 ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsp -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 ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocsp -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. Descriptografe a assinatura usando a chave pública extraída e verifique o conteúdo do arquivo disk.raw baixado.

Clique para exhibir

```
# 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 licenciamento baseado em capacidade para Cloud Volumes ONTAP

Gerencie suas licenças baseadas em capacidade no NetApp Console para garantir que sua conta NetApp tenha capacidade suficiente para seus sistemas Cloud Volumes ONTAP .

Licenças baseadas em capacidade permitem que você pague pelo Cloud Volumes ONTAP por TiB de capacidade.

Você pode gerenciar licenças do Cloud Volumes ONTAP baseadas em capacidade no NetApp Console.



Embora o uso real e a medição dos produtos e serviços gerenciados no Console sejam sempre calculados em GiB e TiB, os termos GB/GiB e TB/TiB são usados de forma intercambiável. Isso se reflete nas listagens do Cloud Marketplace, nas cotações de preços, nas descrições das listagens e em outras documentações de suporte.

["Saiba mais sobre as licenças do Cloud Volumes ONTAP"](#) .

Como as licenças são adicionadas ao NetApp Console

Após adquirir uma licença do seu representante de vendas da NetApp , a NetApp lhe enviará um e-mail com o número de série e detalhes adicionais do licenciamento.

Enquanto isso, o Console consulta automaticamente o serviço de licenciamento da NetApp para obter detalhes sobre as licenças associadas à sua conta do Site de Suporte da NetApp . Se não houver erros, ele adiciona as licenças.

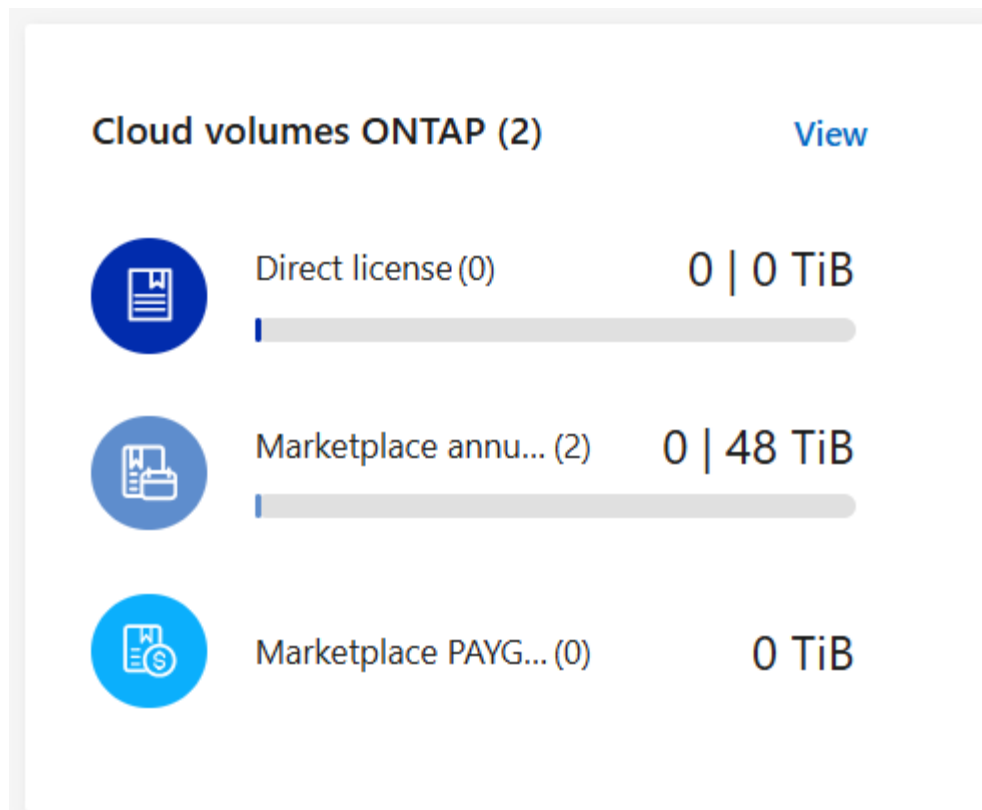
Se o Console não puder adicionar a licença, você precisará adicioná-la manualmente. Por exemplo, se o agente do Console estiver instalado em um local sem acesso à Internet, você precisará adicionar as licenças. ["Aprenda como adicionar licenças adquiridas à sua conta"](#) .

Visualize a capacidade consumida em sua conta

O Console mostra a capacidade total consumida na sua conta e a capacidade consumida pelo pacote de licenciamento. Isso pode ajudar você a entender como está sendo cobrado e se precisa comprar capacidade adicional.

Passos

1. No painel de navegação esquerdo, selecione **Administração > Licenças e assinaturas**.
2. Na guia **Visão geral**, o bloco Cloud Volumes ONTAP exibe a capacidade atual provisionada para sua conta.



- *Licença direta* é a capacidade total provisionada de todos os sistemas Cloud Volumes ONTAP na sua conta NetApp . A cobrança é baseada no tamanho provisionado de cada volume, independentemente do espaço local, usado, armazenado ou efetivo dentro do volume.
- *Contrato anual* é a capacidade total licenciada (traga sua própria licença (BYOL) ou contrato de marketplace) que você comprou da NetApp.
- *PAYGO* é a capacidade total provisionada usando assinaturas do marketplace em nuvem. O carregamento via PAYGO é usado somente se a capacidade consumida for maior que a capacidade licenciada ou se não houver licença BYOL disponível no Console.

3. Selecione **Exibir** para ver a capacidade consumida para cada um dos seus pacotes de licenciamento.
4. Selecione a aba **Licenças** para ver detalhes de cada licença de pacote que você comprou.

Para entender melhor as capacidades exibidas no pacote Essentials, você deve estar familiarizado com o funcionamento do carregamento. ["Saiba mais sobre a cobrança do pacote Essentials"](#) .

5. Selecione a aba **Assinaturas** para ver a capacidade consumida pelo modelo de consumo de licença. Esta aba inclui licenças PAYGO e de contrato anual.

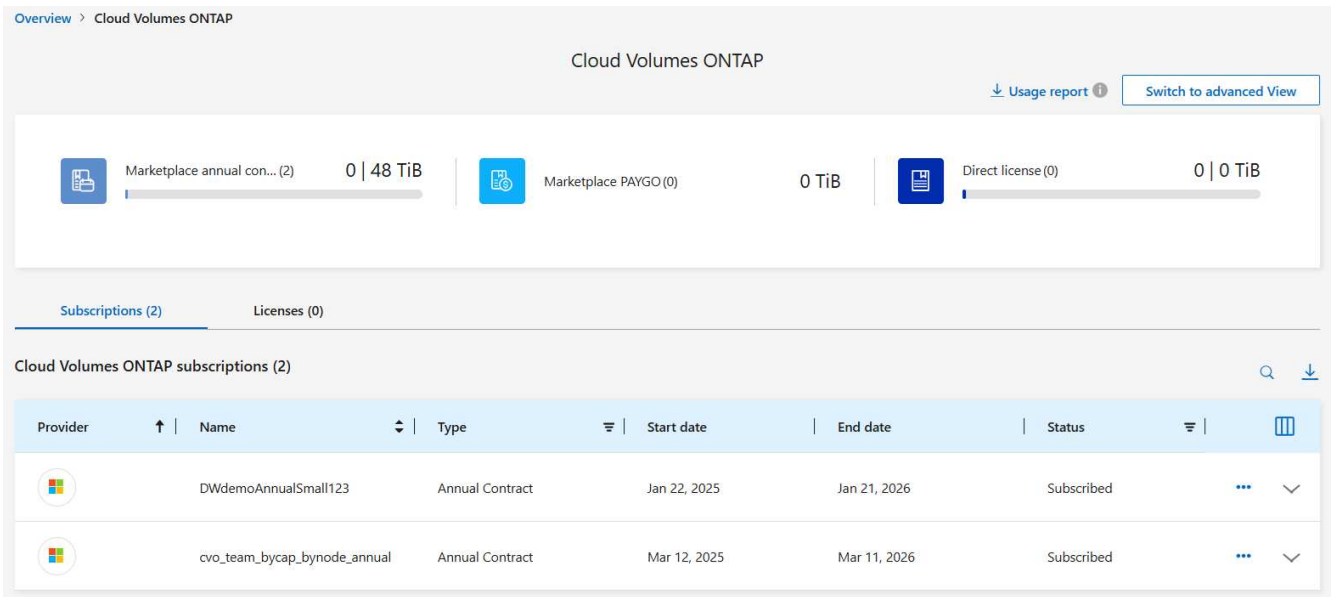
Você verá apenas as assinaturas associadas à organização que você está visualizando no momento.

6. Ao visualizar as informações sobre suas assinaturas, você pode interagir com os detalhes na tabela. Expanda uma linha para ver mais detalhes.
 - Selecione  para escolher quais colunas aparecem na tabela. Observe que as colunas Prazo e Renovação automática não aparecem por padrão. A coluna Renovação Automática exibe informações de renovação somente para contratos do Azure.

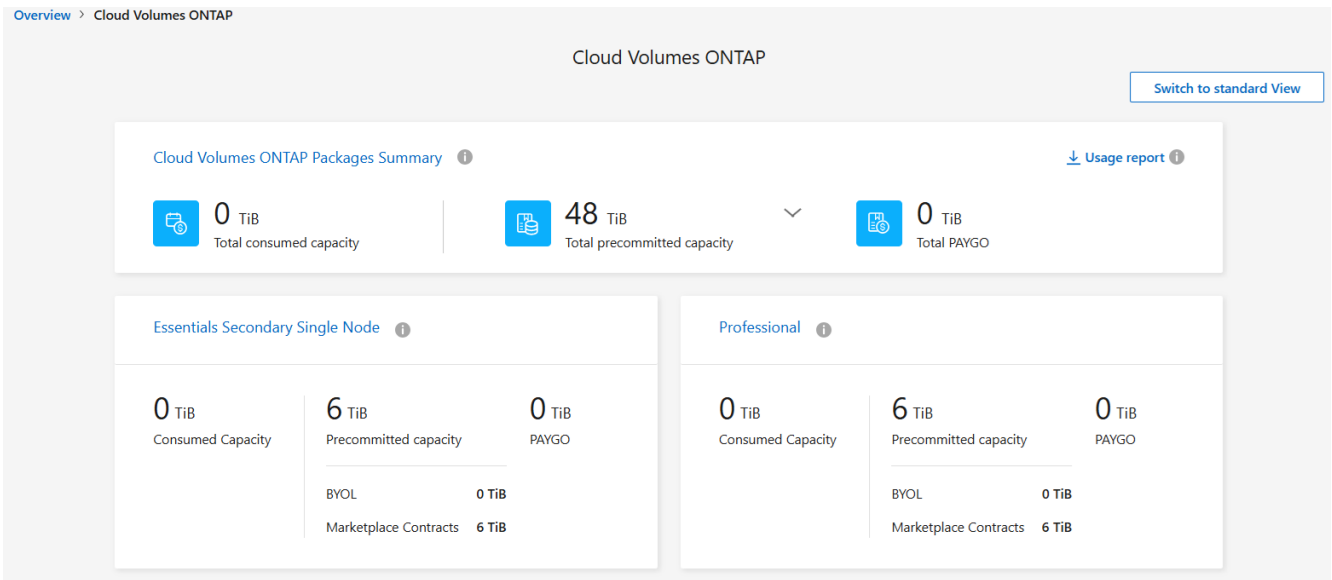
Visualizando detalhes do pacote

Você pode visualizar detalhes sobre a capacidade usada por pacote alternando para o modo legado na página Cloud Volumes ONTAP .

- 1. No painel de navegação esquerdo, selecione **Administração > Licenças e assinaturas**.
- 2. Na guia **Visão geral**, o bloco Cloud Volumes ONTAP exibe a capacidade atual provisionada para sua conta.
- 3. Selecione **Exibir** para ver a capacidade provisionada para cada um dos seus pacotes de licenciamento.
- 4. Selecione **Alternar para visualização avançada**.



- 5. Veja os detalhes do pacote que você deseja ver.



Alterar métodos de cobrança

O licenciamento baseado em capacidade está disponível na forma de um *pacote*. Ao criar um sistema Cloud Volumes ONTAP , você pode escolher entre vários pacotes de licenciamento com base nas necessidades do

seu negócio. Se suas necessidades mudarem depois de criar o sistema, você poderá 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

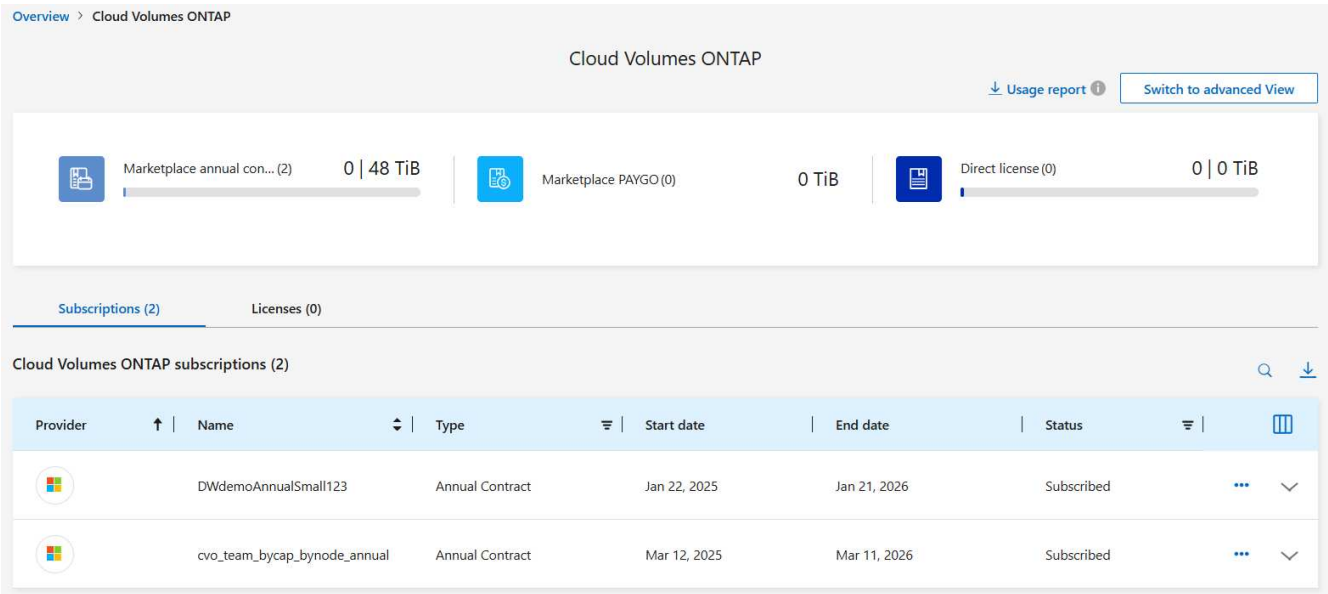
- Alterar o método de cobrança não afeta se você será cobrado por meio de uma licença adquirida da NetApp (BYOL) ou da assinatura pré-paga (PAYGO) do seu provedor de nuvem.

O Console sempre tenta cobrar primeiro uma licença. Se uma licença não estiver disponível, será cobrada uma assinatura do marketplace. Você não precisa converter uma assinatura BYOL em uma assinatura de mercado ou vice-versa.

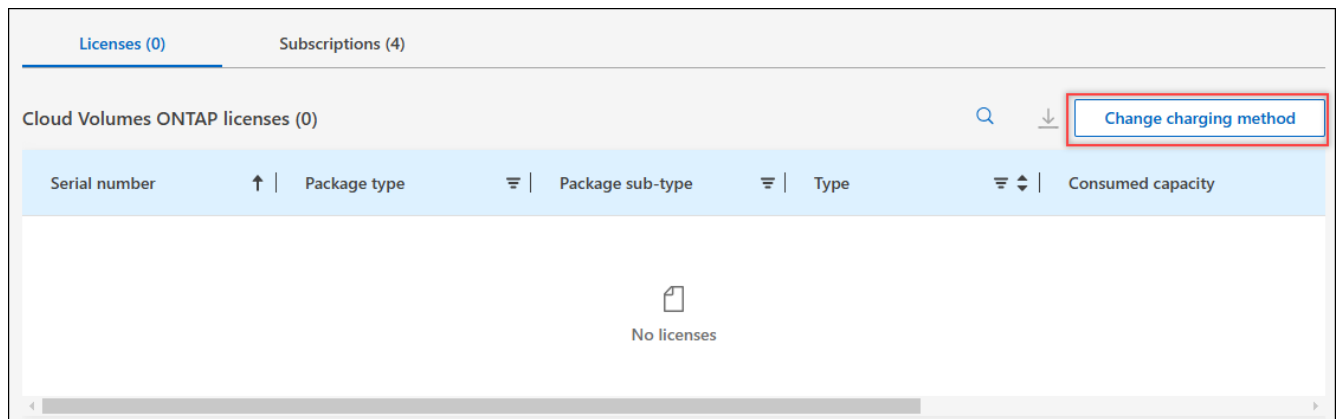
- Se você tiver uma oferta ou contrato privado do mercado do seu provedor de nuvem, mudar para um método de cobrança que não esteja incluído no seu contrato resultará em cobrança de BYOL (se você comprou uma licença da NetApp) ou PAYGO.

Passos

1. No painel de navegação esquerdo, selecione **Administração > Licenças e assinaturas**.
2. Selecione a aba **Visão geral**.
3. No bloco Cloud Volumes ONTAP , selecione **Exibir**.
4. Selecione **Alternar para visualização avançada**.



5. Role para baixo até a tabela **Licença baseada em capacidade** e selecione **Alterar método de cobrança**.



6. No pop-up **Alterar método de cobrança**, selecione um sistema Cloud Volumes ONTAP , escolha o novo método de cobrança e confirme que você entendeu que a alteração do tipo de pacote afetará as taxas de serviço.

7. Selecione **Alterar método de cobrança**.

Baixar relatórios de uso

Você pode baixar quatro relatórios de uso do Console. 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 para download capturam dados em um determinado 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 inclui as seguintes informações:
 - Capacidade total consumida
 - Capacidade pré-comprometida total
 - Capacidade total de BYOL
 - Capacidade total de contratos do Marketplace
 - Capacidade total do PAYGO
- *** Uso do pacote Cloud Volumes ONTAP *:** Este relatório inclui as seguintes informações para cada pacote:
 - Capacidade total consumida
 - Capacidade pré-comprometida total
 - Capacidade total de BYOL
 - Capacidade total de contratos do Marketplace
 - Capacidade total do PAYGO
- **Uso de VMs de armazenamento:** Este relatório mostra como a capacidade cobrada é dividida entre os sistemas Cloud Volumes ONTAP e as máquinas virtuais de armazenamento (SVMs). Essas informações

estão disponíveis somente no relatório. Ele contém as seguintes informações:

- ID e nome do sistema (aparece como UUID)
 - Nuvem
 - ID da conta NetApp
 - Configuração do sistema
 - Nome da SVM
 - Capacidade provisionada
 - Resumo da capacidade carregada
 - Termo de cobrança do Marketplace
 - Pacote ou recurso Cloud Volumes ONTAP
 - Nome da assinatura do SaaS Marketplace de cobrança
 - ID de assinatura do SaaS Marketplace de cobrança
 - Tipo de carga de trabalho
- **Uso de volumes:** Este relatório mostra como a capacidade cobrada é dividida por volumes em um sistema Cloud Volumes ONTAP . Essas informações não estão disponíveis em nenhuma tela do Console. Inclui as seguintes informações:
- ID e nome do sistema (aparece como UUID)
 - Nome da SVN
 - ID do volume
 - Tipo de volume
 - Capacidade de volume provisionado



Os volumes FlexClone não estão incluídos neste relatório porque esses tipos de volumes não geram cobranças.

Passos

1. No painel de navegação esquerdo, selecione **Administração > Licenças e assinaturas**.
2. Na guia **Visão geral**, selecione **Exibir** no bloco Cloud Volumes ONTAP .
3. Selecione **Relatório de uso**.

O relatório de uso é baixado.

4. Abra o arquivo baixado para acessar os relatórios.

Gerenciar assinaturas do Keystone para o Cloud Volumes ONTAP por meio do NetApp Console

Gerencie suas assinaturas Keystone a partir da BlueXP digital wallet habilitando assinaturas para uso com o Cloud Volumes ONTAP e solicitando alterações na capacidade comprometida para os níveis de serviço da sua assinatura. Solicitar capacidade adicional para um nível de serviço fornece mais armazenamento para clusters ONTAP locais ou para sistemas Cloud Volumes ONTAP .

O NetApp Keystone é um serviço flexível baseado em assinatura, com pagamento conforme o crescimento, que oferece uma experiência de nuvem híbrida para clientes que preferem OpEx a CapEx ou leasing.

["Saiba mais sobre a Keystone"](#)

Autorize sua conta

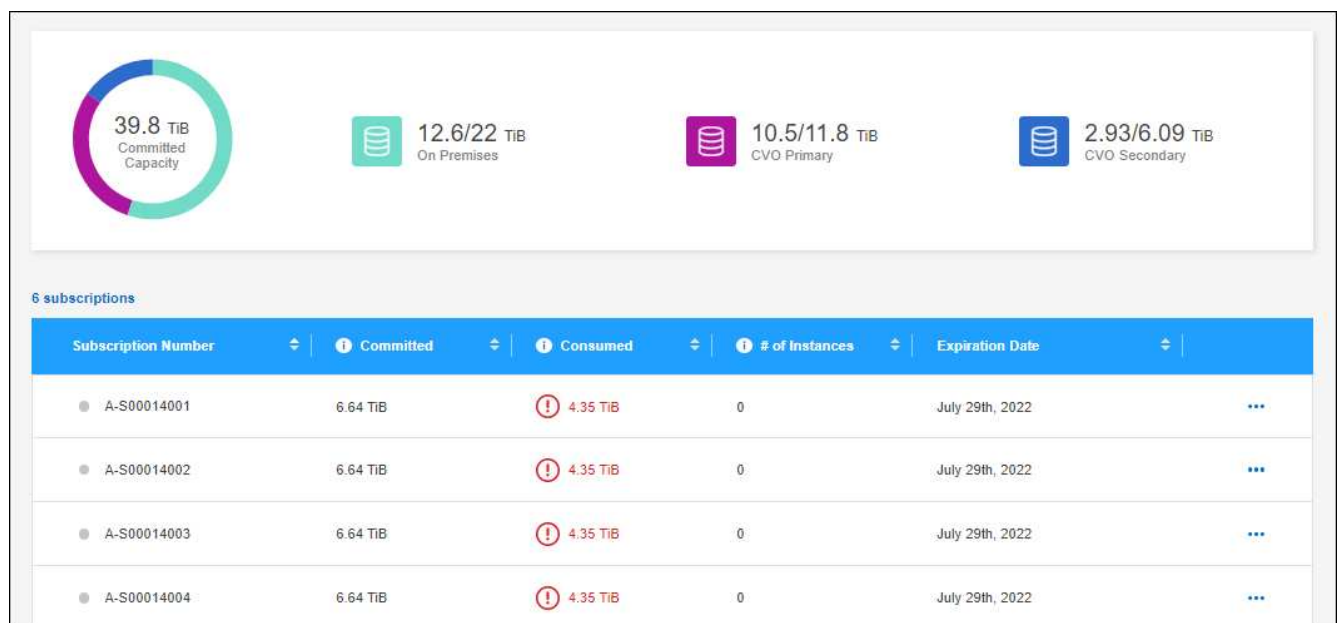
Antes de poder usar e gerenciar assinaturas do Keystone no BlueXP, você precisa entrar em contato com a NetApp para autorizar sua conta de usuário do BlueXP com suas assinaturas do Keystone.

Passos

1. No menu de navegação do BlueXP, selecione **Governança > Carteira digital**.
2. Selecione * Assinaturas 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 sua solicitação autorizando sua conta de usuário a acessar as assinaturas.

4. Volte para a aba * Assinaturas Keystone * para visualizar suas assinaturas.



Vincular uma assinatura

Depois que a NetApp autorizar sua conta, você poderá vincular assinaturas do Keystone para uso com o Cloud Volumes ONTAP. Esta ação permite que os usuários selecionem a assinatura como método de cobrança para novos sistemas Cloud Volumes ONTAP.

Passos

1. No menu de navegação do BlueXP, selecione **Governança > Carteira digital**.
2. Selecione * Assinaturas Keystone *.
3. Para a assinatura que você deseja vincular, clique em ... 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	View detail and edit
A-S00014003	6.64 TiB	4.35 TiB	0	July 29th, 2022	Link

Resultado

A assinatura agora está vinculada à sua organização ou conta BlueXP e disponível para seleção ao criar um ambiente de trabalho do Cloud Volumes ONTAP .

Solicitar capacidade mais ou menos comprometida

Se quiser alterar a capacidade comprometida para os níveis de serviço da sua assinatura, você pode enviar uma solicitação à NetApp diretamente do BlueXP. Solicitar capacidade adicional para um nível de serviço fornece mais armazenamento para clusters locais ou para sistemas Cloud Volumes ONTAP .

Passos

1. No menu de navegação do BlueXP , selecione **Governança > Carteira digital**.
2. Selecione * Assinaturas Keystone *.
3. Para a assinatura que você deseja ajustar a capacidade, clique em ... 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	Enter amount TiB
Premium	0.977 TiB	0.488 TiB	Enter amount TiB
Performance	0 TiB	0 TiB	Enter amount TiB
Standard	0.732 TiB	0.439 TiB	Enter amount TiB
Value	0.977 TiB	 0.879 TiB	Enter amount TiB
Data Tiering	0 TiB	0 TiB	Enter amount TiB
CVO Primary	1.96 TiB	 1.76 TiB	3 TiB
CVO Secondary	1.02 TiB	0.488 TiB	Enter amount TiB

Additional Information

Is there anything else we should know about your request?
Please be as descriptive as possible.

Submit

Cancel

5. Role para baixo, insira quaisquer detalhes adicionais para a solicitação e clique em **Enviar**.

Resultado

Sua solicitação cria um tíquete no sistema da NetApp para processamento.

Monitorar o uso

O painel do BlueXP digital advisor permite monitorar o uso da assinatura do Keystone e gerar relatórios.

["Saiba mais sobre o monitoramento do uso da assinatura"](#)

Desvincular uma assinatura

Se você não quiser mais usar uma assinatura Keystone com o BlueXP, você pode desvincular a assinatura. Observe que você só pode desvincular uma assinatura que não esteja vinculada a uma assinatura existente do Cloud Volumes ONTAP .

Passos

1. No menu de navegação do BlueXP , selecione **Governança > Carteira digital**.
2. Selecione * Keystone*.
3. Para a assinatura que você deseja desvincular, clique em **...** e selecione **Desvincular**.

Resultado

A assinatura é desvinculada da sua organização ou conta BlueXP e não está mais disponível para seleção ao criar um ambiente de trabalho do Cloud Volumes ONTAP .

Gerenciar licenciamento baseado em nó para Cloud Volumes ONTAP

Gerencie licenças baseadas em nós no NetApp Console 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 estão disponíveis para novos clientes):

- Licenças BYOL (Traga sua própria licença) adquiridas da NetApp
- Assinaturas de pagamento por hora (PAYGO) do marketplace do seu provedor de nuvem

Você pode gerenciar licenças do Cloud Volumes ONTAP baseadas em nós no NetApp Console.

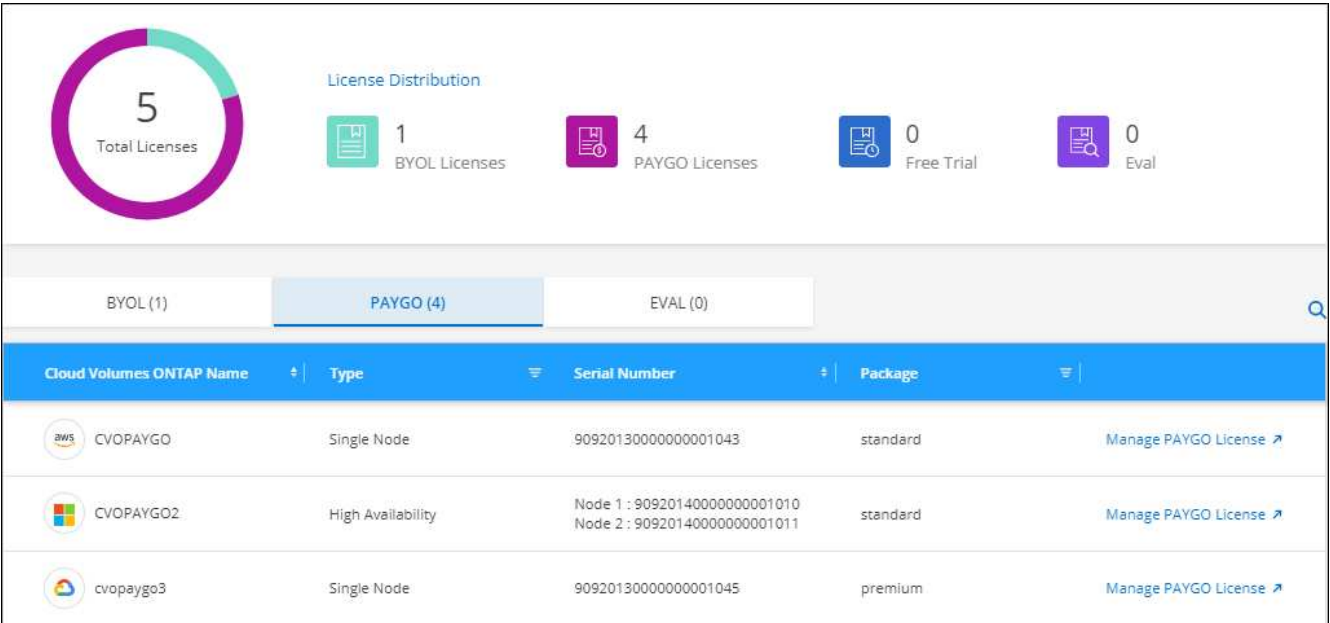
["Saiba mais sobre as licenças do Cloud Volumes ONTAP"](#) .

Gerenciar licenças PAYGO

O menu Licenças e assinaturas permite que você visualize 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 painel de navegação esquerdo, selecione **Administração > Licenças e assinaturas**.
2. Selecione a aba **Visão geral**.
3. No bloco Cloud Volumes ONTAP , selecione **Exibir**.
4. Selecione **Licenças baseadas em nós** no menu suspenso.
5. Clique em **PAYGO**.
6. Veja detalhes na tabela sobre cada uma das suas licenças PAYGO.



7. Se necessário, clique em **Gerenciar licença PAYGO** para alterar a licença PAYGO ou para alterar o tipo

de instância.

Gerenciar licenças BYOL

Gerencie licenças que você comprou diretamente da NetApp adicionando e removendo licenças de sistema e licenças de capacidade extra.



A NetApp restringiu a compra, extensão e renovação de licenças BYOL. Para obter mais informações, consulte ["Disponibilidade restrita de licenciamento BYOL para Cloud Volumes ONTAP"](#).

Adicionar licenças não atribuídas

Adicione uma licença baseada em nó ao Console para que você possa selecionar a licença ao criar um novo sistema Cloud Volumes ONTAP. O Console identifica essas licenças como *não atribuídas*.

Passos

1. No painel de navegação esquerdo, selecione **Administração > Licenças e assinaturas**.
2. Selecione a aba **Visão geral**.
3. No bloco Cloud Volumes ONTAP, selecione **Exibir**.
4. Selecione **Licenças baseadas em nós** no menu suspenso.
5. Clique em **Não atribuído**.
6. Clique em **Adicionar licenças não atribuídas**.
7. Digite o número de série da licença ou carregue o arquivo de licença.

Se você ainda não tiver o arquivo de licença, consulte a seção abaixo.

8. Clique em **Adicionar licença**.

Resultado

O Console adiciona a licença. A licença será identificada como não atribuída até que você a associe a um novo sistema Cloud Volumes ONTAP. Depois disso, a licença é movida para a aba **BYOL** em **Licenças e assinaturas**.

Trocar licenças baseadas em nós não atribuídas

Se você tiver uma licença baseada em nó não atribuída para o Cloud Volumes ONTAP que não tenha usado, poderá trocá-la convertendo-a em uma licença do NetApp Backup and Recovery, uma licença do NetApp Data Classification ou uma licença do NetApp Cloud Tiering.

A troca da licença revoga a licença do Cloud Volumes ONTAP e cria uma licença equivalente em dólares para o serviço:

- O licenciamento para um par Cloud Volumes ONTAP HA é convertido em uma licença direta de 51 TiB
- O licenciamento de um único nó do Cloud Volumes ONTAP é convertido em uma licença direta de 32 TiB

A licença convertida tem a mesma data de expiração que a licença do Cloud Volumes ONTAP.

["Veja o passo a passo de como trocar licenças baseadas em nós."](#)

Passos

1. No painel de navegação esquerdo, selecione **Administração > Licenças e assinaturas**.
2. Selecione a aba **Visão geral**.
3. No bloco Cloud Volumes ONTAP , selecione **Exibir**.
4. Selecione **Licenças baseadas em nós** no menu suspenso.
5. Clique em **Não atribuído**.
6. Clique em **Trocar Licença**.

BYOL (14)	Eval (2)	Unassigned (3)	PAYGO (6)	 Add Unassigned Licenses		
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		...

7. Selecione o serviço com o qual você gostaria de trocar a licença.
8. Se solicitado, selecione uma licença adicional para o par HA.
9. Leia o consentimento legal e clique em **Concordo**.

Resultado

O Console converte a licença não atribuída para o serviço que você selecionou. Você pode visualizar a nova licença na aba **Licenças de Serviços de Dados**.

Obter um arquivo de licença do sistema

Na maioria dos casos, o Console pode obter automaticamente seu arquivo de licença usando sua conta do Site de Suporte da NetApp . Mas se isso não for possível, você precisará carregar manualmente o arquivo de licença. Se você não tiver o arquivo de licença, poderá obtê-lo em netapp.com.

Passos

1. Vá para o "[Gerador de arquivo de licença NetApp](#)" e faça login usando suas credenciais do site de suporte da NetApp .
2. Digite sua senha, escolha seu produto, insira o número de série, confirme que você leu e aceitou a política de privacidade e 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	Ben
Last Name	
Company	Network Appliance, Inc
Email Address	
Username	

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

☐ I have read NetApp's new **Global Data** may use my personal data.

3. Escolha se deseja receber o arquivo JSON serialnumber.NLF por e-mail ou download direto.

Atualizar uma licença do sistema

Quando você renova uma assinatura BYOL entrando em contato com um representante da NetApp , o Console obtém automaticamente a nova licença da NetApp e a instala no sistema Cloud Volumes ONTAP . Se o Console não conseguir acessar o arquivo de licença pela conexão segura com a Internet, você poderá obter o arquivo e carregá-lo manualmente.

Passos

1. No painel de navegação esquerdo, selecione **Administração > Licenças e assinaturas**.
2. Selecione a aba **Visão geral**.
3. No bloco Cloud Volumes ONTAP , selecione **Exibir**.
4. Selecione **Licenças baseadas em nós** no menu suspenso.
5. Na guia **BYOL**, expanda os detalhes de um sistema Cloud Volumes ONTAP .
6. Clique no menu de ação ao lado da licença do sistema e selecione **Atualizar licença**.
7. Carregue o arquivo de licença (ou arquivos se você tiver um par HA).
8. Clique em **Atualizar licença**.

Resultado

O Console atualiza a licença no sistema Cloud Volumes ONTAP .

Gerenciar licenças de capacidade extra

Você pode adquirir licenças de capacidade extra para um sistema Cloud Volumes ONTAP BYOL para alocar mais do que os 368 TiB de capacidade fornecidos 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 adquirir para um único sistema de nó ou par de HA é ilimitado.

Adicionar licenças de capacidade

Adquira uma licença de capacidade extra entrando em contato conosco pelo ícone de bate-papo no canto inferior direito do Console. Depois de comprar a licença, você pode aplicá-la a um sistema Cloud Volumes ONTAP .

Passos

1. No painel de navegação esquerdo, selecione **Administração > Licenças e assinaturas**.
2. Selecione a aba **Visão geral**.
3. No bloco Cloud Volumes ONTAP , selecione **Exibir**.
4. Selecione **Licenças baseadas em nós** no menu suspenso.
5. Na guia **BYOL**, expanda os detalhes de um sistema Cloud Volumes ONTAP .
6. Clique em **Adicionar Licença de Capacidade**.
7. Digite o número de série ou carregue o arquivo de licença (ou arquivos, se você tiver um par HA).
8. 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 Console.

Passos

1. No painel de navegação esquerdo, selecione **Administração > Licenças e assinaturas**.
2. Selecione a aba **Visão geral**.
3. No bloco Cloud Volumes ONTAP , selecione **Exibir**.
4. Selecione **Licenças baseadas em nós** no menu suspenso.
5. Na guia **BYOL**, expanda os detalhes de um sistema Cloud Volumes ONTAP .
6. Clique no menu de ação ao lado da licença de capacidade e selecione **Atualizar licença**.
7. Carregue o arquivo de licença (ou arquivos se você tiver um par HA).
8. Clique em **Atualizar licença**.

Remover licenças de capacidade

Se uma licença de capacidade extra expirou e não estiver mais em uso, você poderá removê-la a qualquer momento.

Passos

1. No painel de navegação esquerdo, selecione **Administração > Licenças e assinaturas**.
2. Selecione a aba **Visão geral**.

3. No bloco Cloud Volumes ONTAP , selecione **Exibir**.
4. Selecione **Licenças baseadas em nós** no menu suspenso.
5. Na guia **BYOL**, expanda os detalhes de um sistema Cloud Volumes ONTAP .
6. Clique no menu de ação ao lado da licença de capacidade e selecione **Remover licença**.
7. Clique em **Remover**.

Mudança entre PAYGO e BYOL

A conversão de um sistema de licenciamento PAYGO por nó para licenciamento BYOL por nó (e vice-versa) não é suportada. Se você quiser alternar entre uma assinatura paga conforme o uso e uma assinatura BYOL, será necessário implantar um novo sistema e replicar os dados do sistema existente para o novo sistema.

Passos

1. Crie um novo sistema Cloud Volumes ONTAP .
2. Configure uma replicação de dados única entre os sistemas para cada volume que você precisa replicar.

["Aprenda a replicar dados entre sistemas"](#)

3. Encerre o sistema Cloud Volumes ONTAP que você não precisa mais excluindo o sistema original.

["Aprenda como excluir um sistema Cloud Volumes ONTAP"](#) .

Links relacionados

<https://docs.netapp.com/pt-br/storage-management-cloud-volumes-ontap/concept-licensing.html#end-of-availability-of-node-based-licenses> "Fim da disponibilidade de licenças baseadas em nós" [xref:./task-convert-node-capacity.html](#) "Converter licenças baseadas em nó em licenças baseadas em capacidade"

Administração de volume e LUN

Crie um FlexVol volume em um sistema Cloud Volumes ONTAP

Se precisar de mais armazenamento após iniciar seu sistema Cloud Volumes ONTAP inicial, você poderá criar novos volumes FlexVol para NFS, CIFS ou iSCSI no NetApp Console.

Você tem várias maneiras de criar um novo volume:

- Especifique detalhes para um novo volume e deixe o Console lidar com os agregados de dados subjacentes para você. [Saber mais](#)
- Crie um volume em um agregado de dados de sua escolha. [Saber mais](#)
- Crie um volume no segundo nó em uma configuração de HA. [Saber mais](#)

Antes de começar

Algumas notas sobre provisionamento de volume:

- Quando você cria um volume iSCSI, o Console cria automaticamente um LUN para você. Simplificamos criando apenas um LUN por volume, portanto não há gerenciamento envolvido. Depois de criar o

volume, ["use o IQN para conectar-se ao LUN de seus hosts"](#) .

- Você pode criar LUNs adicionais no ONTAP System Manager ou no ONTAP CLI.
- Se você quiser usar o CIFS na AWS, precisará configurar o DNS e o Active Directory. Para mais detalhes, consulte ["Requisitos de rede para Cloud Volumes ONTAP para AWS"](#) .
- Se a configuração do Cloud Volumes ONTAP for compatível com o recurso Amazon EBS Elastic Volumes, talvez você queira ["saiba mais sobre o que acontece quando você cria um volume"](#) .

Criar um volume

A maneira mais comum de criar um volume é especificar o tipo de volume que você precisa e então deixar o Console cuidar da alocação de disco para você. Mas você também tem a opção de escolher o agregado específico no qual deseja criar o volume.

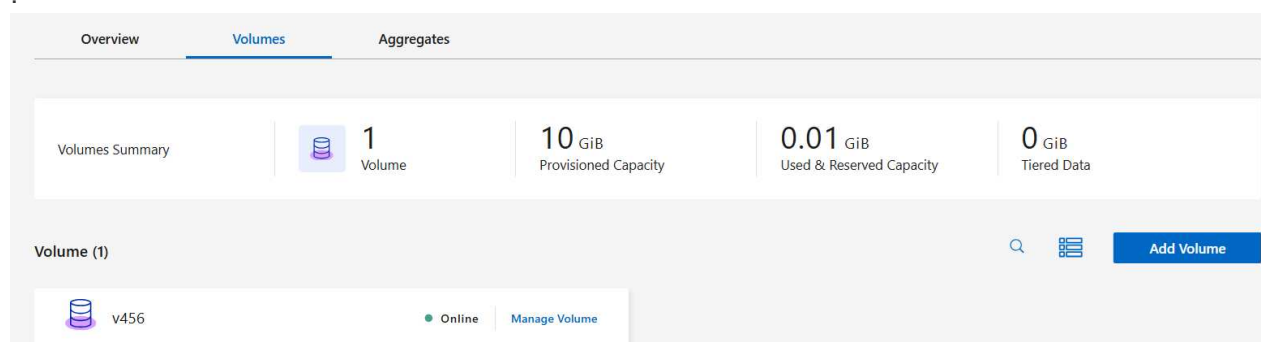
Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique duas vezes no nome do sistema Cloud Volumes ONTAP no qual você deseja provisionar um FlexVol volume.

Você pode criar um volume deixando que o Console cuide da 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 no seu sistema Cloud Volumes ONTAP .

Qualquer agregado

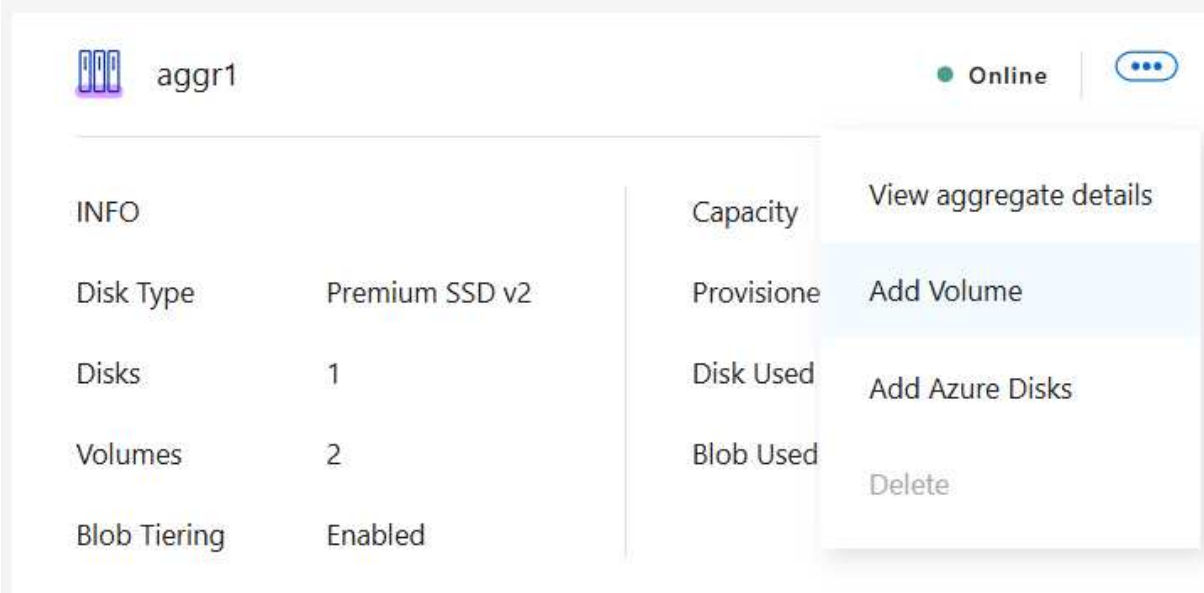
Selecione a aba Volumes e clique em **Adicionar Volume**



Agregado específico

- Na aba **Agregados**, vá até o agregado desejado e clique no botão **...** ícone.
- Selecione **Adicionar volume**

Aggregate (1)



INFO		Capacity	
Disk Type	Premium SSD v2	Provisioned Capacity	
Disks	1	Disk Used	
Volumes	2	Blob Used	
Blob Tiering	Enabled		

3. Siga as etapas do assistente para criar o volume.

- Detalhes, proteção e tags:** insira detalhes básicos sobre o volume e selecione uma política de instantâneo.

Alguns campos nesta página são autoexplicativos. A lista a seguir descreve campos para os quais você pode precisar de orientação:

Campo	Descrição
Nome do volume	O nome identificável que você pode inserir para o novo volume.

Campo	Descrição
Tamanho do volume	O tamanho máximo que você pode inserir depende muito se você habilita o provisionamento fino, que permite criar um volume maior que o armazenamento físico disponível atualmente.
VM de armazenamento (SVM)	Uma VM de armazenamento é uma máquina virtual executada no ONTAP que fornece serviços de armazenamento e dados aos seus clientes. Você pode conhecer isso como SVM ou vserver. O Cloud Volumes ONTAP é configurado com uma VM de armazenamento por padrão, mas algumas configurações oferecem suporte a VMs de armazenamento adicionais. Você pode especificar a VM de armazenamento para o novo volume.
Política de Snapshot	Uma política de cópia de instantâneo especifica a frequência e o número de cópias de instantâneo do NetApp criadas automaticamente. Uma cópia do NetApp Snapshot é uma imagem do sistema de arquivos de um momento específico que não tem impacto no desempenho e requer armazenamento mínimo. Você pode escolher a política padrão ou nenhuma. Você pode escolher nenhum para dados transitórios: por exemplo, tempdb para Microsoft SQL Server.

- b. **Protocolo:** Escolha um protocolo para o volume (NFS, CIFS ou iSCSI) e forneça as informações necessárias.

Se você selecionar CIFS e um servidor não estiver configurado, o Console solicitará que você configure a conectividade CIFS após clicar em **Avançar**.

["Saiba mais sobre os protocolos e versões de clientes suportados"](#) .

As seções a seguir descrevem 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 Console 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 chamados de listas de controle de acesso ou ACLs). Você pode especificar usuários ou grupos locais ou de domínio do Windows, ou usuários ou grupos do UNIX. Se você especificar um nome de usuário de domínio do Windows, deverá incluir o domínio do usuário usando o formato domínio\nome de usuário.

Endereço IP primário e secundário do DNS

Os endereços IP dos servidores DNS que fornecem resolução de nomes para o servidor CIFS. Os servidores DNS listados devem conter os registros de localização de serviço (SRV) necessários para localizar os servidores LDAP do Active Directory e os controladores de domínio para o domínio ao qual o servidor CIFS se juntará.

Se você estiver configurando o Google Managed Active Directory, o AD poderá ser acessado por padrão com o endereço IP 169.254.169.254.

Domínio do Active Directory para ingressar

O FQDN do domínio do Active Directory (AD) ao qual você deseja que o servidor CIFS ingresse.

Credenciais autorizadas para ingressar no domínio

O nome e a senha de uma conta do Windows com privilégios suficientes para adicionar computadores à Unidade Organizacional (UO) especificada dentro do domínio do AD.

Nome NetBIOS do servidor CIFS

Um nome de servidor CIFS exclusivo no domínio do AD.

Unidade Organizacional

A unidade organizacional dentro do domínio do AD a ser associada ao servidor CIFS. O padrão é CN=Computadores.

- Para configurar o AWS Managed Microsoft AD como o servidor AD para o Cloud Volumes ONTAP, insira **OU=Computers,OU=corp** neste campo.
- Para configurar o Azure AD Domain Services como o servidor AD para o Cloud Volumes ONTAP, insira **OU=AADDC Computers** ou **OU=AADDC Users** neste campo. <https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou>["Documentação do Azure: Criar uma Unidade Organizacional (UO) em um domínio gerenciado do Azure AD Domain Services"]
- Para configurar o Google Managed Microsoft AD como o servidor AD para o Cloud Volumes ONTAP, insira **OU=Computers,OU=Cloud** neste campo. https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Documentação do Google Cloud: Unidades organizacionais no Google Managed Microsoft AD"]

Domínio DNS

O domínio DNS para a máquina virtual de armazenamento (SVM) do Cloud Volumes ONTAP . Na maioria dos casos, o domínio é o mesmo que o domínio do AD.

Servidor NTP

Selecione **Usar domínio do Active Directory** para configurar um servidor NTP usando o DNS do Active Directory. Se você precisar configurar um servidor NTP usando um endereço diferente, use a API. Para obter informações, consulte o ["Documentação de automação do NetApp Console"](#) .

Observe que você só pode configurar um servidor NTP 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 você cria um volume iSCSI, o Console cria automaticamente um LUN para você. Simplificamos criando apenas um LUN por volume, portanto não há gerenciamento envolvido. Depois de criar o volume, ["use o IQN para conectar-se ao LUN de seus hosts"](#) .

Grupo iniciador

Grupos iniciadores (igroups) 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 padrão (NICs), placas de mecanismo de descarregamento TCP (TOE) com iniciadores de software, adaptadores de rede convergentes (CNAs) ou adaptadores de bust de host dedicados (HBAs) e são identificados por nomes qualificados iSCSI (IQNs).

a. **Tipo de disco:** escolha um tipo de disco subjacente para o volume com base em suas necessidades de desempenho e requisitos de custo.

- ["Dimensionando seu sistema na AWS"](#)
- ["Dimensionando seu sistema no Azure"](#)
- ["Dimensionando seu sistema no Google Cloud"](#)

4. **Perfil de uso e política de níveis:** escolha se deseja habilitar ou desabilitar os recursos de eficiência de armazenamento no volume e, em seguida, selecione um ["política de níveis de volume"](#) .

O ONTAP inclui vários recursos de eficiência de armazenamento que podem reduzir a quantidade total de armazenamento necessária. Os recursos de eficiência de armazenamento da NetApp oferecem os seguintes benefícios:

Provisionamento fino

Apresenta mais armazenamento lógico para hosts ou usuários do que você realmente tem em seu pool de armazenamento físico. Em vez de pré-alocar espaço de armazenamento, o espaço de armazenamento é alocado dinamicamente para cada volume à medida que os dados são gravados.

Desduplicação

Melhora a eficiência localizando blocos idênticos de dados e substituindo-os por referências a um único bloco compartilhado. Essa técnica reduz os requisitos de capacidade de armazenamento eliminando

blocos redundantes de dados que residem no mesmo volume.

Compressão

Reduz a capacidade física necessária para armazenar dados compactando dados dentro de um volume no armazenamento primário, secundário e de arquivo.

5. **Revisar**: revise os detalhes sobre o volume e clique em **Adicionar**.

Resultado

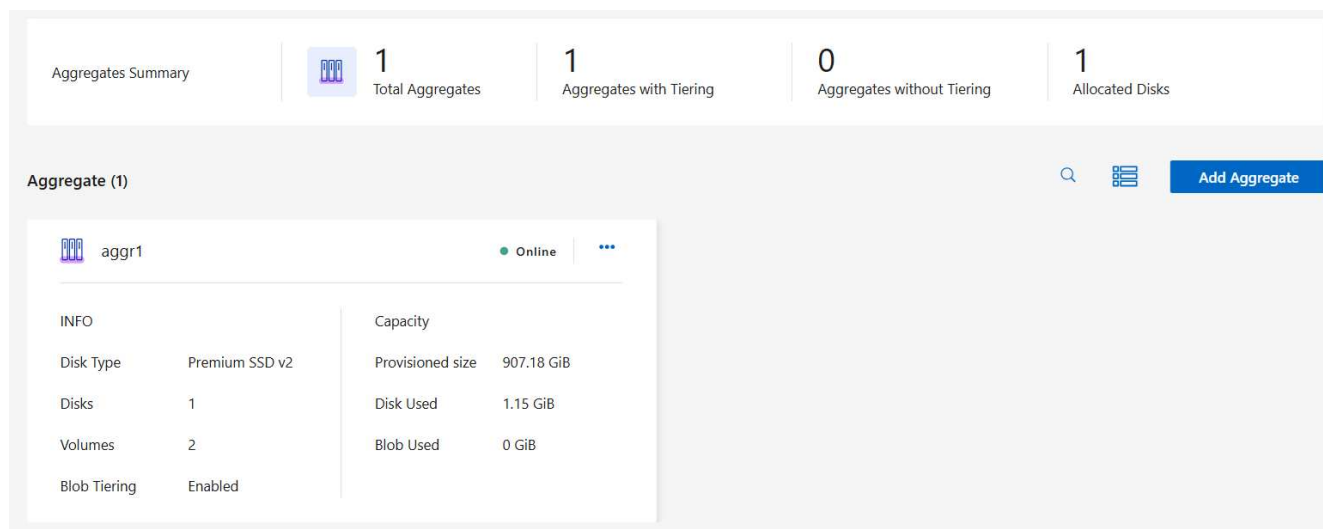
O Console cria o volume no sistema Cloud Volumes ONTAP .

Crie um volume no segundo nó em uma configuração de HA

Por padrão, o Console cria volumes no primeiro nó em uma configuração de HA. Se precisar de uma configuração ativa-ativa, na qual ambos os nós fornecem dados aos clientes, você deve criar agregados e volumes no segundo nó.

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique duas vezes no nome do sistema Cloud Volumes ONTAP no qual você deseja gerenciar agregados.
3. Na guia Agregados, clique em **Adicionar agregado** e crie o agregado.



Aggregates Summary

Metric	Value
Total Aggregates	1
Aggregates with Tiering	1
Aggregates without Tiering	0
Allocated Disks	1

Aggregate (1)

aggr1 Online

Category	Item	Value
INFO	Disk Type	Premium SSD v2
	Disks	1
	Volumes	2
	Blob Tiering	Enabled
Capacity	Provisioned size	907.18 GiB
	Disk Used	1.15 GiB
	Blob Used	0 GiB

4. Para Home Node, escolha o segundo nó no par HA.
5. Depois que o Console criar o agregado, selecione-o e clique em **Criar volume**.
6. Insira os detalhes do novo volume e clique em **Criar**.

Resultado

O Console cria o volume no segundo nó do par HA.



Para pares de HA implantados em várias Zonas de Disponibilidade da AWS, você deve montar o volume para clientes usando o endereço IP flutuante do nó no qual o volume reside.

Depois de criar um volume

Se você provisionou um compartilhamento CIFS, conceda aos usuários ou grupos permissões para os arquivos e pastas e verifique se esses usuários podem acessar o compartilhamento e criar um arquivo.

Se quiser aplicar cotas aos volumes, você deve usar o ONTAP System Manager ou o ONTAP CLI. As cotas permitem que você restrinja ou rastreie o espaço em disco e o número de arquivos usados por um usuário, grupo ou qtree.

Gerenciar volumes em sistemas Cloud Volumes ONTAP

Você pode gerenciar volumes e servidores CIFS no NetApp Console. Você também pode mover volumes para evitar problemas de capacidade.

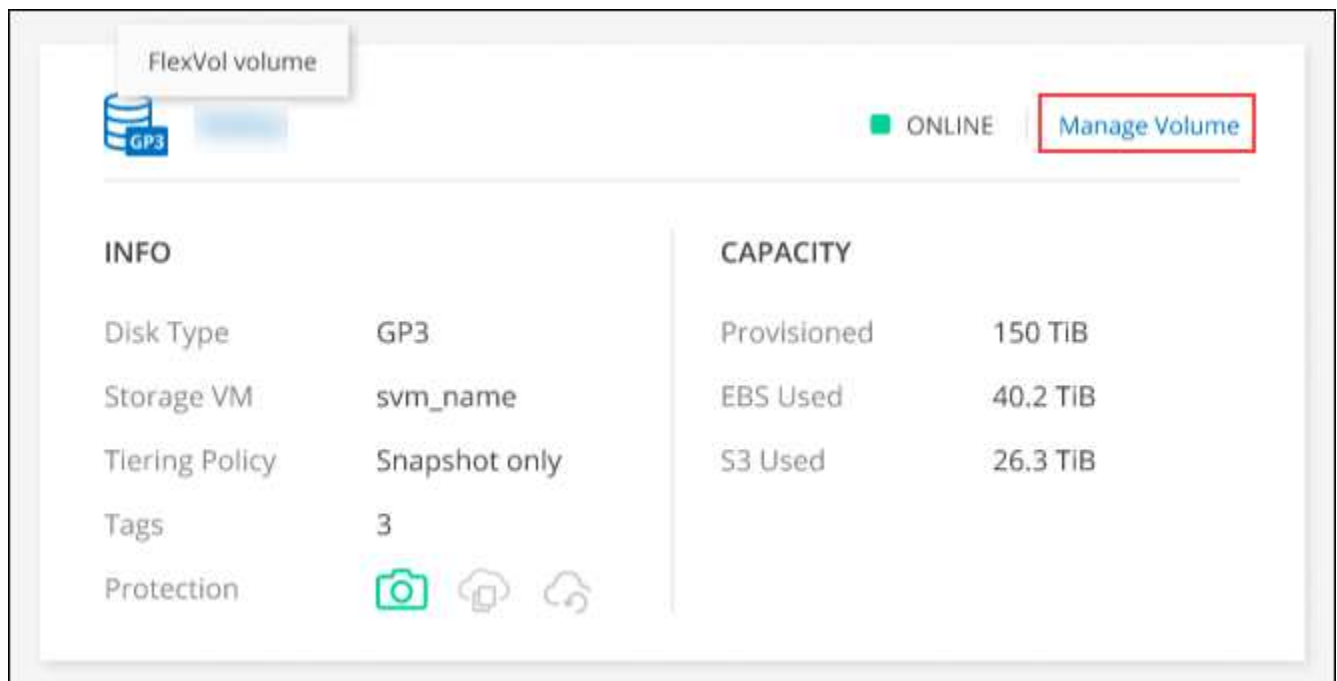
Você pode gerenciar volumes no NetApp Console Standard View ou por meio do ONTAP System Manager, incluído no Console para gerenciamento avançado de volumes. A visualização padrão fornece um conjunto limitado de opções para modificar seus volumes. O System Manager fornece um nível avançado de gerenciamento, como clonagem, redimensionamento, alteração de configurações para anti-ransomware, análise, proteção e rastreamento de atividades, além de movimentação de volumes entre camadas. Para obter informações, consulte ["Administrar o Cloud Volumes ONTAP usando o System Manager"](#).

Gerenciar volumes

Ao usar a Exibição Padrão do Console, você pode gerenciar volumes de acordo com suas necessidades de armazenamento. Você pode visualizar, editar, clonar, restaurar e excluir volumes.

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique duas vezes no sistema Cloud Volumes ONTAP no qual você deseja gerenciar volumes.
3. Selecione a aba **Volumes**.



4. No bloco de volume necessário, clique em **Gerenciar volume**.

Tarefa	Ação
Exibir informações sobre um volume	Em Ações de volume no painel Gerenciar volumes, clique em Exibir detalhes do volume .
Obtenha o comando de montagem NFS	- Em Ações de volume no painel Gerenciar volumes, clique em Comando de montagem. - Clique em Copiar.
Clonar um volume	- Em Ações de volume no painel Gerenciar volumes, clique em Clonar o volume. - Modifique o nome do clone conforme necessário e clique em Clonar. Este processo cria um volume FlexClone . Um volume FlexClone é uma cópia gravável, pontual e que economiza espaço porque usa uma pequena quantidade de espaço para metadados e só consome espaço adicional conforme os dados são alterados ou adicionados. Para saber mais sobre os volumes do FlexClone , consulte o "Guia de gerenciamento de armazenamento lógico ONTAP 9" .
Editar um volume (somente volumes de leitura e gravação)	- Em Ações de volume no painel Gerenciar volumes, clique em Editar configurações de volume - Modifique a política de 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.  Se precisar de políticas de Snapshot personalizadas, você pode criá-las usando o ONTAP System Manager.
Excluir um volume	- Em Ações de volume no painel Gerenciar volumes, clique em Excluir o volume. - Na janela Excluir volume, digite o nome do volume que você deseja excluir. - Clique em Excluir novamente para confirmar.
Crie uma cópia do Snapshot sob demanda	- Em Ações de proteção no painel Gerenciar volumes, clique em Criar uma cópia de instantâneo. - Altere o nome, se necessário, e clique em Criar.
Restaurar dados de uma cópia do Snapshot para um novo volume	- Em Ações de proteção no painel Gerenciar volumes, clique em Restaurar da cópia do instantâneo. - Selecione uma cópia do Snapshot, insira um nome para o novo volume e clique em Restaurar.

Tarefa	Ação
Alterar o tipo de disco subjacente	a. Em Ações avançadas no painel Gerenciar volumes, clique em Alterar tipo de disco. b. Selecione o tipo de disco e clique em Alterar.  O Console move o volume para um agregado existente que usa o tipo de disco selecionado ou cria um novo agregado para o volume.
Alterar a política de níveis	a. Em Ações avançadas no painel Gerenciar volumes, clique em Alterar política de camadas. b. Selecione uma política diferente e clique em Alterar.  O Console move o volume para um agregado existente que usa o tipo de disco selecionado com camadas ou cria um novo agregado para o volume.
Excluir um volume	a. Selecione um volume e clique em Excluir. b. Digite o nome do volume na caixa de diálogo. c. Clique em Excluir novamente para confirmar.

Redimensionar um volume

Por padrão, um volume cresce automaticamente até um tamanho máximo quando fica sem espaço. O valor padrão é 1.000, o que significa que o volume pode crescer até 11 vezes seu tamanho. Este valor pode ser configurado nas configurações do agente do Console.

Se precisar redimensionar seu volume, você pode fazer isso no ONTAP System Manager no Console.

Passos

1. Clique na visualização do Gerenciador de Sistema para redimensionar um volume por meio do Gerenciador de Sistema ONTAP . Consulte "[Como começar](#)" .
2. No menu de navegação à esquerda, selecione **Armazenamento > Volumes**.
3. Na lista de volumes, identifique aquele que você deve redimensionar.
4. Clique no ícone de opções  .
5. Selecione **Redimensionar**.
6. Na tela **Redimensionar volume**, edite a capacidade e a porcentagem de reserva do Snapshot conforme necessário. Você pode comparar o espaço existente e disponível com a capacidade modificada.
7. Clique em **Salvar**.

Resize volume

CAPACITY

25

GiB

SNAPSHOT RESERVE %

1

Existing

DATA SPACE

20 GiB

SNAPSHOT RESERVE

0 Bytes

New

DATA SPACE

24.75 GiB

SNAPSHOT RESERVE

256 MiB

Cancel

Save

Certifique-se de levar em consideração os limites de capacidade do seu sistema ao redimensionar volumes. Vá para o ["Notas de versão do Cloud Volumes ONTAP"](#) para mais informações.

Modificar o servidor CIFS

Se você alterar seus servidores DNS ou o domínio do Active Directory, precisará modificar o servidor CIFS no Cloud Volumes ONTAP para que ele possa continuar a fornecer armazenamento aos clientes.

Passos

1. Na guia **Visão geral** do sistema Cloud Volumes ONTAP , clique na guia **Recurso** no painel do lado direito.
2. No campo Configuração do CIFS, clique no **ícone de lápis** para exibir a janela Configuração do CIFS.
3. Especifique as configurações para o servidor CIFS:

Tarefa	Ação
Selecione VM de armazenamento (SVM)	Selecionar a máquina virtual de armazenamento Cloud Volume ONTAP (SVM) exibe suas informações CIFS configuradas.
Domínio do Active Directory para ingressar	O FQDN do domínio do Active Directory (AD) ao qual você deseja que o servidor CIFS ingresse.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com privilégios suficientes para adicionar computadores à Unidade Organizacional (UO) especificada dentro do domínio do AD.

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 Active Directory e os controladores de domínio para o domínio ao qual o servidor CIFS se juntará. <code>ifndef::gcp[]</code> Se você estiver configurando o Google Managed Active Directory, o AD poderá ser acessado por padrão com o endereço IP 169.254.169.254. <code>endif::gcp[]</code>
Domínio DNS	O domínio DNS para a máquina virtual de armazenamento (SVM) do Cloud Volumes ONTAP. Na maioria dos casos, o domínio é o mesmo que o domínio do AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio do AD.
Unidade Organizacional	A unidade organizacional dentro do domínio do AD a ser associada ao servidor CIFS. O padrão é CN=Computadores. • Para configurar o AWS Managed Microsoft AD como o servidor AD para o Cloud Volumes ONTAP, insira OU=Computers,OU=corp neste campo. • Para configurar o Azure AD Domain Services como o servidor AD para o Cloud Volumes ONTAP, insira OU=AADDC Computers ou OU=AADDC Users neste campo. "Documentação do Azure: Criar uma Unidade Organizacional (UO) em um domínio gerenciado do Azure AD Domain Services" • Para configurar o Google Managed Microsoft AD como o servidor AD para o Cloud Volumes ONTAP, insira OU=Computers,OU=Cloud 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 da capacidade, melhor desempenho e para satisfazer acordos de nível de serviço.

Você pode mover um volume no ONTAP System Manager selecionando um volume e o agregado de destino, iniciando a operação de movimentação de volume e, opcionalmente, monitorando o trabalho de movimentação de volume. Ao usar o Gerenciador do Sistema, uma operação de movimentação de volume é concluída automaticamente.

Passos

1. Use o ONTAP System Manager ou o ONTAP CLI para mover os volumes para o agregado.

Na maioria das situações, você pode usar o Gerenciador do Sistema para mover volumes.

Para obter instruções, consulte o ["Guia de movimentação expressa do ONTAP 9 Volume"](#).

Mover um volume quando o Console exibir uma mensagem de Ação Necessária

O Console pode exibir uma mensagem Ação Necessária informando que mover um volume é necessário para evitar problemas de capacidade, mas que você precisa corrigir o problema sozinho. Se isso acontecer, você precisará identificar como corrigir o problema e então mover um ou mais volumes.



O Console exibe estas mensagens de Ação Necessária quando um agregado atinge 90% da capacidade utilizada. Se a hierarquização de dados estiver habilitada, as mensagens serão exibidas quando um agregado atingir 80% da capacidade utilizada. Por padrão, 10% de espaço livre é reservado para camadas de dados. ["Saiba mais sobre a proporção de espaço livre para camadas de dados"](#).

Passos

1. [Identificar como corrigir problemas de capacidade](#).
2. Com base na sua análise, mova volumes para evitar problemas de capacidade:
 - [Mover volumes para outro sistema para evitar problemas de capacidade](#).
 - [Mover volumes para outro agregado para evitar problemas de capacidade](#).

Identificar como corrigir problemas de capacidade

Se o Console não puder fornecer recomendações para mover um volume a fim de evitar problemas de capacidade, você deverá identificar os volumes que precisa mover e se deve movê-los para outro agregado no mesmo sistema ou para outro sistema.

Passos

1. Veja 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 a serem movidos para fora do agregado:
 - a. No sistema Cloud Volumes ONTAP, clique na guia **Agregados**.
 - b. No bloco agregado, clique em  ícone e clique em **Exibir detalhes agregados**.
 - c. Na aba **Visão geral** da tela **Detalhes do agregado**, revise o tamanho de cada volume e escolha um ou mais volumes para mover para fora do agregado.

Você deve escolher volumes grandes o suficiente para liberar espaço no total, evitando problemas adicionais de capacidade no futuro.

Aggregate Details	
aggr1	
Overview	Capacity Allocation
Provider Properties	
State	online
Home Node	drillup01
Encryption Type	cloudEncrypted
Volumes	2 ^
	www_drillup01_root (1 GiB)
	drillup01 (500 GiB)

- Se o sistema não tiver atingido o limite do disco, você deverá mover os volumes para um agregado existente ou um novo agregado no mesmo sistema.

Para obter informações, consulte [Mover volumes para outro agregado para evitar problemas de capacidade](#).

- Se o sistema atingiu o limite do disco, faça o seguinte:
 - Exclua todos os volumes não utilizados.
 - Reorganize volumes para liberar espaço em um agregado.

Para obter informações, consulte [Mover volumes para outro agregado para evitar problemas de capacidade](#).

- Mova dois ou mais volumes para outro sistema que tenha espaço.

Para obter informações, consulte [Mover volumes para outro agregado para evitar problemas de capacidade](#).

Mover 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 caso o sistema tenha atingido o limite de disco.

Sobre esta tarefa

Você pode seguir as etapas desta tarefa para corrigir a seguinte mensagem de Ação Necessária:

Mover um volume é necessário para evitar problemas de capacidade; no entanto, o Console não pode executar essa ação para você porque o sistema atingiu o limite do disco.

Passos

1. Identifique um sistema Cloud Volumes ONTAP que tenha capacidade disponível ou implante um novo sistema.
2. Arraste e solte o sistema de origem no sistema de destino para executar uma replicação de dados única do volume.

Para obter informações, consulte ["Replicando dados entre sistemas"](#) .

3. Acesse a página Status de replicação e interrompa o relacionamento SnapMirror para converter o volume replicado de um volume de proteção de dados para um volume de leitura/gravação.

Para obter informações, consulte ["Gerenciando cronogramas e relacionamentos de replicação de dados"](#) .

4. Configure o volume para acesso a dados.

Para obter informações sobre como configurar um volume de destino para acesso a dados, consulte o ["Guia Expresso de Recuperação de Desastres de Volume ONTAP 9"](#) .

5. Exclua o volume original.

Para obter informações, consulte ["Gerenciar volumes"](#) .

Mover volumes para outro agregado para evitar problemas de capacidade

Você pode mover um ou mais volumes para outro agregado para evitar problemas de capacidade.

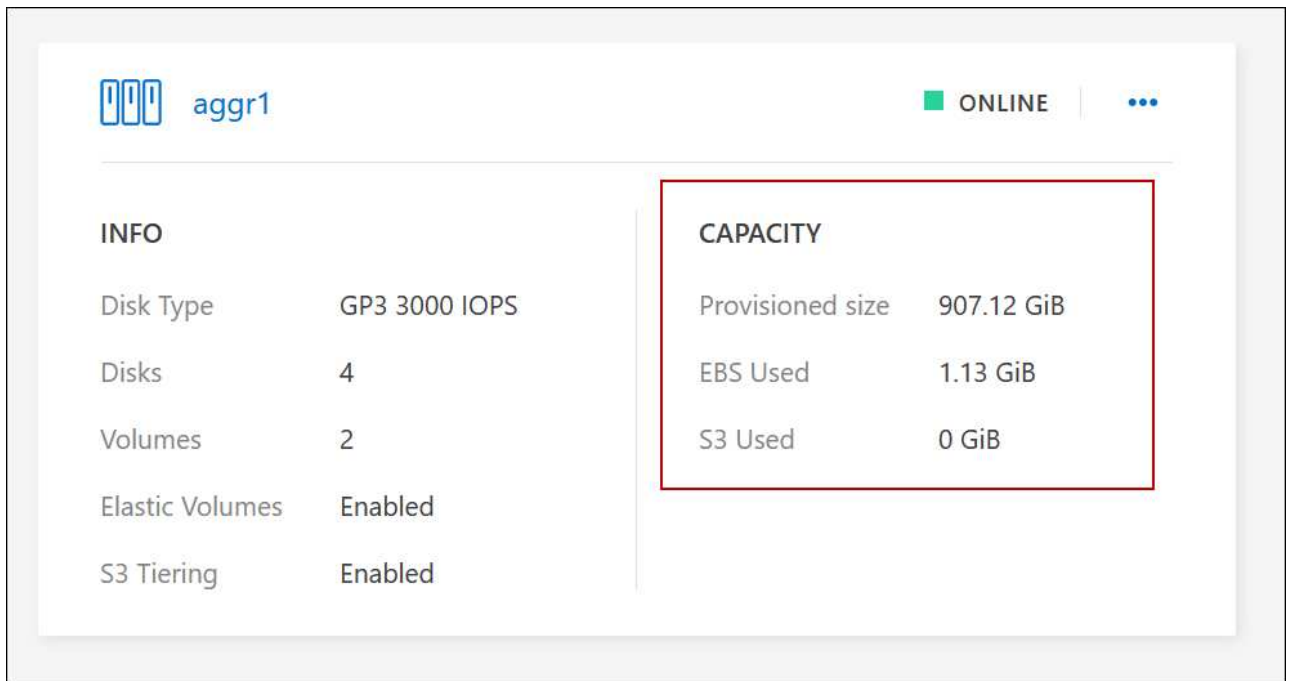
Sobre esta tarefa

Você pode seguir as etapas desta tarefa para corrigir a seguinte mensagem de Ação Necessária:

Mover dois ou mais volumes é necessário para evitar problemas de capacidade; no entanto, o Console 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 sistema Cloud Volumes ONTAP , clique na **guia Agregados**.
 - b. No bloco agregado necessário, clique em  ícone e então **Exibir detalhes agregados** para visualizar a capacidade disponível (tamanho provisionado menos capacidade agregada usada).



2. Se necessário, adicione discos a um agregado existente:
 - a. Selecione o agregado e clique em **...** ícone > **Adicionar discos**.
 - b. Selecione o número de discos a serem adicionados e clique em **Adicionar**.
3. Se nenhum agregado tiver capacidade disponível, crie um novo agregado.

Para obter informações, consulte ["Criando agregados"](#).

4. Use o ONTAP System Manager ou o ONTAP CLI para mover os volumes para o agregado.
5. Na maioria das situações, você pode usar o Gerenciador do Sistema para mover volumes.

Para obter instruções, consulte o ["Guia de movimentação expressa do ONTAP 9 Volume"](#).

Razões pelas quais uma movimentação de volume pode ter um desempenho lento

Mover um volume pode levar 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 pai de um clone.
- O agregado de origem ou destino tem um único disco HDD otimizado para throughput (st1).
- Um dos agregados usa um esquema de nomenclatura mais antigo para objetos. Ambos os agregados devem usar o mesmo formato de nome.

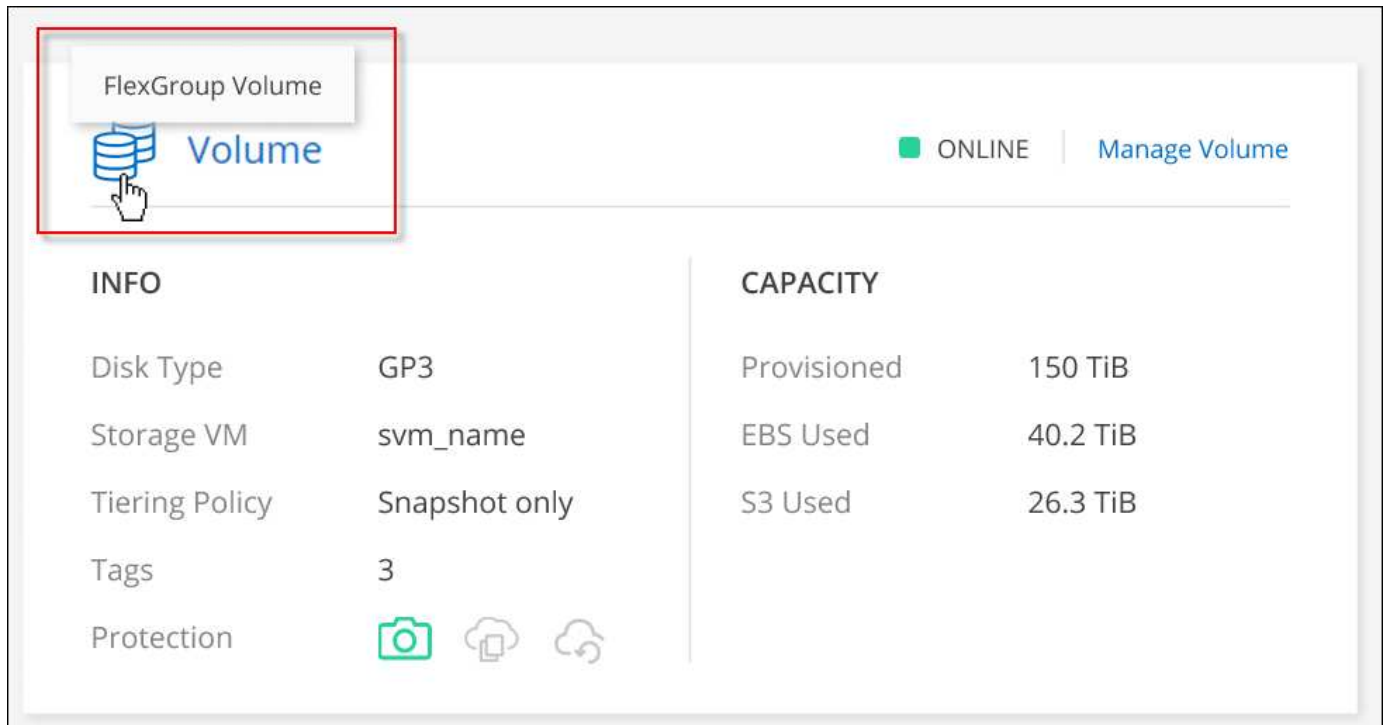
Um esquema de nomenclatura mais antigo será usado se a hierarquização de dados tiver sido habilitada em um agregado na versão 9.4 ou anterior.

- As configurações de criptografia não correspondem nos agregados de origem e destino, ou uma nova chave está em andamento.
- A opção *-tiering-policy* foi especificada na movimentação do volume para alterar a política de camadas.

- A opção *-generate-destination-key* foi especificada na movimentação do volume.

Exibir volumes do FlexGroup

Você pode visualizar volumes FlexGroup criados por meio do ONTAP System Manager ou do ONTAP CLI diretamente na guia Volumes no Console. Você pode ver informações detalhadas dos volumes FlexGroup por meio de um bloco dedicado **Volumes**, onde você pode identificar cada grupo de volumes FlexGroup por meio do texto do ícone. Além disso, você pode identificar e classificar volumes FlexGroup na exibição de lista de volumes por meio da 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 visualizar volumes FlexGroup existentes no Console. Não é possível criar volumes FlexGroup no Console.

Dados Cloud Volumes ONTAP inativos em camadas para um armazenamento de objetos de baixo custo

Você pode reduzir os custos de armazenamento do Cloud Volumes ONTAP combinando uma camada de desempenho de SSD ou HDD para dados ativos com uma camada de capacidade de armazenamento de objetos para dados inativos. A hierarquização de dados é alimentada pela tecnologia FabricPool. Para uma visão geral de alto nível, consulte ["Visão geral da hierarquização de dados"](#).

Para configurar a hierarquização de dados, você precisa fazer o seguinte:

1

Escolha uma configuração suportada

A maioria das configurações são suportadas. Se você tiver um sistema Cloud Volumes ONTAP executando a versão mais recente, estará pronto para começar. ["Saber mais"](#).

2**Garantir a conectividade entre o Cloud Volumes ONTAP e o armazenamento de objetos**

- Para AWS, você precisará de um VPC Endpoint para S3. [Saber mais](#) .
- No caso do Azure, você não precisará fazer nada, desde que o NetApp Console tenha as permissões necessárias. [Saber mais](#) .
- Para o Google Cloud, você precisa configurar a sub-rede para o Private Google Access e configurar uma conta de serviço. [Saber mais](#) .

3**Certifique-se de ter um agregado com hierarquização habilitada**

A hierarquização de dados deve ser habilitada em um agregado para habilitá-la em um volume. Você deve estar ciente dos requisitos para novos volumes e para volumes existentes. [Saber mais](#) .

4**Escolha uma política de camadas ao criar, modificar ou replicar um volume**

O NetApp Console solicita que você escolha uma política de camadas ao criar, modificar ou replicar um volume.

- ["Dados de nível de volumes de leitura e gravação"](#)
- ["Dados em camadas de volumes de proteção de dados"](#)

O que não é necessário para a hierarquização de dados?

- Você não precisa instalar uma licença de recurso para habilitar a hierarquização de dados.
- Você não precisa criar um armazenamento de objetos para a camada de capacidade. O Console faz isso por você.
- Você não precisa habilitar a hierarquização de dados no nível do sistema.



O Console cria um armazenamento de objetos para dados frios quando cria o sistema, [desde que não haja problemas de conectividade ou permissões](#) . Depois disso, você só precisa habilitar a hierarquização de dados nos volumes (e em alguns casos, [em agregados](#)).

Configurações que suportam camadas de dados

Você pode habilitar a hierarquização de dados ao usar configurações e recursos específicos.

Suporte na AWS

- A hierarquização de dados é suportada na AWS a partir do Cloud Volumes ONTAP 9.2.
- O nível de desempenho pode ser SSDs de uso geral (gp3 ou gp2) ou SSDs de IOPS provisionados (io1).



Não recomendamos hierarquizar dados para armazenamento de objetos ao usar HDDs com taxa de transferência otimizada (st1).

- Os dados inativos são colocados em camadas nos buckets do Amazon S3. Não há suporte para hierarquização com outros provedores.

Suporte no Azure

- O armazenamento em camadas de dados é suportado no Azure da seguinte forma:
 - Versão 9.4 com sistemas de nó único
 - Versão 9.6 com pares HA
- O nível de desempenho pode ser discos gerenciados SSD Premium, discos gerenciados SSD Standard ou discos gerenciados HDD Standard.
- Os dados inativos são hierarquizados no Microsoft Azure Blob. Não há suporte para hierarquização com outros provedores.

Suporte no Google Cloud

- A hierarquização de dados é suportada no Google Cloud a partir do Cloud Volumes ONTAP 9.6.
- O nível de desempenho pode ser discos persistentes SSD, discos persistentes balanceados ou discos persistentes padrão.
- Os dados inativos são armazenados em camadas no Google Cloud Storage. Não há suporte para hierarquização com outros provedores.

Interoperabilidade de recursos

- A hierarquização de dados é suportada com tecnologias de criptografia.
- O provisionamento fino deve ser habilitado nos volumes.

Requisitos

Dependendo do seu provedor de nuvem, certas conexões e permissões devem ser configuradas para que o Cloud Volumes ONTAP possa hierarquizar dados frios no armazenamento de objetos.

Requisitos para hierarquizar dados frios no AWS S3

Certifique-se de que o Cloud Volumes ONTAP tenha uma conexão com o S3. A melhor maneira de fornecer essa conexão é criando um VPC Endpoint para o serviço S3. Para obter instruções, consulte o ["Documentação da AWS: Criando um endpoint de gateway"](#) .

Ao criar o VPC Endpoint, certifique-se de selecionar a região, a VPC e a tabela de rotas que correspondem à instância do Cloud Volumes ONTAP . Você também deve modificar o grupo de segurança para adicionar uma regra HTTPS de saída que habilite o tráfego para o ponto de extremidade S3. Caso contrário, o Cloud Volumes ONTAP não poderá se conectar ao serviço S3.

Se você tiver algum problema, consulte ["Central de conhecimento do AWS Support: Por que não consigo me conectar a um bucket do S3 usando um endpoint de VPC de gateway?"](#) .

Requisitos para hierarquizar dados frios no armazenamento de Blobs do Azure

Você não precisa configurar uma conexão entre a camada de desempenho e a camada de capacidade, desde que o Console tenha as permissões necessárias. O Console habilita um ponto de extremidade de serviço VNet para você se a função personalizada do agente do Console tiver estas permissões:

```
"Microsoft.Network/virtualNetworks/subnets/write",  
"Microsoft.Network/routeTables/join/action",
```

A função personalizada inclui as permissões por padrão. ["Exibir permissão do Azure para o agente do Console"](#)

Requisitos para hierarquizar dados frios em um bucket do Google Cloud Storage

- A sub-rede na qual o Cloud Volumes ONTAP reside deve ser configurada para o Private Google Access. Para obter instruções, consulte ["Documentação do Google Cloud: Configurando o acesso privado do Google"](#).
- Uma conta de serviço deve ser anexada ao Cloud Volumes ONTAP.

["Aprenda como configurar esta conta de serviço"](#).

Você será solicitado a selecionar esta conta de serviço ao criar um sistema Cloud Volumes ONTAP.

Se você não selecionar uma conta de serviço durante a implantação, será necessário desligar o Cloud Volumes ONTAP, acessar o console do Google Cloud e anexar a conta de serviço às instâncias do Cloud Volumes ONTAP. Você pode então habilitar a hierarquização de dados conforme descrito na próxima seção.

- Para criptografar o bucket com chaves de criptografia gerenciadas pelo cliente, ative o bucket de armazenamento do Google Cloud para usar a chave.

["Aprenda a usar chaves de criptografia gerenciadas pelo cliente com o Cloud Volumes ONTAP"](#).

Habilitar a hierarquização de dados após implementar os requisitos

O Console cria um armazenamento de objetos para dados frios quando o sistema é criado, desde que não haja problemas de conectividade ou permissões. Se você não implementou os requisitos listados acima até depois de criar o sistema, será necessário habilitar manualmente a hierarquização por meio da API ou do ONTAP System Manager, que cria o armazenamento de objetos.



A capacidade de habilitar a hierarquização por meio do Console estará disponível em uma versão futura do Cloud Volumes ONTAP.

Certifique-se de que a hierarquização esteja habilitada em agregados

A hierarquização de dados deve ser habilitada em um agregado para habilitar a hierarquização de dados em um volume. Você deve estar ciente dos requisitos para novos volumes e para volumes existentes.

• Novos volumes

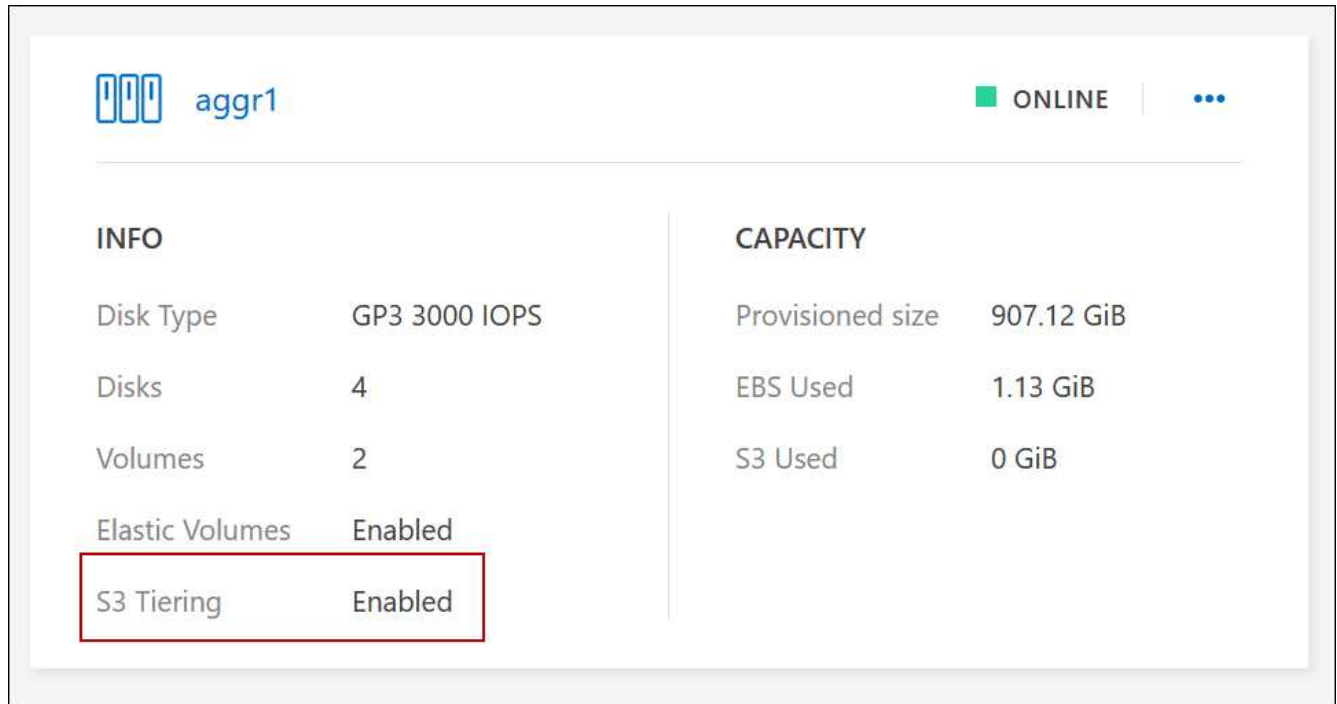
Se você estiver habilitando a hierarquização de dados em um novo volume, não precisará se preocupar em habilitar a hierarquização de dados em um agregado. O Console cria o volume em um agregado existente que tenha a hierarquização habilitada ou cria um novo agregado para o volume se ainda não existir um agregado habilitado para hierarquização de dados.

• Volumes existentes

Para habilitar a hierarquização de dados em um volume existente, certifique-se de que ela esteja habilitada no agregado subjacente. Se a hierarquização de dados não estiver habilitada no agregado existente, você precisará usar o ONTAP System Manager para anexar um agregado existente ao armazenamento de objetos.

Etapas para confirmar se a hierarquização está habilitada em um agregado

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Abra o sistema Cloud Volumes ONTAP .
3. Selecione a aba **Agregados** e verifique se a hierarquização está habilitada ou desabilitada no agregado.



Etapas para habilitar a hierarquização em um agregado

1. No ONTAP System Manager, clique em **Armazenamento > Níveis**.
2. Clique no menu de ação do agregado e selecione **Anexar camadas de nuvem**.
3. Selecione a camada de nuvem a ser anexada e clique em **Salvar**.

O que vem a seguir?

Agora você pode habilitar a hierarquização de dados em volumes novos e existentes, conforme explicado na próxima seção.

Dados de nível de volumes de leitura e gravação

O Cloud Volumes ONTAP pode hierarquizar dados inativos em volumes de leitura e gravação para armazenamento de objetos econômico, liberando a camada de desempenho para dados importantes.

Passos

1. Na aba **Volumes** no sistema, crie um novo volume ou altere o nível de um volume existente:

Tarefa	Ação
Criar 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 níveis no painel direito.

2. Selecione uma política de níveis.

Para uma descrição dessas políticas, consulte ["Visão geral da hierarquização de dados"](#).

Exemplo

Change Tiering Policy

Volume_1

Tiering Policy

☒ **Auto** - Tiers cold Snapshot copies and cold user data from the active file system to object storage.
Minimum cooling days: 31 (2-183)

☐ **All** - Immediately tiers all data (not including metadata) to object storage.

☐ **Snapshot Only** - Tiers cold Snapshot copies to object storage.

☐ **None** - Data tiering is disabled.

S3 Storage classes

Standard-Infrequent Access

S3 Storage Encryption Key

aws/s3

O Console cria um novo agregado para o volume se ainda não existir um agregado habilitado para camadas de dados.

Dados em camadas de volumes de proteção de dados

O Cloud Volumes ONTAP pode hierarquizar dados de um volume de proteção de dados para uma camada de capacidade. Se você ativar o volume de destino, os dados serão movidos gradualmente para a camada de desempenho à medida que forem lidos.

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, selecione o sistema Cloud Volumes ONTAP que contém o volume de origem e arraste-o para o sistema no qual você deseja replicar o volume.
3. Siga as instruções até chegar à página de hierarquização e habilitar a hierarquização de dados para armazenamento de objetos.

Exemplo



S3 Tiering

What are storage tiers?

☒ Enabled ☐ Disabled

Note: If you enable S3 tiering, thin provisioning must be enabled on volumes created in this aggregate.

Para obter ajuda com a replicação de dados, consulte ["Replicando dados de e para a nuvem"](#).

Alterar a classe de armazenamento para dados em camadas

Depois de implantar o Cloud Volumes ONTAP, você pode reduzir seus custos de armazenamento alterando a classe de armazenamento para dados inativos que não foram acessados por 30 dias. Os custos de acesso serão maiores se você acessar os dados, então leve isso em consideração antes de alterar a classe de armazenamento.

A classe de armazenamento para dados em camadas abrange todo o sistema, não é por volume.

Para obter informações sobre classes de armazenamento suportadas, consulte ["Visão geral da hierarquização de dados"](#).

Passos

1. No sistema Cloud Volumes ONTAP, clique no ícone de menu e depois clique em **Classes de armazenamento** ou **Níveis de armazenamento de blobs**.
2. Escolha uma classe de armazenamento e clique em **Salvar**.

Alterar a proporção de espaço livre para camadas de dados

A proporção de espaço livre para hierarquização de dados define quanto espaço livre é necessário nos SSDs/HDDs do Cloud Volumes ONTAP ao hierarquizar dados no armazenamento de objetos. A configuração padrão é 10% de espaço livre, mas você pode ajustá-la de acordo com suas necessidades.

Por exemplo, você pode escolher menos de 10% de espaço livre para garantir que está utilizando a capacidade adquirida. O Console pode então comprar discos adicionais para você quando capacidade adicional for necessária (até você atingir o limite de discos para o agregado).



Se não houver espaço suficiente, o Cloud Volumes ONTAP não poderá mover os dados e você poderá sofrer degradação de desempenho. Qualquer mudança deve ser feita com cautela. Caso não tenha certeza, entre em contato com o Suporte da NetApp para obter orientação.

A proporção é importante para cenários de recuperação de desastres 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 desempenho. Se não houver espaço suficiente, o Cloud Volumes ONTAP não poderá mover os dados. Leve isso em consideração ao alterar a proporção para que você possa atender às suas necessidades comerciais.

Passos

1. No painel de navegação esquerdo, acesse **Administração > Agentes**.
2. Clique no ícone para o agente do Console que gerencia seu sistema Cloud Volumes ONTAP.
3. Selecione *** Configurações do Cloud Volumes ONTAP ***.

NetApp Console

Organization: NetAppNew | Project: Project-1

Agents

Overview

Agents (3 / 58)

Name	Location	Status (1)	Deployment Type
AWSSAgent	US East (N. Virginia)	Active	aws
5678	eastus	Active	
itAWS	US East (N. Virginia)	Active	

Deploy agent

Edit Agent

Go to local UI

Agent Id:

HTTPS Setup

Cloud Volumes ONTAP Settings

Remove Agent

4. Em **Capacidade**, clique em **Limites de capacidade agregada - Proporção de espaço livre para hierarquização de dados**.

Overview > Cloud Volumes ONTAP Settings

Edit Cloud Volumes ONTAP settings

Capacity

Capacity Management Mode	Automatic Mode
Aggregate Capacity Thresholds - Free Space Ratio	10%
Aggregate Capacity Thresholds - Free Space Ratio for Data Tiering	10%
Volume Autosize - Additional Size in Percentage to Which Volumes Can Grow	1000%

General

Automatic Cloud Volumes ONTAP update during deployment	On

Azure

Azure CIFS locks for Azure HA systems	Off
Use Azure Private Link	On

5. Altere a proporção de espaço livre com base em suas necessidades e clique em **Salvar**.

Alterar o período de resfriamento da política de hierarquização automática

Se você habilitou o armazenamento em camadas de dados em um volume do Cloud Volumes ONTAP usando a política de armazenamento em camadas *automático*, poderá ajustar o período de resfriamento padrão com base nas necessidades do seu negócio. Esta ação é suportada somente usando ONTAP CLI e API.

O período de resfriamento é o número de dias que os dados do usuário em um volume devem permanecer inativos antes de serem considerados "frios" e movidos para o armazenamento de objetos.

O período de resfriamento padrão para a política de hierarquização automática é de 31 dias. Você pode alterar o período de resfriamento da seguinte forma:

- 9.8 ou posterior: 2 a 183 dias
- 9.7 ou anterior: 2 a 63 dias

Etapas

1. Use o parâmetro *minimumCoolingDays* com sua solicitação de API ao criar um volume ou modificar um volume existente.

Remover um bucket S3 ao descomissionar um sistema

Você pode excluir um bucket do S3 com os dados em camadas de um sistema Cloud Volumes ONTAP ao desativar o ambiente.

Você pode excluir o bucket S3 somente se:

- O sistema Cloud Volume ONTAP é excluído do Console.
- Todos os objetos são excluídos do bucket e o bucket S3 fica vazio.

Quando você desativa um sistema Cloud Volumes ONTAP, o bucket S3 criado para o ambiente não é excluído automaticamente. Em vez disso, ele permanece em um estado órfão para evitar qualquer perda acidental de dados. Você pode excluir os objetos no bucket, remover o próprio bucket do S3 ou mantê-lo para uso posterior. Consulte ["ONTAP CLI: exclusão de bucket do servidor de armazenamento de objetos do vservers"](#).

Conecte-se a um LUN no Cloud Volumes ONTAP do seu sistema host

Quando você cria um volume iSCSI, o NetApp Console cria automaticamente um LUN para você. Simplificamos criando apenas um LUN por volume, portanto não há gerenciamento envolvido. Depois de criar o volume, use o IQN para se conectar ao LUN a partir dos seus hosts.

Observe o seguinte:

- O gerenciamento automático de capacidade do Console não se aplica a LUNs. Ao criar um LUN, ele desabilita o recurso de crescimento automático.
- Você pode criar LUNs adicionais no ONTAP System Manager ou no ONTAP CLI.

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique duas vezes no sistema Cloud Volumes ONTAP no qual você deseja gerenciar volumes.

3. No sistema, selecione a aba **Volumes**.
4. Vá até o bloco de volume desejado e selecione **Gerenciar volume** para acessar o painel Gerenciar volumes à direita.
5. Clique em **Target iQN**.
6. Clique em **Copiar** para copiar o nome do iQN.
7. Configure uma conexão iSCSI do host para o LUN.
 - ["Configuração expressa do ONTAP 9 iSCSI para Red Hat Enterprise Linux: Iniciando as sessões iSCSI com o destino"](#)
 - ["Configuração expressa do ONTAP 9 iSCSI para Windows: iniciando sessões iSCSI com o destino"](#)
 - ["Configuração do host ONTAP SAN"](#)

Acelere o acesso a dados com volumes FlexCache em um sistema Cloud Volumes ONTAP

Um volume FlexCache é um volume de armazenamento que armazena em cache dados de leitura SMB e NFS de um volume de origem (ou fonte). Leituras subsequentes dos dados armazenados em cache resultam em acesso mais rápido a esses dados.

Você pode usar volumes FlexCache para acelerar o acesso aos dados ou para descarregar o tráfego de volumes muito acessados. 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 precisar acessar o volume de origem. Os volumes FlexCache funcionam bem para cargas de trabalho do sistema que exigem muita leitura.

O NetApp Console fornece gerenciamento de volumes FlexCache com o ["Cache de volume da NetApp"](#).

Você também pode usar o ONTAP CLI ou o ONTAP System Manager para criar e gerenciar volumes FlexCache :

- ["Guia de energia para volumes FlexCache para acesso mais rápido aos dados"](#)
- ["Criando volumes FlexCache no Gerenciador do Sistema"](#)



Trabalhar com FlexCache quando a origem estiver 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 em cache corretamente os dados criptografados.

Antes de começar

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 normalmente significa usar o AWS Key Management Service (KMS). Para obter informações, consulte [Gerencie chaves com o AWS Key Management Service](#) .

Para o Azure, você precisa configurar o Azure Key Vault para NetApp Volume Encryption (NVE). Para obter informações, consulte [Gerenciar chaves com o Azure Key Vault](#) .

Para o Google Cloud, é o Google Cloud Key Management Service. Para obter informações, consulte [Gerencie chaves com o Cloud Key Management Service do Google](#) .

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 válida do FlexCache 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 seja compatível com FlexCache com volumes criptografados. Consulte o mais recente [Notas de versão do ONTAP](#) ou matriz de compatibilidade para mais informações.
4. **Configuração de rede:** certifique-se de que a configuração de rede permita uma comunicação perfeita entre o volume de origem e o volume FlexCache . Isso inclui roteamento adequado e resolução de DNS

em um ambiente de nuvem.

Passos

Crie um volume FlexCache no seu sistema Cloud Volumes ONTAP com um volume de origem criptografado. Para etapas detalhadas e considerações adicionais, consulte as seguintes seções:

- ["Guia de energia para volumes FlexCache para acesso mais rápido aos dados"](#)
- ["Criando volumes FlexCache no Gerenciador do Sistema"](#)

Administração agregada

Crie um agregado para sistemas Cloud Volumes ONTAP

Você pode criar agregados sozinho ou deixar que o NetApp Console faça isso por você ao criar volumes. A vantagem de criar agregados você mesmo é que você pode escolher o tamanho do disco subjacente, o que permite dimensionar seu agregado de acordo com a capacidade ou o desempenho necessários.



Todos os discos e agregados devem ser criados e excluídos diretamente do Console. Você não deve executar essas ações a partir 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 **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique duas vezes no nome do sistema Cloud Volumes ONTAP no 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 e tamanho de disco, consulte "[Planeje sua configuração do Cloud Volumes ONTAP na AWS](#)".
- Se você for solicitado a inserir o tamanho da capacidade do agregado, estará criando um agregado em uma configuração compatível com o recurso Amazon EBS Elastic Volumes. A captura de tela a seguir mostra um exemplo de um novo agregado composto de discos gp3.

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 Elastic Volumes](#)".

Azul

Para obter ajuda com o tipo e tamanho do disco, consulte "[Planeje sua configuração do Cloud Volumes ONTAP no Azure](#)".

Google Cloud

Para obter ajuda com o tipo e tamanho do disco, consulte "[Planeje sua configuração do Cloud Volumes ONTAP no Google Cloud](#)".

4. Clique em **Adicionar** e depois em **Aprovar e Comprar**.

Gerenciar agregados para clusters do Cloud Volumes ONTAP

Gerencie agregados você mesmo adicionando discos, visualizando informações sobre os agregados e excluindo-os.



Todos os discos e agregados devem ser criados e excluídos diretamente do NetApp Console. Você não deve executar essas ações a partir 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

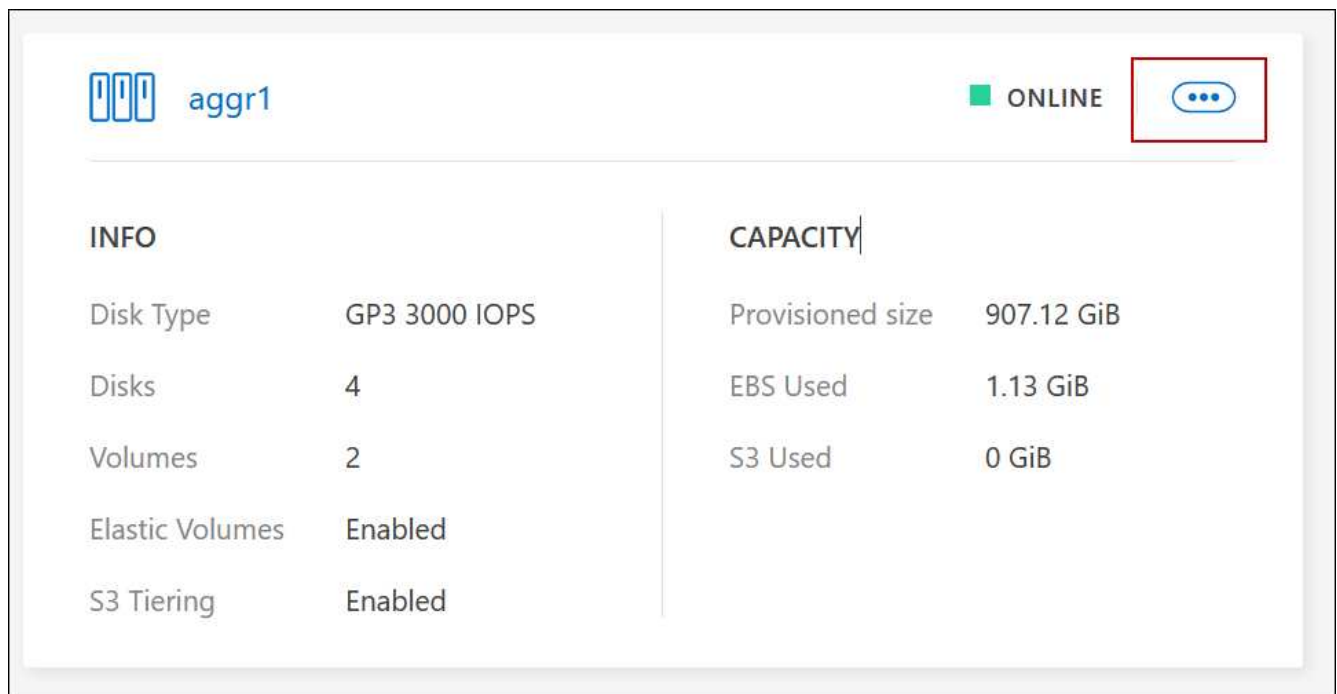
Se você quiser excluir um agregado, primeiro deverá excluir os volumes no agregado.

Sobre esta tarefa

Se um agregado estiver ficando sem espaço, você poderá mover volumes para outro agregado usando o ONTAP System Manager.

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique duas vezes no sistema Cloud Volumes ONTAP no qual você deseja gerenciar agregados.
3. Nos detalhes do sistema, clique na aba **Agregados**.
4. Para o agregado necessário, clique em  ícone para as ações de gerenciamento.



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		

5. Gerencie seus agregados a partir das opções disponíveis no  menu.



Para adicionar discos a um agregado, todos os discos no agregado devem ter o mesmo tamanho.

Para a AWS, você pode aumentar a capacidade de um agregado que oferece suporte ao Amazon EBS Elastic

Volumes.

1. Sob o  menu, clique em **Aumentar capacidade**.
2. Insira a capacidade adicional que você gostaria de adicionar e clique em **Aumentar**.

Observe que você deve aumentar a capacidade do agregado em no mínimo 256 GiB ou 10% do tamanho do agregado. Por exemplo, se você tiver um agregado de 1,77 TiB, 10% é 181 GiB. Isso é menor que 256 GiB, então o tamanho do agregado deve ser aumentado pelo mínimo de 256 GiB.

Gerenciar a capacidade agregada do Cloud Volumes ONTAP em um agente do Console

Cada agente do Console tem configurações que determinam como ele gerencia a capacidade agregada do Cloud Volumes ONTAP.

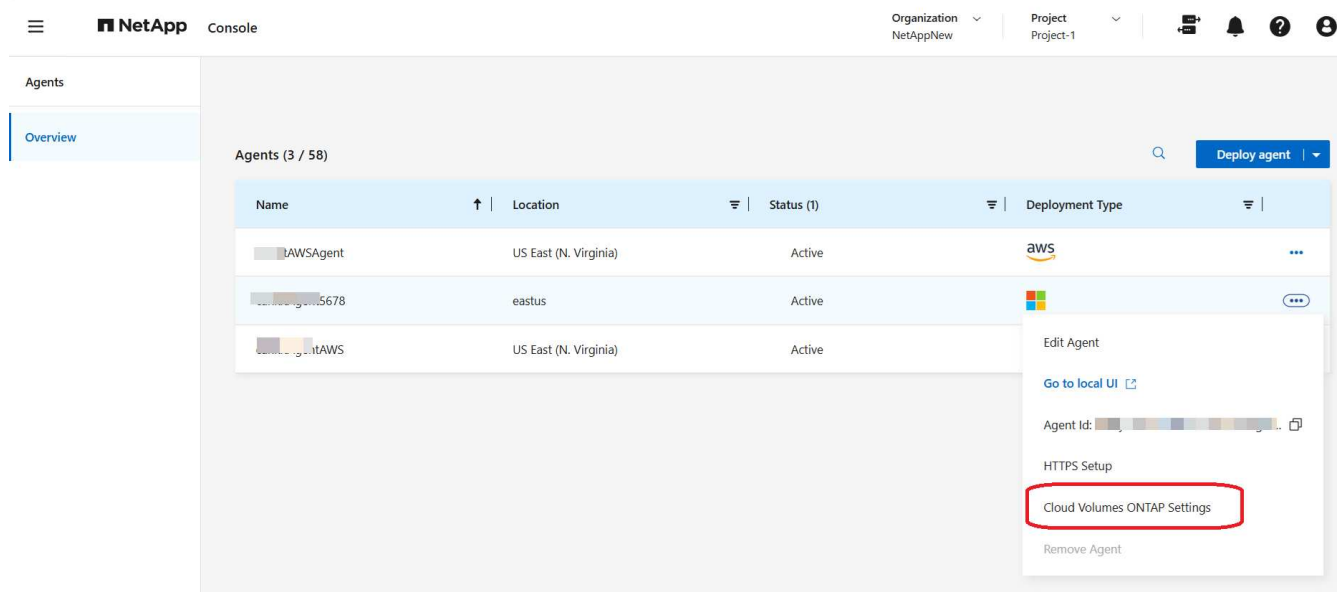
Essas configurações afetam todos os sistemas Cloud Volumes ONTAP gerenciados por um agente do Console. Se você tiver outro agente do Console, ele poderá ser configurado de forma diferente.

Permissões necessárias

Você precisa de privilégios de administrador de conta ou organização do NetApp Console para modificar as configurações do Cloud Volumes ONTAP .

Passos

1. No painel de navegação esquerdo, acesse **Administração > Agentes**.
2. Clique no  ícone para o agente do Console que gerencia seu sistema Cloud Volumes ONTAP .
3. Selecione * Configurações do Cloud Volumes ONTAP *.



The screenshot shows the NetApp Console interface. On the left, the 'Agents' section is selected. The main area displays a table of agents. The first agent, 'AWSAgent', is selected, and a context menu is open over it. The menu options are: 'Edit Agent', 'Go to local UI', 'Agent Id', 'HTTPS Setup', 'Cloud Volumes ONTAP Settings' (which is highlighted with a red rectangle), and 'Remove Agent'.

Name	Location	Status (1)	Deployment Type
AWSAgent	US East (N. Virginia)	Active	aws
5678	eastus	Active	
AWS	US East (N. Virginia)	Active	

4. Em **Capacidade**, modifique qualquer uma das seguintes configurações:

Edit Cloud Volumes ONTAP settings

Capacity

 Capacity Management Mode	Automatic Mode	▼
 Aggregate Capacity Thresholds - Free Space Ratio	10%	▼
 Aggregate Capacity Thresholds - Free Space Ratio for Data Tiering	10%	▼
 Volume Autosize - Additional Size in Percentage to Which Volumes Can Grow	1000%	▼

General

 Automatic Cloud Volumes ONTAP update during deployment	On	▼

Azure

 Azure CIFS locks for Azure HA systems	Off	▼
 Use Azure Private Link	On	▼

Modo de gerenciamento de capacidade

Escolha se o Console deve notificá-lo sobre decisões de capacidade de armazenamento ou se ele deve gerenciar automaticamente os requisitos de capacidade para você.

["Aprenda como funciona o Modo de Gerenciamento de Capacidade"](#) .

Limiar de Capacidade Agregada - Razão de Espaço Livre

Essa proporção é um parâmetro essencial nas decisões de gerenciamento de capacidade, e entender seu impacto é essencial, independentemente de você estar no modo automático ou manual de gerenciamento de capacidade. É recomendável definir esse limite considerando suas necessidades específicas de armazenamento e o crescimento previsto para manter um equilíbrio entre utilização de recursos e custo.

No modo manual, se a taxa de espaço livre em um agregado cair abaixo do limite especificado, uma notificação será disparada, alertando você de que 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 de serviço e garantir o desempenho ideal.

A relação de espaço livre é calculada da seguinte forma: (capacidade agregada - capacidade total utilizada no agregado) / capacidade agregada

Consulte ["Gerenciamento automático de capacidade"](#) para saber agora a capacidade é gerenciada automaticamente no Cloud Volumes ONTAP.

Limites de capacidade agregada - Proporção de espaço livre para hierarquização de dados

Define quanto espaço livre é necessário na camada de desempenho (discos) ao hierarquizar dados em uma camada de capacidade (armazenamento de objetos).

A proporção é importante para cenários de recuperação de desastres. À medida que os dados são lidos da camada de capacidade, o Cloud Volumes ONTAP move os dados para a camada de desempenho para fornecer melhor desempenho. Se não houver espaço suficiente, o Cloud Volumes ONTAP não poderá mover os dados.

5. Clique em **Salvar**.

Administração de VM de armazenamento

Gerenciar VMs de armazenamento para Cloud Volumes ONTAP

Uma VM de armazenamento é uma máquina virtual executada no ONTAP que fornece serviços de armazenamento e dados aos seus clientes. Você pode conhecer isso como *SVM* ou *vserver*. O Cloud Volumes ONTAP é configurado com uma VM de armazenamento por padrão, mas algumas configurações oferecem suporte a VMs de armazenamento adicionais.

Número suportado de VMs de armazenamento

Várias VMs de armazenamento são suportadas com determinadas configurações. Vá para o ["Notas de versão do Cloud Volumes ONTAP"](#) para verificar o número de VMs de armazenamento suportadas para sua versão do Cloud Volumes ONTAP.

Trabalhar com várias VMs de armazenamento

O NetApp Console oferece suporte a quaisquer VMs de armazenamento adicionais que você criar no ONTAP System Manager ou na CLI do ONTAP .

Por exemplo, a imagem a seguir mostra como você pode escolher uma VM de armazenamento ao criar um volume.

Details & Protection

Storage VM Name

svm_name1

Volume Name

Size (GiB)

Volume size

Snapshot Policy

default

Default Policy

E a imagem a seguir mostra como você pode escolher uma VM de armazenamento ao replicar um volume para outro sistema.

Destination Volume Name

volume_copy

Destination Storage VM Name

svm_name1

Destination Aggregate

Automatically select the best aggregate

Modifique o nome da VM de armazenamento padrão

O Console nomeia automaticamente a única VM de armazenamento que ele cria para o Cloud Volumes ONTAP. No ONTAP System Manager, na CLI ou na API do ONTAP , você pode modificar o nome da VM de armazenamento se tiver padrões de nomenclatura rígidos. Por exemplo, você pode querer que o nome corresponda à forma como você nomeia as VMs de armazenamento para seus clusters ONTAP .

Gerenciar VMs de armazenamento de serviço de dados para Cloud Volumes ONTAP na AWS

Uma VM de armazenamento é uma máquina virtual executada no ONTAP que fornece serviços de armazenamento e dados aos seus clientes. Você pode conhecer isso como SVM ou vserver. O Cloud Volumes ONTAP é configurado com uma VM de armazenamento por padrão, mas algumas configurações oferecem suporte a VMs de armazenamento adicionais.

Para criar VMs de armazenamento de serviço de dados adicionais, você precisa alocar endereços IP na AWS e, em seguida, executar comandos ONTAP com base na sua configuração do Cloud Volumes ONTAP .

Número suportado de VMs de armazenamento

Várias VMs de armazenamento são suportadas com configurações específicas do Cloud Volumes ONTAP a partir da versão 9.7. Vá para o "[Notas de versão do Cloud Volumes ONTAP](#)" para verificar o número de VMs de armazenamento suportadas para sua versão do Cloud Volumes ONTAP.

Todas as outras configurações do Cloud Volumes ONTAP oferecem suporte a uma VM de armazenamento de serviço de dados e uma VM de armazenamento de destino usada para recuperação de desastres. Você pode ativar a VM de armazenamento de destino para acesso a dados se houver uma interrupção na VM de armazenamento de origem.

Verifique os limites para 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 o "[Seção de limites de armazenamento nas Notas de versão do Cloud Volumes ONTAP](#)" .
2. Identifique o número máximo de endereços IP por interface para seu 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

Endereços IPv4 privados devem ser atribuídos à porta e0a na AWS antes de você criar LIFs para a nova VM de armazenamento.

Observe que um LIF de gerenciamento opcional para uma VM de armazenamento requer um endereço IP privado em um único sistema de nó e em um par de HA em uma única AZ. Este 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 armazenamento em um par de HA, selecione o nó 1.

3. Role para baixo até **Interfaces de rede** e clique em **ID da interface** para a porta e0a.

	Name	Insta...	Instance state	Instance type	Status check
☐	danielleAws	i-070...	Running	m5.2xlarge	2/2 check
☐	occmTiering0702	i-0a7...	Stopped	m5.2xlarge	-
☒	cvoTiering1	i-02a...	Stopped	m5.2xlarge	-

Interface ID	Description
eni-07c301...	Interface for Node & Cluster Management, Inter-Cluster Communication, and Data - 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: acesse a CLI do ONTAP para o Cloud Volumes ONTAP e execute **network interface show** para confirmar se 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 **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 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 várias 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 várias AZs, precisará repetir essas etapas para o nó 2.

Crie uma VM de armazenamento em um sistema de nó único

Essas etapas criam uma nova VM de armazenamento em um sistema de nó único. Um endereço IP privado é necessário para criar um NAS LIF 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 ela.

```
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 em e0a.

3. Opcional: crie um LIF de gerenciamento de VM de armazenamento.

```
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 em e0a.

4. Atribua um ou mais agregados à VM de armazenamento.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Esta etapa é necessária porque a nova VM de armazenamento precisa acessar pelo menos um agregado antes que você possa criar volumes na VM de armazenamento.

Crie uma VM de armazenamento em um par de HA em uma única AZ

Essas etapas criam uma nova VM de armazenamento em um par de HA em uma única AZ. Um endereço IP privado é necessário para criar um NAS LIF 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 ser movidos entre nós se ocorrerem falhas.

Passos

1. Crie a VM de armazenamento e uma rota para ela.

```
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 em e0a de cvo-node1. Este endereço IP pode ser realocado para o e0a do cvo-node2 em caso de aquisição porque a política de serviço default-data-files indica que os IPs podem migrar para o nó parceiro.

3. Opcional: crie um LIF de gerenciamento de VM de armazenamento 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 em e0a.

4. Atribua um ou mais agregados à VM de armazenamento.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Esta etapa é necessária porque a nova VM de armazenamento precisa acessar pelo menos um agregado antes que você possa criar volumes na VM de armazenamento.

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 armazenamento.

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 armazenamento em um par de HA em várias AZs

Essas etapas criam uma nova VM de armazenamento em um par de HA em várias AZs.

Um endereço IP *flutuante* é necessário para um NAS LIF 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 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, onde um iSCSI LIF é criado no nó 1 e no nó 2.

Passos

1. Crie a VM de armazenamento e uma rota para ela.

```
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 todas as VPCs na região da AWS na qual você implanta 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 parceiro.

3. Opcional: crie um LIF de gerenciamento de VM de armazenamento 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 dar suporte à migração LIF dos IPs flutuantes na VM de armazenamento. 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 na 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 dar suporte à migração LIF dos IPs flutuantes na VM de armazenamento. 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 na eth0 (e0a) do `cvo_node2`.

6. Atribua um ou mais agregados à VM de armazenamento.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Esta etapa é necessária porque a nova VM de armazenamento precisa acessar pelo menos um agregado antes que você possa criar volumes na VM de armazenamento.

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 armazenamento.

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
```

Gerenciar VMs de armazenamento de serviço de dados para Cloud Volumes ONTAP no Azure

Uma VM de armazenamento é uma máquina virtual executada no ONTAP que fornece serviços de armazenamento e dados aos seus clientes. Você pode conhecer isso como SVM ou vserver. O Cloud Volumes ONTAP é configurado com uma VM de armazenamento por padrão, mas você pode criar VMs de armazenamento adicionais ao executar o Cloud Volumes ONTAP no Azure.

Para criar e gerenciar VMs adicionais de armazenamento de dados no Azure, você deve usar as APIs. Isso ocorre porque as APIs automatizam o processo de criação de VMs de armazenamento e configuração das interfaces de rede necessárias. Ao criar as VMs de armazenamento, o NetApp Console configura os serviços LIF necessários, bem como um LIF iSCSI necessário para comunicações SMB/CIFS de saída da VM de armazenamento.

Para obter informações sobre como executar chamadas de API Cloud Volumes ONTAP, consulte ["Sua primeira chamada de API"](#).

Número suportado de VMs de armazenamento

A partir do Cloud Volumes ONTAP 9.9.0, com base na sua licença, várias VMs de armazenamento são suportadas com configurações específicas. Consulte o ["Notas de versão do Cloud Volumes ONTAP"](#) para verificar o número de VMs de armazenamento suportadas para sua versão do Cloud Volumes ONTAP.

Todas as versões do Cloud Volumes ONTAP anteriores à 9.9.0 oferecem suporte a uma VM de armazenamento de serviço de dados e uma VM de armazenamento de destino usada para recuperação de desastres. Você pode ativar a VM de armazenamento de destino para acesso a dados se houver uma interrupção na VM de armazenamento de origem.

Criar uma VM de armazenamento

Com base na sua configuração e no tipo de licença, você pode criar várias VMs de armazenamento em um único sistema de nó ou em uma configuração de alta disponibilidade (HA) usando as APIs do NetApp Console.

Sobre esta tarefa

Ao criar VMs de armazenamento usando as APIs, juntamente com a configuração das interfaces de rede necessárias, o Console também modifica as `default-data-files` políticas nas VMs de armazenamento de dados removendo os seguintes serviços do LIF de dados do NAS e adicionando-os ao LIF de dados do iSCSI usado para conexões de gerenciamento de saída:

- `data-fpolicy-client`
- `management-ad-client`
- `management-dns-client`
- `management-ldap-client`
- `management-nis-client`

Antes de começar

O agente do Console requer permissões específicas para criar VMs de armazenamento para o Cloud Volumes ONTAP. As permissões necessárias estão incluídas em ["as políticas fornecidas pela NetApp"](#).

Sistema de nó único

Use a seguinte chamada de API para criar uma VM de armazenamento em um sistema de nó único.

POST /azure/vsa/working-environments/{workingEnvironmentId}/svm

Inclua os seguintes parâmetros no corpo da solicitação:

```
{ "svmName": "myNewSvm1"
  "svmPassword": "optional, the API takes the cluster password if not
provided"
  "mgmtLif": "optional, to create an additional management LIF, if you
want to use the storage VM for management purposes"}
```

Par HA

Use a seguinte chamada de API para criar uma VM de armazenamento em um par de HA:

POST /azure/ha/working-environments/{workingEnvironmentId}/svm

Inclua os seguintes parâmetros no corpo da solicitação:

```
{ "svmName": "NewSvmName"
  "svmPassword": "optional value, the API takes the cluster password if
not provided"
  "mgmtLif": "optional value, to create an additional management LIF, if
you want to use the storage VM for management purposes"}
```

Gerenciar VMs de armazenamento em sistemas de nó único e pares de HA

Usando as APIs, você pode renomear e excluir VMs de armazenamento em configurações de nó único e HA.

Antes de começar

O agente do Console requer permissões específicas para gerenciar VMs de armazenamento para o Cloud Volumes ONTAP. As permissões necessárias estão incluídas em ["as políticas fornecidas pela NetApp"](#).

Renomear uma VM de armazenamento

Para renomear uma VM de armazenamento, você deve fornecer os nomes da VM de armazenamento existente e da nova VM de armazenamento como parâmetros.

Passos

- Use a seguinte chamada de API para renomear uma VM de armazenamento em um sistema de nó único:

PUT /azure/vsa/working-environments/{workingEnvironmentId}/svm

Inclua os seguintes parâmetros no corpo da solicitação:

```
{
  "svmNewName": "NewSvmName",
  "svmName": "OldSvmName"
}
```

- Use a seguinte chamada de API para renomear uma VM de armazenamento em um par de HA:

```
PUT /azure/ha/working-environments/{workingEnvironmentId}/svm
```

Inclua os seguintes parâmetros no corpo da solicitação:

```
{
  "svmNewName": "NewSvmName",
  "svmName": "OldSvmName"
}
```

Excluir uma VM de armazenamento

Em uma configuração de nó único ou HA, você pode remover uma VM de armazenamento se ela não tiver nenhum volume ativo.

Passos

- Use a seguinte chamada de API para excluir uma VM de armazenamento em um sistema de nó único:

```
DELETE /azure/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}
```

- Use a seguinte chamada de API para excluir uma VM de armazenamento em um par de HA:

```
DELETE /azure/ha/working-environments/{workingEnvironmentId}/svm/{svmName}
```

Informações relacionadas

- ["Prepare-se para usar a API"](#)
- ["Fluxos de trabalho do Cloud Volumes ONTAP"](#)
- ["Obtenha os identificadores necessários"](#)
- ["Use as APIs REST para o NetApp Console"](#)

Gerenciar VMs de armazenamento de dados para o Cloud Volumes ONTAP no Google Cloud

Uma VM de armazenamento é uma máquina virtual executada no ONTAP que fornece serviços de armazenamento e dados aos seus clientes. Você pode conhecer isso como SVM ou vserver. O Cloud Volumes ONTAP é configurado com uma VM de armazenamento por padrão, mas algumas configurações oferecem suporte a VMs de armazenamento adicionais.

Para criar e gerenciar VMs adicionais de armazenamento de dados no Google Cloud, você deve usar as APIs. Isso ocorre porque as APIs automatizam o processo de criação de VMs de armazenamento e configuração das interfaces de rede necessárias. Ao criar as VMs de armazenamento, o NetApp Console configura os serviços LIF necessários, bem como um LIF iSCSI necessário para comunicações SMB/CIFS de saída da VM de armazenamento.

Para obter informações sobre como executar chamadas de API Cloud Volumes ONTAP, consulte ["Sua primeira chamada de API"](#).

Número suportado de VMs de armazenamento

A partir do Cloud Volumes ONTAP 9.11.1, com base na sua licença, várias VMs de armazenamento são suportadas com configurações específicas. Consulte o ["Notas de versão do Cloud Volumes ONTAP"](#) para verificar o número de VMs de armazenamento suportadas para sua versão do Cloud Volumes ONTAP.

Todas as versões do Cloud Volumes ONTAP anteriores à 9.11.1 oferecem suporte a uma VM de armazenamento de serviço de dados e uma VM de armazenamento de destino usada para recuperação de desastres. Você pode ativar a VM de armazenamento de destino para acesso a dados se houver uma interrupção na VM de armazenamento de origem.

Criar uma VM de armazenamento

Com base na sua configuração e no tipo de licença, você pode criar várias VMs de armazenamento em um único sistema de nó ou em uma configuração de alta disponibilidade (HA) usando as APIs.

Sobre esta tarefa

Ao criar VMs de armazenamento usando as APIs, juntamente com a configuração das interfaces de rede necessárias, o Console também modifica as `default-data-files` políticas nas VMs de armazenamento de dados removendo os seguintes serviços do LIF de dados do NAS e adicionando-os ao LIF de dados do iSCSI usado para conexões de gerenciamento de saída:

- `data-fpolicy-client`
- `management-ad-client`
- `management-dns-client`
- `management-ldap-client`
- `management-nis-client`

Antes de começar

O agente do Console requer permissões específicas para criar VMs de armazenamento para pares de HA do Cloud Volumes ONTAP. As permissões necessárias estão incluídas em ["as políticas fornecidas pela NetApp"](#).

Sistema de nó único

Use a seguinte chamada de API para criar uma VM de armazenamento em um sistema de nó único.

```
POST /gcp/vsa/working-environments/{workingEnvironmentId}/svm
```

Inclua os seguintes parâmetros no corpo da solicitação:

```
{ "svmName": "NewSvmName"
  "svmPassword": "optional value, the API takes the cluster password if
not provided"
  "mgmtLif": "optional value, to create an additional management LIF, if
you want to use the storage VM for management purposes"}
```

Par HA

Use a seguinte chamada de API para criar uma VM de armazenamento em um par de HA:

POST /gcp/ha/working-environments/{workingEnvironmentId}/svm/

Inclua os seguintes parâmetros no corpo da solicitação:

```
{ "svmName": "NewSvmName"
  "svmPassword": "optional value, the API takes the cluster password if
not provided"
}
```

Gerenciar VMs de armazenamento

Usando as APIs, você pode renomear e excluir VMs de armazenamento em configurações de nó único e HA.

Antes de começar

O agente do Console requer permissões específicas para gerenciar VMs de armazenamento para pares de alta disponibilidade do Cloud Volumes ONTAP . As permissões necessárias estão incluídas em ["as políticas fornecidas pela NetApp"](#) .

Renomear uma VM de armazenamento

Para renomear uma VM de armazenamento, você deve fornecer os nomes da VM de armazenamento existente e da nova VM de armazenamento como parâmetros.

Passos

- Use a seguinte chamada de API para renomear uma VM de armazenamento em um sistema de nó único:

PUT /gcp/vsa/working-environments/{workingEnvironmentId}/svm

Inclua os seguintes parâmetros no corpo da solicitação:

```
{
  "svmNewName": "NewSvmName",
  "svmName": "OldSvmName"
}
```

- Use a seguinte chamada de API para renomear uma VM de armazenamento em um par de HA:

```
PUT /gcp/ha/working-environments/{workingEnvironmentId}/svm
```

Inclua os seguintes parâmetros no corpo da solicitação:

```
{
  "svmNewName": "NewSvmName",
  "svmName": "OldSvmName"
}
```

Excluir uma VM de armazenamento

Em uma configuração de nó único ou HA, você pode remover uma VM de armazenamento se ela não tiver nenhum volume ativo.

Passos

- Use a seguinte chamada de API para excluir uma VM de armazenamento em um sistema de nó único:

```
DELETE /gcp/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}
```

- Use a seguinte chamada de API para excluir uma VM de armazenamento em um par de HA:

```
DELETE /gcp/ha/working-environments/{workingEnvironmentId}/svm/{svmName}
```

Informações relacionadas

- ["Prepare-se para usar a API"](#)
- ["Fluxos de trabalho do Cloud Volumes ONTAP"](#)
- ["Obtenha os identificadores necessários"](#)
- ["Use as APIs REST para o NetApp Console"](#)

Configurar recuperação de desastres de VM de armazenamento para Cloud Volumes ONTAP

O NetApp Console não oferece suporte de configuração ou orquestração para recuperação de desastres de VM de armazenamento (SVM). Para executar essas tarefas, use o ONTAP System Manager ou o ONTAP CLI.

Se você configurar a replicação do SnapMirror SVM entre dois sistemas Cloud Volumes ONTAP, a replicação deverá ser entre dois sistemas de pares 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 instruções do ONTAP CLI.

- ["Guia expresso de preparação para recuperação de desastres do SVM"](#)
- ["Guia de Recuperação de Desastres SVM Express"](#)

Segurança e criptografia de dados

Criptografe volumes no Cloud Volumes ONTAP com soluções de criptografia da NetApp

O Cloud Volumes ONTAP oferece suporte ao NetApp Volume Encryption (NVE) e ao NetApp Aggregate Encryption (NAE). NVE e NAE são soluções baseadas em software que permitem a criptografia de dados em repouso de volumes compatível com FIPS 140-2. ["Saiba mais sobre essas soluções de criptografia"](#) .

Tanto o NVE quanto o NAE são suportados por um gerenciador de chaves externo.

```
] fim se::aws[] ifdef::azure[] fim se::azure[] ifdef::gcp[] fim se::gcp[] ifdef::aws[] fim se::aws[] ifdef::azure[] fim  
se::azure[] ifdef::gcp[] fim se::gcp[]
```

Gerencie chaves de criptografia Cloud Volumes ONTAP 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 ponto de extremidade de gerenciamento de chaves da 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 corretamente o serviço de gerenciamento de chaves.

Antes de começar

- O Cloud Volumes ONTAP deve estar executando a versão 9.12.0 ou posterior
- Você deve ter instalado a licença de Criptografia de Volume (VE) e
- Você deve ter instalada a licença do Multi-tenant Encryption Key Management (MTEKM).
- Você deve ser um administrador de cluster ou SVM
- Você deve ter uma assinatura ativa da AWS



Você só pode configurar chaves para um SVM de dados.

Configuração

AWS

1. Você deve criar um ["conceder"](#) para a chave AWS KMS que será usada pela função do IAM que gerencia a criptografia. A função do IAM deve incluir uma política que permita as seguintes operações:
 - DescribeKey
 - Encrypt
 - Decrypt Para criar uma subvenção, consulte ["Documentação do AWS"](#) .
2. ["Adicione uma política à função do IAM apropriada."](#) A política deve apoiar a DescribeKey , Encrypt , e Decrypt operações.

Cloud Volumes ONTAP

1. Mude para 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, digite a chave secreta.
5. Confirme se o AWS KMS foi configurado corretamente:
`security key-manager external aws show -vserver svm_name`

Gerencie chaves de criptografia Cloud Volumes ONTAP com o Azure Key Vault

Você pode usar o Azure Key Vault (AKV) para proteger suas chaves de criptografia ONTAP em um aplicativo implantado pelo Azure. Consulte o ["Documentação da Microsoft"](#) .

O AKV pode ser usado para proteger chaves do NetApp Volume Encryption (NVE) somente para SVMs de dados. Para mais informações, consulte o ["Documentação do ONTAP"](#) .

O gerenciamento de chaves com o AKV pode ser habilitado com a CLI ou a API REST do ONTAP .

Ao usar o AKV, esteja ciente de que, por padrão, um SVM LIF de dados é usado para se comunicar com o ponto de extremidade 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 corretamente 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 Criptografia de Volume (VE) instalada (a licença de Criptografia de Volume da NetApp é instalada automaticamente em cada sistema Cloud Volumes ONTAP registrado no Suporte da NetApp)
- Você deve ter uma licença de gerenciamento de chaves de criptografia multilocatário (MT_EK_MGMT)
- Você deve ser um administrador de cluster ou SVM
- Uma assinatura do Active Azure

Limitações

- O AKV só pode ser configurado em um SVM de dados
- NAE não pode ser usado com AKV. O NAE requer um servidor KMIP com suporte externo.
- Os nós Cloud Volumes ONTAP pesquisam o AKV a cada 15 minutos para confirmar a acessibilidade e a disponibilidade das chaves. Este período de pesquisa não é configurável e, após quatro falhas consecutivas na tentativa de pesquisa (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 Azure Key Vault e chaves. Se você já concluiu essas etapas, certifique-se de ter as configurações corretas, principalmente em [Criar um Azure Key Vault](#) , e então prossiga para [Configuração do](#)

- [Registro de aplicativo do Azure](#)
- [Criar segredo do cliente do Azure](#)
- [Criar um Azure Key Vault](#)
- [Criar chave de criptografia](#)
- [Criar um ponto de extremidade do Azure Active Directory \(somente HA\)](#)
- [Configuração do Cloud Volumes ONTAP](#)

Registro de aplicativo do Azure

1. Primeiro, você deve registrar seu aplicativo na assinatura do Azure que deseja que o Cloud Volumes ONTAP use para acessar o Azure Key Vault. No portal do Azure, selecione **Registros de aplicativos**.
2. Selecione **Novo registro**.
3. Forneça um nome para seu 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 do cliente do Azure

1. No portal do Azure para registro do aplicativo Azure Key Vault, selecione o painel **Certificados e segredos**.
2. Selecione **Novo segredo do cliente**. Insira um nome significativo para o seu 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 sequência secreta listada na coluna **Valor** e armazene-a em um local seguro para uso posterior em [Configuração do Cloud Volumes ONTAP](#) . O valor secreto não será exibido novamente depois que você sair da página.

Criar um Azure Key Vault

1. Se você tiver um Azure Key Vault existente, poderá conectá-lo à sua configuração do Cloud Volumes ONTAP ; no entanto, você deve adaptar as políticas de acesso às configurações neste 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 preço. Além disso, insira o número de dias para manter os cofres excluídos e selecione **Ativar proteção de limpeza** 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 cofre**.
 - b. Em **Acesso a recursos**, selecione **Azure Disk Encryption 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 **Gerenciamento de chaves, segredos e certificados**.
8. Escolha cada um dos menus suspensos de permissões (chave, segredo, certificado) e depois **Selecionar tudo** no topo da lista do menu para selecionar todas as permissões disponíveis. Você deve ter:

- **Permissões de chave:** 20 selecionadas
- **Permissões secretas:** 8 selecionadas
- **Permissões de certificado:** 16 selecionadas

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 **Avançar** para selecionar o aplicativo registrado **Principal** do Azure que você criou em [Registro de aplicativo do Azure](#) . Selecione **Avançar**.



Somente 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 **Avançar** duas vezes até chegar em **Revisar e criar**. Em seguida, clique em **Criar**.
11. Selecione **Avançar** para avançar para as opções de **Rede**.
12. Escolha o método de acesso à rede apropriado ou selecione **Todas as redes** e **Revisar + Criar** para criar o cofre de chaves. (O método de acesso à rede pode ser prescrito por uma política de governança ou pela sua equipe corporativa de segurança na nuvem.)
13. Registre o URI do Key Vault: No key vault que você criou, navegue até o menu Visão geral e copie o **URI do Vault** da coluna da direita. Você precisará disso para uma etapa posterior.

Criar chave de criptografia

1. No menu do Key Vault que você criou para o Cloud Volumes ONTAP, navegue até a opção **Chaves**.
2. Selecione **Gerar/importar** para criar uma nova chave.
3. Deixe a opção padrão definida como **Gerar**.
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 **Chaves** e selecione a chave que você acabou de criar.
7. Selecione o ID da chave em **Versão atual** para visualizar as propriedades da chave.
8. Localize o campo **Identificador de chave**. Copie o URI até, mas não incluindo, a string hexadecimal.

Criar um ponto de extremidade do Azure Active Directory (somente HA)

1. Este processo só é necessário se você estiver configurando o Azure Key Vault para um sistema HA Cloud Volumes ONTAP .
2. No portal do Azure, navegue até **Redes Virtuais**.
3. Selecione a Rede Virtual onde você implantou o sistema Cloud Volumes ONTAP e selecione o menu **Sub-redes** no lado esquerdo da página.
4. Selecione o nome da sub-rede para sua implantação do Cloud Volumes ONTAP na lista.
5. Navegue até o título **Pontos de extremidade de serviço**. No menu suspenso, 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 **Salvar** para capturar suas configurações.

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 o SVM de dados desejado e verifique sua configuração de DNS:

```
vserver services name-service dns show
```

- a. Se existir uma entrada DNS para o SVM de dados desejado e ela 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 SVM do administrador do cluster:

```
vserver services name-service dns create -vserver SVM_name -domains domain  
-name-servers IP_address
```

- b. Verifique se o serviço DNS foi criado para o SVM de dados:

```
vserver services name-service dns show
```

4. Habilite o Azure Key Vault usando a ID do cliente e a ID do locatário salvas 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` o valor deve utilizar o `<https:// <key vault host name>/keys/<key label>` formatar.

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 é `OK`, o SVM não consegue acessar o serviço Azure Key Vault com toda a conectividade e permissões necessárias. Certifique-se de que suas políticas de rede e roteamento do Azure não bloqueiem sua vNet privada de alcançar o ponto de extremidade público do Azure Key Vault. Se isso acontecer, considere usar um ponto de extremidade privado do Azure para acessar o Key Vault de dentro da vNet. Também pode ser necessário adicionar uma entrada de hosts

estáticos no seu SVM para resolver o endereço IP privado do seu ponto de extremidade.

O `kms_wrapped_key_status` irá relatar 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 habilitará a criptografia do 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
```

9. Opcional: se você quiser atualizar as credenciais no certificado de autenticação do Azure Key Vault, use o seguinte comando:

```
security key-manager external azure update-credentials -vserver v1  
-authentication-method certificate
```

Links relacionados

- ["Configurar o Cloud Volumes ONTAP para usar uma chave gerenciada pelo cliente no Azure"](#)
- ["Documentação do Microsoft Azure: Sobre o Azure Key Vault"](#)
- ["Guia de referência de comando ONTAP"](#)

Gerencie chaves de criptografia Cloud Volumes ONTAP com o Google Cloud KMS

Você pode usar ["Serviço de gerenciamento de chaves da plataforma Google Cloud \(Cloud KMS\)"](#) para proteger suas chaves de criptografia Cloud Volumes ONTAP em um aplicativo implantado no Google Cloud Platform.

O gerenciamento de chaves com o Cloud KMS pode ser habilitado com o ONTAP CLI ou o ONTAP REST API.

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 ponto de extremidade de gerenciamento de chaves da 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 corretamente o serviço de gerenciamento de chaves.

Antes de começar

- Seu sistema deve estar executando o Cloud Volumes ONTAP 9.10.1 ou posterior
- Você deve usar um SVM de dados. O Cloud KMS pode ser configurado somente em um SVM de dados.
- Você deve ser um administrador de cluster ou SVM
- A licença de Criptografia de Volume (VE) deve ser instalada no SVM
- A partir do Cloud Volumes ONTAP 9.12.1 GA, a licença de gerenciamento de chaves de criptografia multilocatário (MTEKM) também deve ser instalada
- É necessária uma assinatura ativa do Google Cloud Platform

Configuração

Google Cloud

1. No seu ambiente do Google Cloud, ["crie um chaveiro e uma chave GCP simétricos"](#) .
2. Atribua uma função personalizada à chave do Cloud KMS e à conta de serviço do Cloud Volumes ONTAP .
 - a. Crie a função personalizada:

```
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.locations.get,cloudkms.locations.list,resourceManager.projects.get
  --stage=GA
```

- b. Atribua a função personalizada que você criou:

```
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
```



Se você estiver no Cloud Volumes ONTAP 9.13.0 ou posterior, não precisará criar uma função personalizada. Você pode atribuir o `predefinido[cloudkms.cryptoKeyEncrypterDecrypter ^]` papel.

3. Baixe 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. Crie 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 da sua conta do GCP.

6. Confirme se o processo habilitado 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`

Solução de problemas

Se precisar solucionar problemas, você pode seguir os logs brutos da API REST nas duas etapas finais acima:

1. `set d`
2. `systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2_client.log`

Habilite soluções de proteção contra ransomware da NetApp para Cloud Volumes ONTAP

Ataques de ransomware podem custar tempo, recursos e reputação a uma empresa. O NetApp Console permite que você implemente duas soluções NetApp para ransomware: proteção contra extensões de arquivo comuns de ransomware e proteção autônoma contra ransomware (ARP). Essas soluções fornecem ferramentas eficazes para visibilidade, detecção e correção.

Proteção contra extensões de arquivo comuns de ransomware

Disponível no Console, a configuração Proteção contra Ransomware permite que você utilize a funcionalidade ONTAP FPolicy para se proteger contra tipos comuns de extensão de arquivo de ransomware.

Passos

1. Na página **Sistemas**, clique duas vezes no nome do sistema Cloud Volumes ONTAP que você configurou para usar proteção contra ransomware.
2. Na guia Visão geral, clique no painel Recursos e depois clique no ícone de lápis ao lado de **Proteção contra ransomware**.

Information	Features
System Tags	3 Tags 
Scheduled Downtime	Off 
Blob Access Tiering	Hot 
Instance Type	Standard_E8ds_v4 
Charging Method	Capacity-based 
Write Speed	<i>Not Supported</i> 
Ransomware Protection	Off 
Support Registration	Not Registered 
WORM	Disabled 
CIFS Setup	

3. Implemente a solução NetApp para ransomware:

- Clique em **Ativar política de instantâneo**, se você tiver volumes que não tenham uma política de instantâneo habilitada.

A tecnologia NetApp Snapshot oferece a melhor solução do setor para remediação de ransomware. A chave para uma recuperação bem-sucedida é restaurar a partir de backups não infectados. As cópias de instantâneos são somente leitura, o que evita a corrupção por 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 habilitar a solução FPolicy da ONTAP, que pode bloquear operações de arquivo com base na extensão do arquivo.

Esta solução preventiva melhora a proteção contra ataques de ransomware ao bloquear 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, encryptedRS, crjoker, EnCiPhErEd, LeChiffre



Este escopo é criado quando você ativa o FPolicy no Cloud Volumes ONTAP. A lista é baseada em tipos comuns de arquivos de ransomware. Você pode personalizar as extensões de arquivo bloqueadas usando os comandos `vserver fpolicy policy 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 Autonomous Ransomware Protection (ARP), que realiza análises em cargas de trabalho para detectar e alertar 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 ataques potenciais com base na "atividade anormal" detectada. 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 assinaturas de licença própria (BYOL) e de mercado 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 ONTAP System Manager e do ONTAP CLI.

Para obter mais informações sobre como habilitar o ARP com o ONTAP System Manager e o ONTAP CLI, consulte o "[Documentação do ONTAP : Habilitar proteção autônoma contra ransomware](#)".

Autonomous Ransomware Protection

0 TiB

Protected Capacity

100 TiB

Precommitted capacity

0 TiB

PAYGO

BYOL

100 TiB

Marketplace Contracts

0 TiB

Crie cópias instantâneas invioláveis de arquivos WORM no Cloud Volumes ONTAP

Você pode criar cópias instantâneas invioláveis de arquivos WORM (gravação única, leitura múltipla) em um sistema Cloud Volumes ONTAP e manter os instantâneos em formato inalterado por um período de retenção específico. Essa funcionalidade é alimentada pela tecnologia SnapLock e fornece uma camada adicional de proteção de dados e conformidade.

Antes de começar

Certifique-se de que o volume usado para criar cópias do Snapshot seja um volume SnapLock . Para obter informações sobre como habilitar a proteção SnapLock em volumes, consulte o ["Documentação do ONTAP : Configurar SnapLock"](#) .

Passos

1. Crie cópias de Snapshot do volume SnapLock . Para obter informações sobre como criar cópias de Snapshot usando a CLI ou o System Manager, consulte o ["Documentação do ONTAP : Visão geral do gerenciamento de cópias de instantâneos locais"](#) .

As cópias do Snapshot herdam as propriedades WORM do volume, tornando-as à prova de violação. A tecnologia SnapLock subjacente garante que um instantâneo permaneça protegido contra edição e exclusão até que o período de retenção especificado tenha decorrido.

2. Você pode modificar o período de retenção se houver necessidade de editar esses instantâneos. Para obter informações, consulte o ["Documentação ONTAP : Definir o tempo de retenção"](#) .



Embora uma cópia do Snapshot seja protegida por um período de retenção específico, o volume de origem pode ser excluído por um administrador de cluster, já que o armazenamento WORM no Cloud Volumes ONTAP opera sob um modelo de "administrador de armazenamento confiável". Além disso, um administrador de nuvem confiável pode excluir os dados WORM operando nos recursos de armazenamento em nuvem.

Administração do sistema

Atualizar o software Cloud Volumes ONTAP

Atualize o Cloud Volumes ONTAP no NetApp Console para obter 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 somente do console

Você não deve atualizar o Cloud Volumes ONTAP usando o ONTAP System Manager ou o ONTAP CLI, mas apenas o Console. Caso contrário, isso pode afetar a estabilidade do sistema.

Como atualizar

O Console oferece duas maneiras de atualizar o Cloud Volumes ONTAP:

- Seguindo as notificações de atualização que aparecem no sistema
- Ao colocar a imagem de atualização em um local HTTPS e, em seguida, fornecer ao Console 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 no momento.

Versão atual	Versões para as quais você pode atualizar diretamente
9.16.1 (somente para Azure e Google Cloud)	9.17.1 (somente para Azure e Google Cloud)
9.15.1	9.16.1 (somente para Azure e Google Cloud)
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
9.12.1	9.13.1
	9.13.0
9.12.0	9.12.1

Versão atual	Versões para as quais você pode atualizar diretamente
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 suportados para o Cloud Volumes ONTAP são diferentes daqueles para um cluster ONTAP local.
- Se você atualizar seguindo as notificações que aparecem em um sistema, o Console 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, certifique-se de seguir estes caminhos de atualização suportados.
- Em alguns casos, pode ser necessário atualizar algumas vezes para atingir a versão desejada.

Por exemplo, se você estiver executando a versão 9.8 e quiser atualizar para a 9.10.1, primeiro precisará atualizar para a versão 9.9.1 e depois para a 9.10.1.

Lançamentos de patches

A partir de janeiro de 2024, as atualizações de patch só estarão disponíveis se houver um lançamento de patch para as três versões mais recentes do Cloud Volumes ONTAP. Versões de patch ocasionalmente estão disponíveis para implantação, quando a versão RC ou GA não está disponível para implantação.

Usamos a versão mais recente do GA para determinar as três versões mais recentes a serem exibidas no Console. Por exemplo, se a versão atual do GA for 9.13.1, os patches para 9.11.1-9.13.1 aparecerão no Console. Se você quiser atualizar para uma versão de patch para versões 9.11.1 ou inferiores, você precisará usar o procedimento de atualização manual por [baixando a imagem ONTAP](#).

Como regra geral para lançamentos de patch (P), você pode atualizar de uma versão para qualquer versão P da versão atual que você está executando ou para a próxima versão.

Aqui estão alguns exemplos:

- 9.13.0 > 9.13.1P15
- 9.12.1 > 9.13.1P2

Revertendo ou rebaixando

Não há suporte para reverter ou fazer downgrade do Cloud Volumes ONTAP para uma versão anterior.

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 traga sua própria licença (BYOL). Você precisará ["registrar manualmente os sistemas PAYGO"](#), enquanto os sistemas BYOL são registrados por padrão.



Um sistema que não esteja registrado para suporte ainda receberá notificações de atualização de software que aparecem no Console quando uma nova versão estiver disponível. Mas você precisará registrar o sistema antes de poder atualizar o software.

Atualizações do mediador HA

O Console também atualiza a instância do mediador conforme necessário durante o processo de atualização do Cloud Volumes ONTAP.

Atualizações na AWS com tipos de instância EC2 c4, m4 e r4

O Cloud Volumes ONTAP não oferece mais suporte aos tipos de instância EC2 c4, m4 e r4. 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 [alterar o tipo de instância](#). Se você não puder alterar o tipo de instância, você precisa [habilitar rede aprimorada](#) antes de atualizar. Leia as seções a seguir para saber mais sobre como alterar o tipo de instância e habilitar a rede aprimorada.

No Cloud Volumes ONTAP executando versões 9.13.0 e superiores, não é possível atualizar com os tipos de instância EC2 c4, m4 e r4. Neste caso, você precisa reduzir o número de discos e então [alterar o tipo de instância](#) ou implantar uma nova configuração de par HA com os tipos de instância EC2 c5, m5 e r5 e migrar os dados.

Alterar o tipo de instância

Os tipos de instância EC2 c4, m4 e r4 permitem mais discos por nó do que os tipos de instância EC2 c5, m5 e r5. Se a contagem de discos por nó para a instância EC2 c4, m4 ou r4 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 de camadas por instância EC2"](#) ["Alterar o tipo de instância EC2 para Cloud](#)

Se você não conseguir alterar o tipo de instância, siga as etapas em [Habilitar rede aprimorada](#).

Habilitar rede aprimorada

Para atualizar para o Cloud Volumes ONTAP versões 9.8 e posteriores, você deve habilitar a *rede aprimorada* no cluster que executa o tipo de instância c4, m4 ou r4. Para habilitar o ENA, consulte o artigo da Base de Conhecimento "[Como habilitar redes aprimoradas como SR-IOV ou ENA em instâncias do AWS Cloud Volumes ONTAP](#)".

Prepare-se para atualizar

Antes de executar uma atualização, você deve verificar se seus sistemas estão prontos e fazer as alterações de configuração necessárias.

- [Planeje o tempo de inatividade](#)
- [Verifique se a devolução automática ainda está habilitada](#)
- [Suspender transferências do SnapMirror](#)
- [Verifique se os agregados estão online](#)
- [Verifique se todos os LIFs estão nas portas de origem](#)

Planeje o tempo de inatividade

Ao atualizar um sistema de nó único, o processo de atualização deixa o sistema offline 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 a E/S não é interrompida. Durante esse processo de atualização ininterrupta, cada nó é atualizado em conjunto para continuar fornecendo E/S aos clientes.

Protocolos orientados a sessão podem causar efeitos adversos em clientes e aplicativos em determinadas áreas durante atualizações. Para mais detalhes, consulte o "[Documentação do ONTAP](#)".

Verifique se a devolução automática ainda está habilitada

O retorno automático deve ser habilitado em um par de Cloud Volumes ONTAP HA (esta é a configuração padrão). Caso contrário, a operação falhará.

["Documentação do ONTAP : Comandos para configurar o retorno automático"](#)

Suspender transferências do SnapMirror

Se um sistema Cloud Volumes ONTAP tiver relacionamentos SnapMirror ativos, é melhor suspender as transferências antes de atualizar o software Cloud Volumes ONTAP. Suspender as transferências evita falhas do SnapMirror. Você deve suspender as transferências do sistema de destino.



Embora o NetApp Backup and Recovery use uma implementação do SnapMirror para criar arquivos de backup (chamado SnapMirror Cloud), os backups não precisam ser suspensos quando um sistema é atualizado.

Sobre esta tarefa

Estas etapas descrevem como usar o ONTAP System Manager para a versão 9.3 e posteriores.

Passos

1. Efetue login no Gerenciador do Sistema a partir do sistema de destino.

Você pode efetuar login no System Manager apontando seu navegador da web para o endereço IP do LIF de gerenciamento do cluster. Você pode encontrar o endereço IP no sistema Cloud Volumes ONTAP .



O computador do qual você está acessando o Console deve ter uma conexão de rede com o Cloud Volumes ONTAP. Por exemplo, talvez você precise fazer login no Console a partir de um host de salto que esteja na rede do seu provedor de nuvem.

2. Clique em **Proteção > Relacionamentos**.
3. Selecione o relacionamento e clique em **Operações > Desativar**.

Verifique se os agregados estão online

Os agregados para o Cloud Volumes ONTAP devem estar online antes de você atualizar o software. Os agregados devem estar on-line na maioria das configurações, mas se não estiverem, você deve colocá-los on-line.

Sobre esta tarefa

Estas etapas descrevem como usar o ONTAP System Manager para a versão 9.3 e posteriores.

Passos

1. No sistema Cloud Volumes ONTAP , clique na guia **Agregados**.
2. No bloco agregado necessário, clique em  ícone e, em seguida, selecione **Exibir detalhes agregados**.

Aggregate Details

aggr1

Overview	Capacity Allocation	Provider Properties
State	online	
Home Node	aggr1-01	
Encryption Type	cloudEncrypted	
Volumes	2	

3. Se o agregado estiver offline, use o ONTAP System Manager para colocá-lo online:
 - 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 nas portas de origem

Antes de atualizar, todos os LIFs devem estar em portas domésticas. Consulte a documentação do ONTAP para ["verificar se todos os LIFs estão nas portas de origem"](#) .

Se ocorrer um erro de falha de atualização, consulte o artigo da Base de Conhecimento (KB) ["Falha na atualização do Cloud Volumes ONTAP"](#) .

Atualizar Cloud Volumes ONTAP

O Console 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, consulte [Atualização das notificações do console](#) .

Outra maneira de realizar atualizações de software é usar uma imagem em uma URL externa. Esta opção é útil se o Console não puder acessar o bucket S3 para atualizar o software ou se você recebeu um patch. Para obter mais informações, consulte [Atualização de uma imagem disponível em um URL](#) .

Atualização das notificações do console

O Console exibe uma notificação nos 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 por meio das notificações, você precisa 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 do software de um bucket S3, instalando a imagem e reiniciando o sistema.

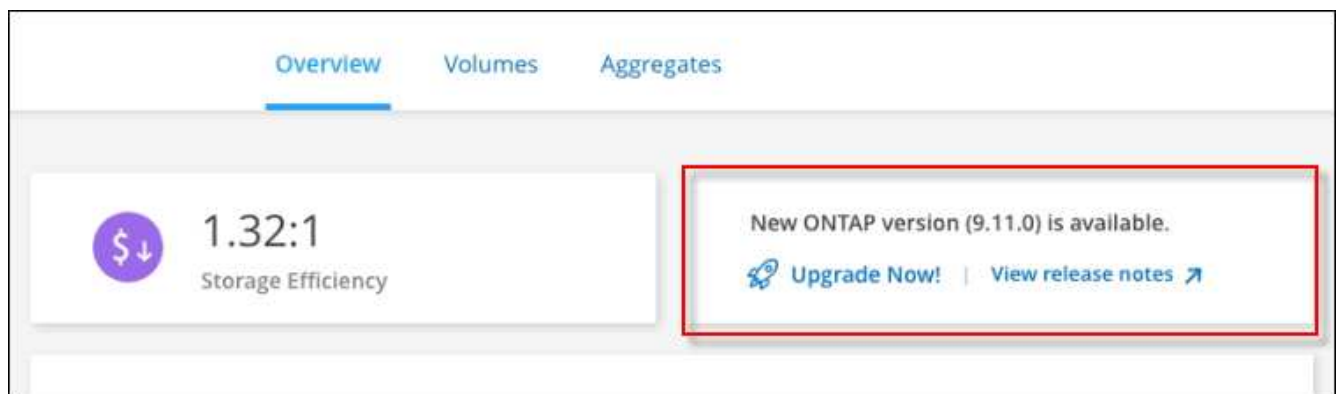
Antes de começar

Operações 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 **Armazenamento > Gerenciamento**.
2. Selecione um sistema Cloud Volumes ONTAP .

Uma notificação aparece 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.

Upgrade Cloud Volumes ONTAP Version



You are about to upgrade Cloud Volumes ONTAP ⓘ

9.12.1 → 9.13.1P10 (Jul 7, 2024)

[Select other versions](#)

End User License Agreement (EULA)

1. DEFINITIONS

1.1. "Documentation" means technical documentation describing the features and functions of the Software.

1.2. "NetApp Cloud Provider" means a third party authorized by NetApp to offer or enable the use of the Software as part of such provider's cloud-based service.

1.3. "NetApp Partner" means an authorized NetApp distributor, reseller or other channel partner. 1.4. "Open Source Software" means third party software that is openly and freely licensed under the terms of a public

☐ I read and approve the End User License Agreement (EULA)

Upgrade

Cancel

Se você 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 no 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 (por exemplo, o próximo patch da versão instalada). Para um caminho de atualização compatível com sua versão atual do Cloud Volumes ONTAP , consulte "[Caminhos de atualização suportados](#)".
5. Clique em **Salvar** e depois em **Aplicar**

Select the ONTAP version you want to upgrade to:

Version	Date
☐ 9.12.1P14	Aug 22, 2024
☐ 9.12.1P13	Jul 7, 2024
☐ 9.13.1P10	Jul 7, 2024
☐ 9.13.1P9	May 9, 2024

☒ All versions

Write the version you want to upgrade to:

Write the version here

Save Cancel

Apply Cancel

6. Na página Atualizar Cloud Volumes ONTAP , leia o EULA e selecione **Li e aprovo o EULA**.

7. Selecione **Atualizar**.

8. Para visualizar o progresso, no sistema Cloud Volumes ONTAP , selecione **Auditoria**.

Resultado

O Console inicia a atualização do software. Você pode executar ações no sistema quando a atualização do software estiver concluída.

Depois que você terminar

Se você suspendeu as transferências do SnapMirror , use o Gerenciador do Sistema para retomá-las.

Atualização de uma imagem disponível em um URL

Você pode colocar a imagem do software Cloud Volumes ONTAP no agente do Console ou em um servidor HTTP e, em seguida, iniciar a atualização do software no Console. Você pode usar esta opção se o Console não puder acessar o bucket S3 para atualizar o software.

Antes de começar

- Operações como criação de volume ou agregado não devem estar em andamento no sistema Cloud Volumes ONTAP .

- Se você usar HTTPS para hospedar imagens ONTAP , a atualização poderá falhar devido a problemas de autenticação SSL, que são 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 Console.

Acesse a Base de conhecimento da NetApp para ver instruções passo a passo:

["NetApp KB: Como configurar o Console 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 na 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, certifique-se de que as regras de saída permitam conexões HTTP para que o Cloud Volumes ONTAP possa acessar a imagem do software.



O grupo de segurança predefinido do Cloud Volumes ONTAP permite conexões HTTP de saída por padrão.

3. Obtenha a imagem do software em ["o site de suporte da NetApp"](#) .
4. Copie a imagem do software para um diretório no agente do Console ou em um servidor HTTP do qual o arquivo será servido.

Há dois caminhos disponíveis. O caminho correto depende da versão do seu agente do Console.

- /opt/application/netapp/cloudmanager/docker_occm/data/ontap/images/
- /opt/application/netapp/cloudmanager/ontap/images/

5. No sistema, clique em ícone e, em seguida, clique em **Atualizar Cloud Volumes ONTAP**.
6. Na página Atualizar versão do Cloud Volumes ONTAP , insira o URL e clique em **Alterar imagem**.

Se você copiou a imagem do software para o agente do Console no caminho mostrado acima, insira o seguinte URL:

`http://<endereço-IP-privado_do_agente_do_console>/ontap/images/<nome-do-arquivo-de-imagem>`



Na URL, **nome-do-arquivo-de-imagem** deve seguir o formato "cot.image.9.13.1P2.tgz".

7. Clique em **Continuar** para confirmar.

Resultado

O Console inicia a atualização do software. Você pode executar ações no sistema depois que a atualização do software estiver concluída.

Depois que você terminar

Se você suspendeu as transferências do SnapMirror , use o Gerenciador do Sistema para retomá-las.

Corrigir falhas de download ao usar um gateway NAT do Google Cloud

O agente do Console baixa automaticamente as atualizações de software para o Cloud Volumes ONTAP. O download pode falhar se sua configuração usar um gateway NAT do Google Cloud. Você pode corrigir esse problema limitando o número de partes em que a imagem do software é dividida. Você deve usar as APIs para concluir esta etapa.

Etapa

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 baixada não será dividida.

Observe que 32 é um valor de exemplo. O valor que você deve usar depende da sua configuração de NAT e do número de sessões que você pode ter simultaneamente.

["Saiba mais sobre a chamada de API /occm/config"](#).

Registre os sistemas de pagamento conforme o uso do Cloud Volumes ONTAP

O suporte da NetApp está incluído nos sistemas pré-pagos (PAYGO) do Cloud Volumes ONTAP, mas você deve primeiro ativar o suporte registrando os sistemas na NetApp.

O registro de um sistema PAYGO com a 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 notificações de atualização de software que aparecem no NetApp Console quando uma nova versão estiver disponível. Mas você precisará registrar o sistema antes de poder atualizar o software.

Passos

1. Se você ainda não adicionou sua conta do Site de Suporte NetApp ao Console, vá para **Configurações da conta** e adicione-a agora.

["Aprenda como adicionar contas do site de suporte da NetApp"](#).

2. Na página **Sistemas**, clique duas vezes no nome do sistema que você deseja registrar.
3. Na guia Visão geral, clique no painel Recursos e depois clique no ícone de lápis ao lado de **Registro de suporte**.

Information	Features
System Tags	3 Tags 
Scheduled Downtime	Off 
Blob Access Tiering	Hot 
Instance Type	Standard_E8ds_v4 
Charging Method	Capacity-based 
Write Speed	<i>Not Supported</i> 
Ransomware Protection	Off 
Support Registration	Not Registered 
WORM	Disabled 
CIFS Setup	

4. Selecione uma conta do site de suporte da NetApp e clique em **Registrar**.

Resultado

O sistema está registrado na NetApp.

Converter uma licença baseada em nó do Cloud Volumes ONTAP em uma licença baseada em capacidade

Após o fim da disponibilidade (EOA) das suas licenças baseadas em nó, você deve fazer

a transição para o licenciamento baseado em capacidade usando a ferramenta de conversão de licenças no NetApp Console.

Para compromissos anuais ou de longo prazo, a NetApp recomenda que você entre em contato com seu representante da NetApp antes da data de 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 em uma assinatura sob demanda de pagamento conforme o uso (PAYGO), é importante planejar sua conversão antes do fim 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 licença no NetApp Console para uma transição tranquila.

Para obter informações sobre o EOA e o EOS, consulte ["Fim da disponibilidade de licenças baseadas em nós"](#).

Sobre esta tarefa

- Ao usar a ferramenta de conversão de licença, a transição do modelo de licenciamento baseado em nó para o modelo de licenciamento baseado em capacidade é realizada no local e on-line, o que elimina a necessidade de qualquer migração de dados ou provisionamento de recursos de nuvem adicionais.
- É uma operação sem interrupções e não ocorre interrupção de serviço nem tempo de inatividade do aplicativo.
- Os dados da conta e do aplicativo no seu sistema Cloud Volumes ONTAP permanecem intactos.
- Os recursos de nuvem subjacentes permanecem inalterados 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 AZs, traga sua própria licença (BYOL) e PAYGO.
- A ferramenta oferece suporte a todas as licenças baseadas em nó 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 qualquer licença baseada em capacidade adquirida no marketplace. A NetApp restringiu a compra, extensão e renovação de licenças BYOL. Para obter mais informações, consulte ["Disponibilidade restrita de licenciamento BYOL para Cloud Volumes ONTAP"](#).
- A conversão é suportada por todos os provedores 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 na sua conta do NetApp Support Site (NSS).
- Ao fazer a transição para o modelo baseado em capacidade, seus dados continuam sendo retidos no mesmo local do licenciamento baseado em nós. Essa abordagem garante que não haja interrupção no posicionamento dos dados e mantém os princípios de soberania dos dados durante toda a transição.

Antes de começar

- Você deve ter uma conta NSS com acesso de cliente ou acesso de administrador.
- Sua conta NSS deve ser registrada com as credenciais de usuário que você usou para acessar o Console.
- O sistema Cloud Volumes ONTAP deve ser vinculado à conta NSS com acesso de cliente ou acesso de administrador.
- Você deve ter uma licença válida baseada em capacidade, seja uma licença BYOL ou uma assinatura de mercado.
- Uma licença baseada em capacidade deve estar disponível em sua conta. Esta licença pode ser uma assinatura de mercado ou um pacote BYOL/oferta privada disponível em **Licenças e assinaturas** no Console.

- Entenda 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 BYOL baseadas em capacidade da conta:
 - Quando **Professional** for selecionado como o pacote de destino, a conta deve ter uma licença BYOL com um pacote Profissional:
 - Quando **Essentials** for selecionado como o pacote de destino, a conta deverá ter uma licença BYOL com o pacote Essentials.
 - Se o pacote de destino não estiver alinhado com a disponibilidade da 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 da sua assinatura do marketplace.
 - Se não houver uma licença BYOL baseada em capacidade, mas apenas uma assinatura de mercado, você deve garantir que o pacote selecionado esteja incluído na sua assinatura de mercado baseada em capacidade.
 - Se não houver capacidade suficiente na sua licença baseada em capacidade existente e se você tiver uma assinatura de mercado para cobrar pelo uso de capacidade adicional, você será cobrado pela capacidade adicional por meio da sua assinatura de mercado.
 - Se não houver capacidade suficiente na sua licença baseada em capacidade existente e você não tiver uma assinatura de 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 para sua licença atual.
 - Se o pacote de destino não estiver alinhado com a disponibilidade da licença BYOL da conta e também se não houver capacidade suficiente na sua licença baseada em capacidade existente, você será cobrado pela sua assinatura do marketplace.



Se algum desses requisitos não for atendido, a conversão da licença não ocorrerá. Em casos específicos, a licença pode ser convertida, mas não pode ser utilizada. Clique no ícone de informações para identificar os problemas e tomar ações corretivas.

Passos

1. Na página **Sistemas**, clique duas vezes no nome do sistema para o qual você deseja modificar o tipo de licença.
2. Na guia Visão geral, clique no painel Recursos.
3. Marque o ícone de lápis ao lado de **Método de carregamento**. Se o método de cobrança do seu sistema for **Node Based**, você pode convertê-lo para carregamento por capacidade.



O ícone será desabilitado se o seu sistema Cloud Volumes ONTAP já estiver carregado pela capacidade ou se algum dos requisitos não for atendido.

4. Na tela **Converter licenças baseadas em nó para baseadas em capacidade**, verifique o nome do sistema e os detalhes da licença de origem.
5. Selecione o pacote de destino para converter a licença existente:
 - Essenciais. O valor padrão é **Essentials**.
 - Profissional
6. Se você tiver uma licença BYOL, poderá marcar a caixa de seleção para excluir a licença baseada em nó do Console após a conclusão da conversão. Se a conversão ainda estiver em andamento, selecionar esta caixa de seleção não removerá a licença do Console. Esta opção não está disponível para assinaturas do

marketplace.

7. Marque a caixa de seleção para confirmar que você entende as implicações da alteração e clique em **Continuar**.

Depois que você terminar

Veja o novo número de série da licença e verifique as alterações no menu **Licenças e assinaturas** do Console.

Preços em diferentes hiperescalares

Para obter detalhes sobre preços, acesse o "[Site do console NetApp](#)".

Para obter informações sobre ofertas privadas em hiperescalares específicos, escreva para:

- AWS - awsapo@netapp.com
- Azure - azurepo@netapp.com
- Google Cloud - gcppo@netapp.com

Iniciar e parar um sistema Cloud Volumes ONTAP

Você pode parar e iniciar o Cloud Volumes ONTAP no NetApp Console para gerenciar seus custos de computação em nuvem.

Agendamento de desligamentos automáticos do Cloud Volumes ONTAP

Talvez você queira 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 Console para desligar e reiniciar automaticamente os sistemas em horários específicos.

Sobre esta tarefa

- Quando você agenda um desligamento automático do seu sistema Cloud Volumes ONTAP, o Console adia o desligamento se uma transferência de dados ativa estiver em andamento.

Ele desliga o sistema após a conclusão da transferência.

- Esta tarefa agenda desligamentos automáticos de ambos os nós em um par HA.
- Snapshots de discos de inicialização e raiz não são criados ao desativar o Cloud Volumes ONTAP por meio de desligamentos agendados.

Os instantâneos são criados automaticamente somente ao executar um desligamento manual, conforme descrito na próxima seção.

Passos

1. Na página **Sistemas**, clique duas vezes no sistema Cloud Volumes ONTAP.
2. Na guia Visão geral, clique no painel Recursos e depois clique no ícone de lápis ao lado de **Tempo de inatividade programado**.

Information	Features
System Tags	3 Tags 
Scheduled Downtime	On 
S3 Storage Classes	Standard 
Instance Type	m5.xlarge 
Charging Method	Capacity-based 
Write Speed	Normal 
Ransomware Protection	Off 
Support Registration	Not Registered 
WORM	Disabled 
CIFS Setup	

3. Especifique o cronograma de desligamento:

- 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.
- Especifique quando você deseja desligar o sistema e por quanto tempo ele deve ficar desligado.

Exemplo

A imagem a seguir mostra uma programação que instrui o Console a desligar o sistema todos os sábados às 20:00 (20:00) por 12 horas. O Console reinicia o sistema todas as segundas-feiras às

Schedule Downtime

Console Time Zone: 13:48 UTC

Select when to turn off your system:

Turn off every day

Sun, Mon, Tue, Wed, Thu, Fri, Sat

at 20 : 00 for 12 hours (1-24)

Turn off every weekdays

Mon, Tue, Wed, Thu, Fri

at 20 : 00 for 12 hours (1-24)

Turn off every weekend

Sat

at 08 : 00 for 48 hours (1-48)

4. Clique em **Salvar**.

Resultado

A programação foi salva. O item de linha Tempo de inatividade agendado correspondente no painel Recursos exibe "Ativado".

Parando Cloud Volumes ONTAP

Interromper o Cloud Volumes ONTAP evita que você acumule custos de computação e cria instantâneos dos discos raiz e de inicialização, o que pode ser útil para solução de problemas.



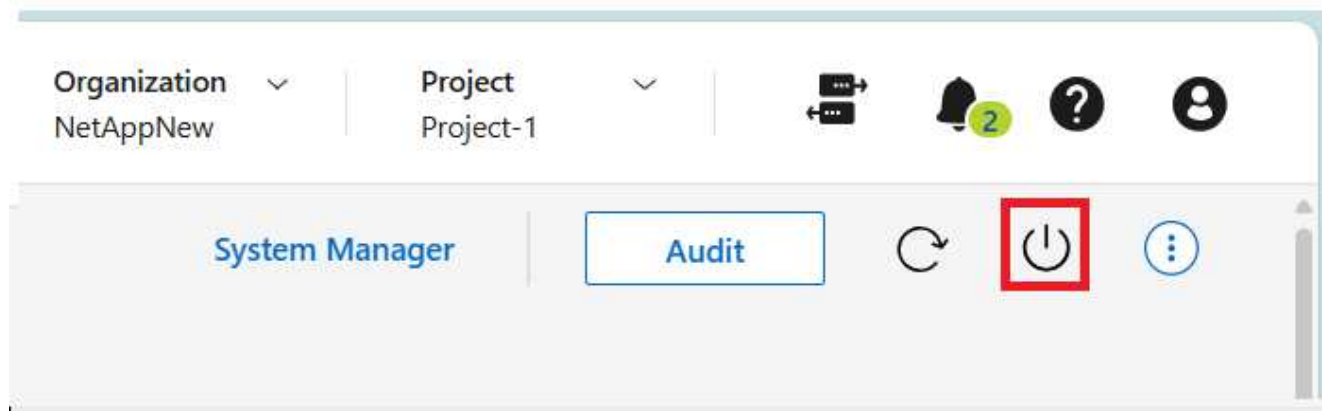
Para reduzir custos, o Console exclui periodicamente snapshots mais antigos de discos raiz e de inicialização. Somente os dois instantâneos mais recentes são retidos para os discos raiz e de inicialização.

Sobre esta tarefa

Quando você interrompe um par HA, o Console desliga ambos os nós.

Passos

1. No sistema, clique no ícone **Desligar**.



2. Mantenha a opção de criar snapshots ativada porque os snapshots podem habilitar a recuperação do sistema.
3. Clique em **Desligar**.

Pode levar alguns minutos para parar o sistema. Você pode reiniciar os sistemas mais tarde na página **Sistemas**.



Os instantâneos são criados automaticamente na reinicialização.

Sincronizar a hora do sistema Cloud Volumes ONTAP usando o servidor NTP

Especificar um servidor NTP sincroniza o horário entre os sistemas na sua rede, o que pode ajudar a evitar problemas devido a diferenças de horário.

Especifique um servidor NTP usando o ["API do console NetApp"](#) ou da interface do usuário quando você ["criar um servidor CIFS"](#).

Modificar a velocidade de gravação do sistema

Você pode escolher uma velocidade de gravação normal ou alta para o Cloud Volumes ONTAP no NetApp Console. A velocidade de gravação padrão é normal. Você pode mudar para alta velocidade de gravação se um desempenho de gravação rápido for necessário para sua carga de trabalho.

Alta velocidade de gravação é suportada com todos os tipos de sistemas de nó único e algumas configurações de pares HA. Veja as configurações suportadas no ["Notas de versão do Cloud Volumes ONTAP"](#)

Antes de alterar a velocidade de gravação, você deve ["entender as diferenças entre as configurações normais e altas"](#).

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 de todo o sistema.

Passos

1. Na página **Sistemas**, clique duas vezes no nome do sistema que você configurou para a velocidade de gravação.
2. Na guia Visão geral, clique no painel Recursos e depois clique no ícone de lápis ao lado de **Velocidade de gravação**.
3. Selecione **Normal** ou **Alto**.

Se você escolher Alto, precisará ler a declaração "Eu entendo..." e confirmar marcando a caixa.



A opção de velocidade de gravação **Alta** é compatível com pares de alta disponibilidade 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**.

Alterar a senha do administrador do cluster Cloud Volumes ONTAP

O Cloud Volumes ONTAP inclui uma conta de administrador de cluster. Você pode alterar a senha desta conta no NetApp Console, se necessário.



Você não deve alterar a senha da conta de administrador por meio do ONTAP System Manager ou do ONTAP CLI. A senha não será refletida no Console. Como resultado, o Console não consegue monitorar a instância corretamente.

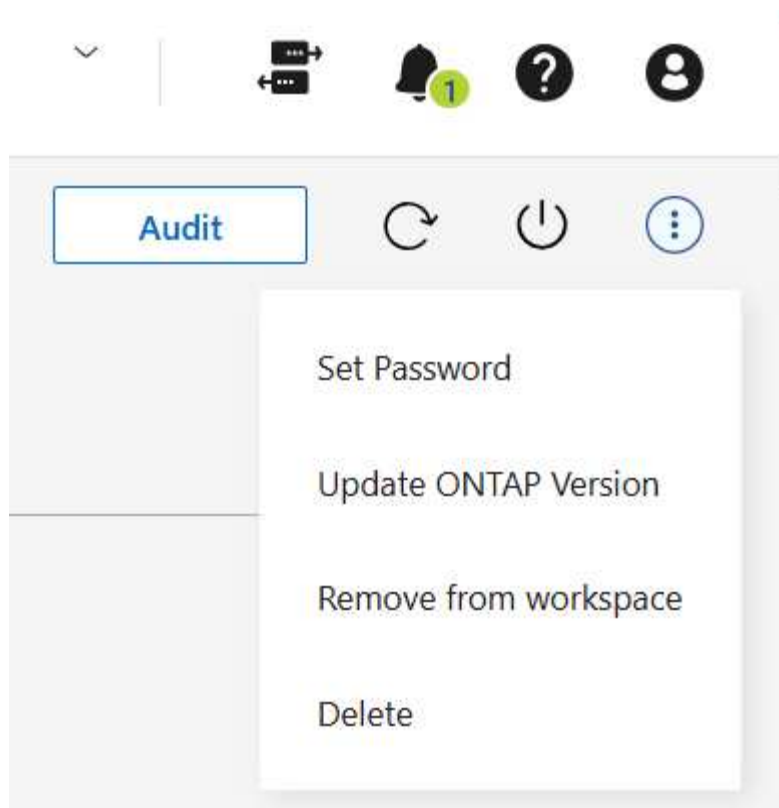
Sobre esta tarefa

A senha deve observar algumas regras. A nova senha:

- Não deve conter a palavra `admin`
- Deve ter entre oito e 50 caracteres de comprimento
- Deve conter pelo menos uma letra e um dígito em inglês
- Não deve conter estes caracteres especiais: `/ ( ) { } [ ] # : % " ? \`

Passos

1. Na página **Sistemas**, clique duas vezes no nome do sistema Cloud Volumes ONTAP .
2. No canto superior direito do Console, clique em  ícone e selecione **Definir senha**.



Adicionar, remover ou excluir sistemas

Adicionar um sistema Cloud Volumes ONTAP existente ao NetApp Console

Você pode descobrir e adicionar sistemas Cloud Volumes ONTAP existentes ao NetApp Console. Você pode fazer isso se tiver implantado um novo sistema.

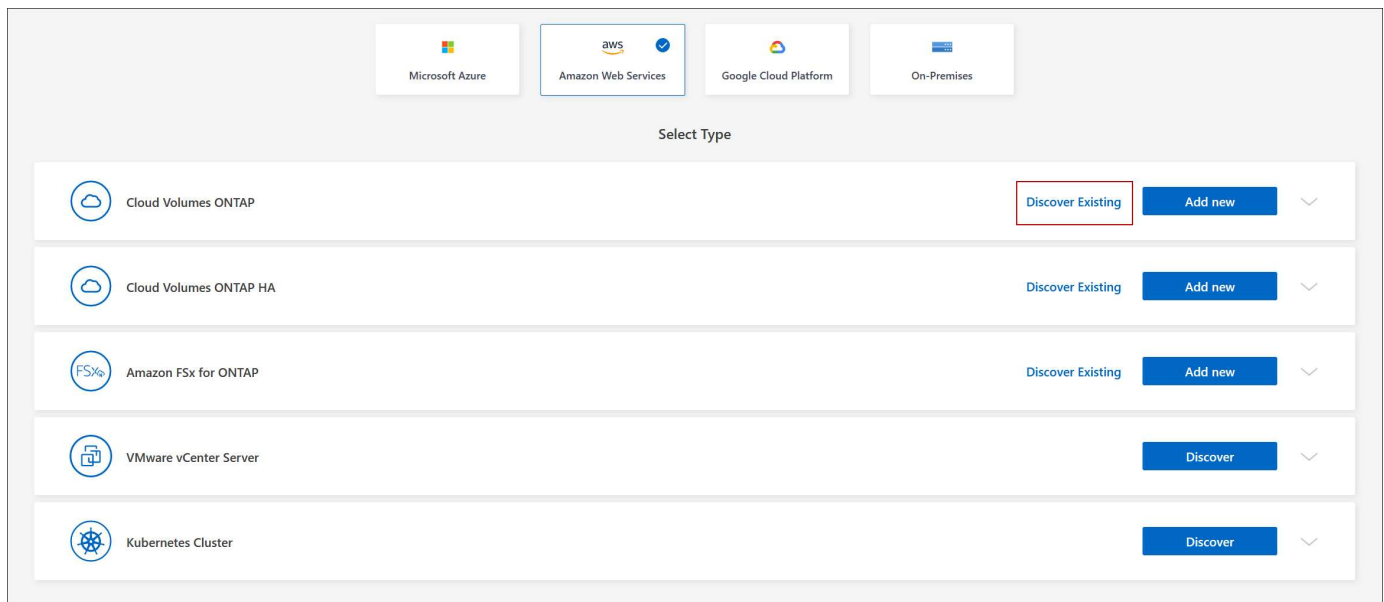
Antes de começar

Você precisa saber a senha da conta de usuário administrador do Cloud Volumes ONTAP .

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistema**, clique em **Adicionar Sistema**.
3. Selecione o provedor de nuvem no qual o sistema reside.
4. Escolha o tipo de sistema Cloud Volumes ONTAP a ser adicionado.
5. Clique no link para descobrir um sistema existente.

+



1. Na página Região, selecione uma região. Você pode ver os sistemas que estão em execução na região selecionada.



Os sistemas Cloud Volumes ONTAP são representados como instâncias nesta página. Na lista, você pode selecionar apenas as instâncias registradas na conta atual.

2. Na página Credenciais, insira a senha do usuário administrador do Cloud Volumes ONTAP e selecione **Ir**.

Resultado

O Console adiciona os sistemas Cloud Volumes ONTAP à página **Sistemas**.

Remover um sistema Cloud Volumes ONTAP do NetApp Console

Você pode remover um sistema Cloud Volumes ONTAP para movê-lo para outro sistema ou para solucionar problemas de descoberta.

Sobre esta tarefa

A remoção de um sistema Cloud Volumes ONTAP o remove do NetApp Console. Ele não exclui o sistema Cloud Volumes ONTAP . Você pode redescobrir o sistema mais tarde, se necessário.

Passos

1. Na página **Sistemas**, clique duas vezes no sistema que você deseja remover.
2. No canto superior direito do Console, clique em **...** ícone e selecione **Remover do espaço de trabalho**.
3. Na janela **Remover do espaço de trabalho**, clique em **Remover**.

Resultado

O Console remove o sistema. Os usuários podem redescobrir o sistema excluído na página **Sistemas** a qualquer momento.

Excluir um sistema Cloud Volumes ONTAP do NetApp Console

Você deve sempre excluir os sistemas Cloud Volumes ONTAP do NetApp Console, em vez do aplicativo do seu provedor de nuvem. Por exemplo, se você encerrar uma

instância licenciada do Cloud Volumes ONTAP do seu provedor de nuvem, não poderá usar a chave de licença para outra instância. Você deve excluir o sistema Cloud Volumes ONTAP do Console para liberar a licença.

Quando você exclui um sistema, o Console encerra as instâncias do Cloud Volumes ONTAP e exclui discos e snapshots.



Outros recursos, como backups gerenciados pelo NetApp Backup and Recovery e instâncias do NetApp Data Classification, não são excluídos quando você exclui um sistema. Você precisará excluí-los manualmente. Caso contrário, você continuará a incorrer em cobranças por esses recursos.

Quando o Console implanta o Cloud Volumes ONTAP no seu provedor de nuvem, ele habilita a proteção de encerramento nas instâncias. Esta opção ajuda a evitar encerramento acidental.

Passos

1. Se você habilitou o Backup e a Recuperação no sistema, determine se os dados de backup ainda são necessários e então ["exclua os backups, se necessário"](#).

O Backup and Recovery é independente do Cloud Volumes ONTAP por design. O Backup e Recuperação não exclui backups automaticamente quando você exclui um sistema Cloud Volumes ONTAP e não há suporte atual na interface do usuário para excluir os backups após o sistema ter sido excluído.

2. Se você habilitou a Classificação de Dados neste sistema e nenhum outro sistema usa este serviço, você precisa excluir a instância do serviço.

["Saiba mais sobre a instância de Classificação de Dados"](#).

3. Exclua o sistema Cloud Volumes ONTAP.
 - a. Na página **Sistemas**, clique duas vezes no nome do sistema Cloud Volumes ONTAP que você deseja excluir.
 - b. No canto superior direito do Console, clique em  ícone e selecione **Excluir**.
 - c. Digite o nome do sistema que você deseja excluir e clique em **Excluir**. Pode levar até cinco minutos para excluir um sistema.



O Backup e a Recuperação são gratuitos apenas para licenças do Cloud Volumes ONTAP Professional. Este benefício gratuito não se aplica a ambientes excluídos. Se cópias de backup do ambiente Cloud Volumes ONTAP forem mantidas em uma instância de Backup e Recuperação, você será cobrado pelas cópias de backup até que elas sejam excluídas.

Administração AWS

Modificar o tipo de instância EC2 para um sistema Cloud Volumes ONTAP na AWS

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 determinar que ela é subdimensionada ou superdimensionada para suas necessidades.

Sobre esta tarefa

- O retorno automático deve ser habilitado em um par de Cloud Volumes ONTAP HA (esta é a configuração

padrão). Caso contrário, a operação falhará.

"Documentação do ONTAP 9: Comandos para configurar o retorno 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 HA, a mudança não é disruptiva. Os pares HA continuam a fornecer dados.



O NetApp Console altera um nó por vez, iniciando a aquisição e aguardando o retorno. A equipe de Garantia de Qualidade da NetApp testou a gravação e a leitura de arquivos durante esse processo e não observou nenhum problema no lado do cliente. Conforme as conexões mudavam, algumas tentativas eram observadas no nível de E/S, mas a camada de aplicação superou a reconfiguração das conexões NFS/CIFS.

Referência

Para obter uma lista de tipos de instância suportados na AWS, consulte "[Instâncias EC2 suportadas](#)".

Se você não conseguir alterar o tipo de instância de c4, m4 ou r4, consulte o artigo da KB "[Convertendo uma instância AWS Xen CVO para Nitro \(KVM\)](#)".

Passos

1. Na página **Sistemas**, selecione o sistema.
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
System 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 pré-paga (PAYGO) baseada em nó, você pode escolher uma licença e um tipo de instância diferentes clicando no ícone de lápis ao lado de **Tipo de licença**.

- 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 é reinicializado com a nova configuração.

Modificar tabelas de rotas para pares de Cloud Volumes ONTAP HA em várias AZs da AWS

Você pode modificar as tabelas de rotas da AWS que incluem rotas para os endereços IP flutuantes para um par de HA implantado em várias Zonas de Disponibilidade (AZs) da AWS. Você pode fazer isso se novos clientes NFS ou CIFS precisarem acessar um par HA na AWS.

Passos

1. Na página **Sistemas**, selecione o sistema.
2. Na guia Visão geral, clique no painel Recursos e, em seguida, clique no ícone de lápis ao lado de **Tabelas de rotas**.
3. Modifique a lista de tabelas de rotas selecionadas e clique em **Salvar**.

Resultado

O NetApp Console envia uma solicitação da AWS para modificar as tabelas de rotas.

Administração do Azure

Alterar o tipo de VM do Azure para 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 ela é subdimensionada ou superdimensionada para suas necessidades.

Sobre esta tarefa

- O retorno automático deve ser habilitado em um par de Cloud Volumes ONTAP HA (esta é a configuração padrão). Caso contrário, a operação falhará.

["Documentação do ONTAP 9: Comandos para configurar o retorno 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 HA, a mudança não é disruptiva. Os pares HA continuam a fornecer dados.



O NetApp Console altera um nó por vez, iniciando a aquisição e aguardando o retorno. A equipe de Garantia de Qualidade da NetApp testou a gravação e a leitura de arquivos durante esse processo e não observou nenhum problema no lado do cliente. Conforme as conexões mudavam, algumas tentativas eram observadas no nível de E/S, mas a camada de aplicação superou a reconfiguração das conexões NFS/CIFS.

Passos

1. Na página **Sistemas**, selecione o sistema.

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 (PAYGO) baseada em nó, poderá escolher uma licença e um tipo de VM diferentes clicando no ícone de lápis ao lado de **Tipo de licença**.

3. 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 é reinicializado com a nova configuração.

Substituir bloqueios CIFS para pares de alta disponibilidade do Cloud Volumes ONTAP no Azure

O administrador da organização ou da conta pode habilitar uma configuração no NetApp Console que evita problemas com o retorno do armazenamento Cloud Volumes ONTAP durante eventos de manutenção do Azure. Quando você habilita essa configuração, o Cloud Volumes ONTAP veta bloqueios CIFS e redefine sessões CIFS ativas.

Sobre esta tarefa

O Microsoft Azure agenda eventos de manutenção periódicos em suas máquinas virtuais. Quando ocorre um evento de manutenção em um par de HA do Cloud Volumes ONTAP, o par de HA inicia a aquisição do armazenamento. Se houver sessões CIFS ativas durante este evento de manutenção, os bloqueios nos arquivos CIFS podem impedir o retorno do armazenamento.

Se você habilitar essa configuração, o Cloud Volumes ONTAP vetará os bloqueios e redefinirá as sessões CIFS ativas. Como resultado, o par HA pode concluir a devolução do armazenamento durante esses eventos de manutenção.



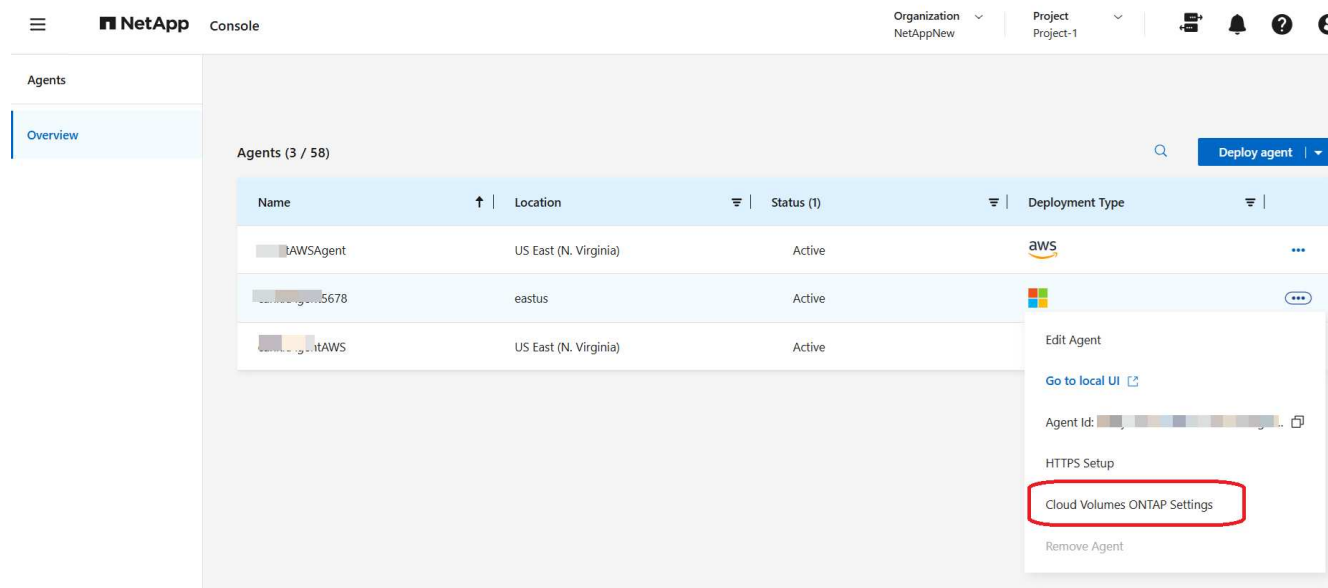
Esse processo pode ser prejudicial aos clientes do CIFS. Dados não confirmados de clientes CIFS podem ser perdidos.

Antes de começar

Você precisa criar um agente do Console antes de poder alterar as configurações do Console. ["Aprenda como"](#).

Passos

1. No painel de navegação esquerdo, acesse **Administração > Agentes**.
2. Clique no  ícone para o agente do Console que gerencia seu sistema Cloud Volumes ONTAP.
3. Selecione *** Configurações do Cloud Volumes ONTAP ***.



4. Em **Azure**, clique em **Bloqueios CIFS do Azure para sistemas HA do Azure**.
5. Clique na caixa de seleção para habilitar o recurso e depois clique em **Salvar**.

Use um Azure Private Link ou pontos de extremidade de serviço para sistemas Cloud Volumes ONTAP

O Cloud Volumes ONTAP usa um Azure Private Link para conexões com suas contas de armazenamento associadas. Se necessário, você pode desabilitar os Links Privados do Azure e usar pontos de extremidade de serviço.

Visão geral

Por padrão, o NetApp Console habilita um Azure Private Link para conexões entre o Cloud Volumes ONTAP e suas contas de armazenamento associadas. Um Link Privado do Azure protege conexões entre pontos de extremidade no Azure e oferece benefícios de desempenho.

Se necessário, você pode configurar o Cloud Volumes ONTAP para usar pontos de extremidade de serviço em vez de um Link Privado do Azure.

Com qualquer configuração, o Console sempre limita o acesso à rede para conexões entre o Cloud Volumes ONTAP e contas de armazenamento. O acesso à rede é limitado à VNet onde o Cloud Volumes ONTAP está implantado e à VNet onde o agente do Console está implantado.

Desabilite os Links Privados do Azure e use pontos de extremidade de serviço em vez deles

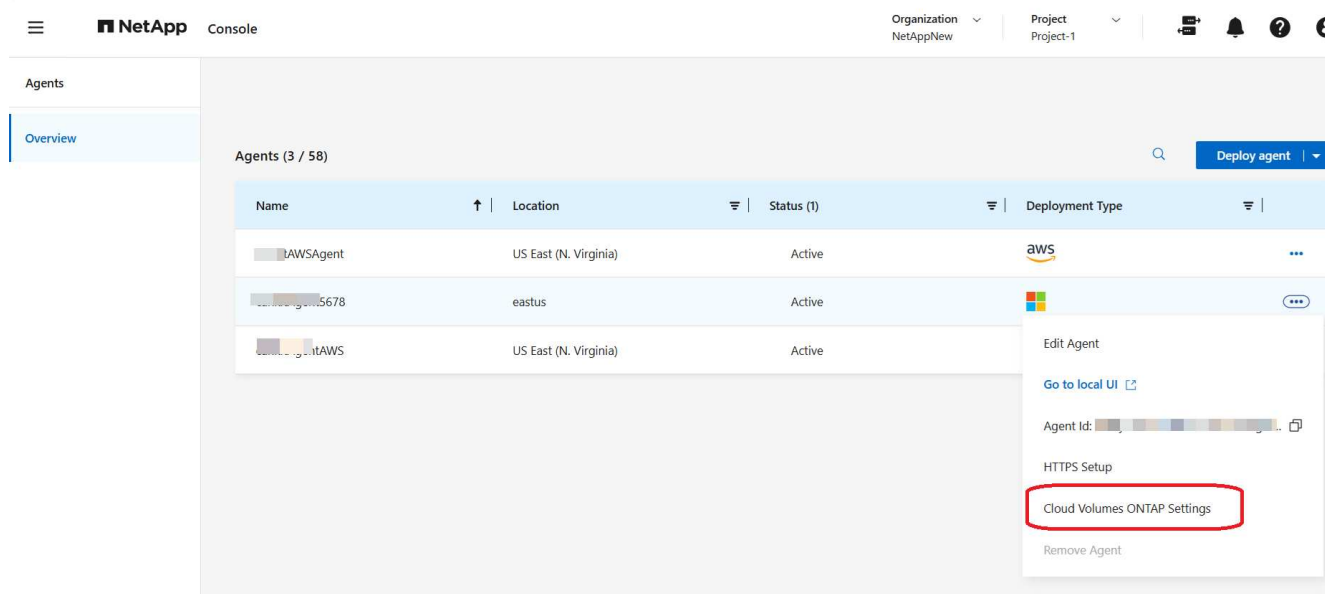
Se necessário para sua empresa, você pode alterar uma configuração no Console para que ele configure o Cloud Volumes ONTAP para usar pontos de extremidade de serviço em vez de um Link Privado do Azure. A alteração desta configuração se aplica aos novos sistemas Cloud Volumes ONTAP que você criar. Os pontos de extremidade de serviço são suportados apenas em "Pares de regiões do Azure" entre o agente do Console e as VNets Cloud Volumes ONTAP.

O agente do Console deve ser implantado na mesma região do Azure que os sistemas Cloud Volumes ONTAP que ele gerencia ou no "Par de regiões do Azure" para os sistemas Cloud Volumes ONTAP.

Passos

1. No painel de navegação esquerdo, acesse **Administração > Agentes**.

2. Clique no **...** ícone para o agente do Console que gerencia seu sistema Cloud Volumes ONTAP .
3. Selecione *** Configurações do Cloud Volumes ONTAP ***.



4. Em **Azure**, clique em **Usar link privado do Azure**.
5. Desmarque **Conexão de link privado entre o Cloud Volumes ONTAP e contas de armazenamento**.
6. Clique em **Salvar**.

Depois que você terminar

Se você desabilitou os Links Privados do Azure e o agente do Console usa um servidor proxy, você deve habilitar o tráfego direto da API.

["Aprenda como habilitar o tráfego direto da API no agente do Console"](#)

Trabalhar com Links Privados do Azure

Na maioria dos casos, não há nada que você precise fazer para configurar links privados do Azure com o Cloud Volumes ONTAP. O Console gerencia os 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

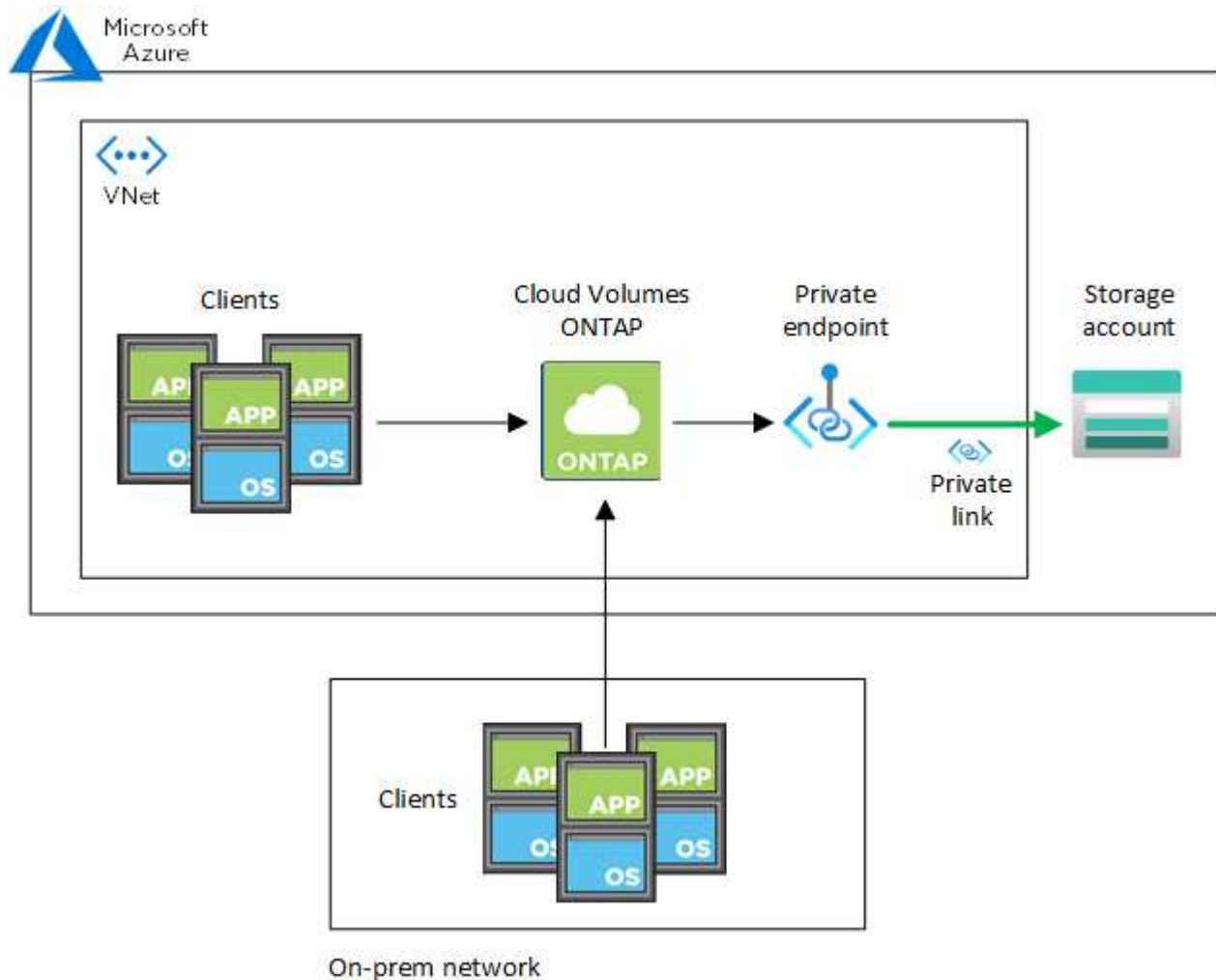
Opcionalmente, se você trabalhar com DNS personalizado, precisará criar um encaminhador condicional para a zona DNS privada do Azure a partir dos seus servidores DNS personalizados. Para saber mais, consulte ["Documentação do Azure sobre o uso de um encaminhador DNS"](#).

Como funcionam as conexões do Private Link

Quando o Console implanta o Cloud Volumes ONTAP no Azure, ele cria um ponto de extremidade privado no grupo de recursos. O ponto de extremidade privado está associado às contas de armazenamento do Cloud Volumes ONTAP. Como resultado, o acesso ao armazenamento do Cloud Volumes ONTAP passa pela rede de backbone da Microsoft.

O acesso do cliente ocorre por meio do link privado quando os clientes estão na mesma VNet que o Cloud Volumes ONTAP, em VNets pareadas ou na sua rede local ao usar uma VPN privada ou conexão ExpressRoute com a VNet.

Aqui está um exemplo que mostra o acesso do cliente por meio de um link privado de dentro da mesma VNet e de uma rede local que tem uma VPN privada ou uma conexão ExpressRoute.



Se o agente do Console e os sistemas Cloud Volumes ONTAP forem implantados em VNets diferentes, você deverá configurar o peering de VNet entre a VNet onde o agente do Console está implantado e a VNet onde os sistemas Cloud Volumes ONTAP estão implantados.

Forneça detalhes sobre seu DNS privado do Azure

Se você usar ["DNS privado do Azure"](#), então você precisa modificar um arquivo de configuração em cada agente do Console. Caso contrário, o Console não poderá definir 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 DNS do Azure ["conforme mostrado na documentação do Azure"](#).

Passos

1. Conecte-se via SSH ao host do agente do Console e efetue login.
2. Navegue até o `/opt/application/netapp/cloudmanager/docker_occm/data` diretório.
3. Editar `app.conf` adicionando o `user-private-dns-zone-settings` parâmetro com os seguintes pares de palavra-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 `subscription` A palavra-chave é necessária somente se a zona DNS privada estiver em uma assinatura diferente daquela do agente do Console.

4. Salve o arquivo e faça logoff do agente do Console.

Não é necessário reinicializar.

Habilitar reversão em caso de falhas

Se o Console não conseguir criar um Link Privado do Azure como parte de ações específicas, ele concluirá a ação sem a conexão do Link Privado do Azure. Isso pode acontecer ao criar um novo sistema (nó único ou par HA) ou quando as seguintes ações ocorrem em um par HA: criar um novo agregado, adicionar discos a um agregado existente ou criar uma nova conta de armazenamento ao ultrapassar 32 TiB.

Você pode alterar esse comportamento padrão habilitando a reversão caso o Console não consiga criar o Link Privado do Azure. Isso pode ajudar a garantir que você esteja em total conformidade com os regulamentos de segurança da sua empresa.

Se você habilitar a reversão, o Console interromperá a ação e reverterá todos os recursos que foram criados como parte da ação.

Você pode habilitar a reversão por meio da API ou atualizando o arquivo `app.conf`.

Habilitar rollback através da API

Etapa

1. Use o PUT `/occm/config` Chamada de API com o seguinte corpo de solicitação:

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

Habilite a reversão atualizando app.conf

Passos

1. Conecte-se via SSH ao host do agente do Console e efetue login.
2. Navegue até o seguinte diretório: `/opt/application/netapp/cloudmanager/docker_occm/data`
3. Edite `app.conf` adicionando o seguinte parâmetro e valor:

```
"rollback-on-private-link-failure": true
. Salve o arquivo e faça logoff do agente do Console.
```

Não é necessário reinicializar.

Mover um grupo de recursos do Azure para o Cloud Volumes ONTAP no console do Azure

O Cloud Volumes ONTAP oferece suporte a movimentações de grupos de recursos do Azure, mas o fluxo de trabalho ocorre somente no console do Azure.

Você pode mover um sistema Cloud Volumes ONTAP de um grupo de recursos para um grupo de recursos diferente no Azure dentro da mesma assinatura do Azure. Não há suporte para mover grupos de recursos entre diferentes assinaturas do Azure.

Passos

1. Remova o sistema Cloud Volumes ONTAP . Consulte ["Removendo sistemas Cloud Volumes ONTAP"](#) .
2. Execute a movimentação do grupo de recursos no console do Azure.

Para concluir a mudança, consulte ["Mover recursos para um novo grupo de recursos ou assinatura na documentação do Microsoft Azure"](#) .

3. Na página **Sistemas**, descubra o sistema.
4. Procure o novo grupo de recursos nas informações do sistema.

Resultado

O sistema e seus recursos (VMs, discos, contas de armazenamento, interfaces de rede, snapshots) estão no novo grupo de recursos.

Segregar o tráfego do SnapMirror no Azure

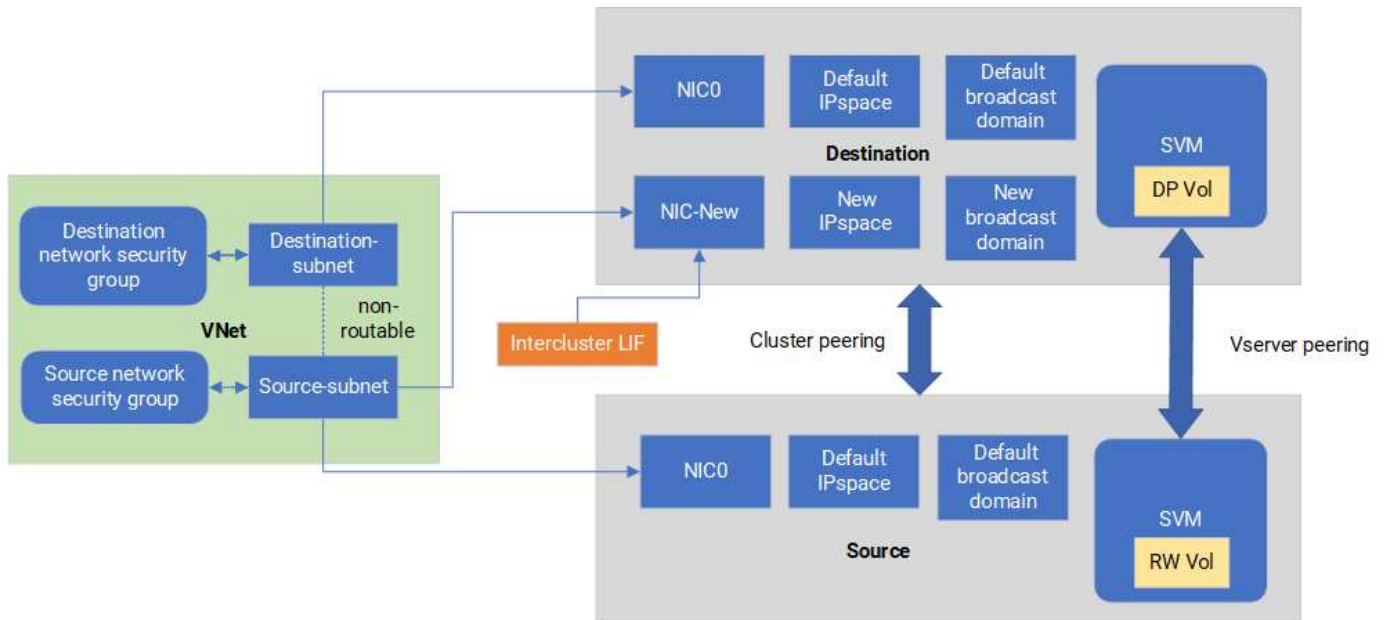
Com o Cloud Volumes ONTAP no Azure, você pode segregar o tráfego de replicação do SnapMirror do tráfego de dados e gerenciamento. Para segregar o tráfego de replicação do SnapMirror do seu tráfego de dados, você adicionará uma nova placa de interface de rede (NIC), um LIF intercluster associado e uma sub-rede não roteável.

Sobre a segregação de tráfego do SnapMirror no Azure

Por padrão, o NetApp Console configura todas as NICs e LIFs em uma implantação do Cloud Volumes ONTAP na mesma sub-rede. Nessas configurações, o tráfego de replicação do SnapMirror e o tráfego de dados e gerenciamento usam a mesma sub-rede. A segregação do tráfego do SnapMirror aproveita uma sub-rede adicional que não é roteável para a sub-rede existente usada para tráfego de dados e gerenciamento.

Figura 1

Os diagramas a seguir mostram a segregação do tráfego de replicação do SnapMirror com uma NIC adicional, um LIF intercluster associado e uma sub-rede não roteável em uma única implantação de nó. Uma implantação de par HA é um pouco diferente.



Antes de começar

Revise as seguintes considerações:

- Você só pode adicionar uma única NIC a uma implantação de nó único ou par HA do Cloud Volumes ONTAP (instância de VM) para segregação de tráfego do SnapMirror .
- Para adicionar uma nova NIC, o tipo de instância de VM que você implanta 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-a 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 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. Desaloque o nó.

```
az vm deallocate --resource-group <dest_node-rg> --name <dest_node-vm>
```

4. Configure regras de 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 o ID da 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 de sub-rede da 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 endereço IP privado. Este endereço IP, <new_added_nic_primary_addr>, é usado para criar um LIF intercluster em [domínio de transmissão](#), [LIF intercluster para o novo NIC](#) .

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, acesse **Rede** e confirme se a nova NIC, por exemplo, nic-new, existe e se a rede acelerada está habilitada.

```
az network nic list --resource-group azure-59806175-60147103-azure-rg --query "[].{NIC: name, VM: virtualMachine.id}"
```

Para implantações de par HA, repita as etapas para o nó parceiro.

Etapa 2: criar um novo IPspace, domínio de transmissão e LIF intercluster para a nova NIC

Um IPspace separado para LIFs interclusters fornece separação lógica entre a funcionalidade de rede para replicação entre clusters.

Use o ONTAP CLI 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 transmissão no novo IPspace (`new_ipspace`) e adicione a porta `nic-new`.

```
dest::> network port show
```

3. Para sistemas de nó único, a porta recém-adicionada é `e0b`. Para implantações de par HA com discos gerenciados, a porta recém-adicionada é `e0d`. Para implantações de pares HA com blobs de página, a porta recém-adicionada é `e0e`. Use o nome do nó, não o nome da VM. Encontre 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 intercluster no novo domínio de transmissão (`new_bd`) e no novo NIC (`nic-new`).

```
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. Verifique a criação do novo LIF intercluster.

```
dest::> net int show
```

Para implantações de par HA, repita as etapas para o nó parceiro.

Etapa 3: verificar o peering do cluster entre os sistemas de origem e destino

Esta seção fornece instruções sobre como verificar o peering entre os sistemas de origem e destino.

Use o ONTAP CLI para as etapas a seguir.

Passos

1. Verifique se o LIF intercluster do cluster de destino pode executar ping no LIF intercluster do cluster de origem. Como o cluster de destino executa esse comando, o endereço IP de destino é o endereço IP do LIF intercluster na origem.

```
dest::> ping -lif <new_dest_node-ic-lif> -vserver <new_ipspace>
-destination <10.161.189.6>
```

2. Verifique se o LIF intercluster do cluster de origem pode executar ping no LIF intercluster 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 HA, repita as etapas para o nó parceiro.

Etapa 4: criar peering SVM entre os sistemas de origem e destino

Esta seção fornece instruções sobre como criar o peering SVM entre os sistemas de origem e de destino.

Use o ONTAP CLI para as etapas a seguir.

Passos

1. Crie o peering de cluster no destino usando o endereço IP do LIF intercluster de origem como `-peer-addr`s . Para pares HA, liste o endereço IP do LIF intercluster de origem para ambos os nós como `-peer-addr`s .

```
dest::> cluster peer create -peer-addr <10.161.189.6> -ipspace
<new_ipspace>
```

2. Digite e confirme a senha.
3. Crie um peering de cluster na origem usando o endereço IP do LIF do cluster de destino como `peer-addr`s . Para pares HA, liste o endereço IP LIF do intercluster de destino para ambos os nós como `-peer-addr`s .

```
src::> cluster peer create -peer-addr <10.161.189.18>
```

4. Digite e confirme a senha.
5. Verifique se o cluster está pareado.

```
src::> cluster peer show
```

O peering bem-sucedido mostra **Disponível** no campo de disponibilidade.

6. Crie um peering SVM no destino. Tanto os SVMs de origem quanto os 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 está pareado.

```
dest::> vserver peer show
```

Mostra de estado de pares*peered* e aplicações de peering mostram*snapmirror*.

Etapas 5: Crie um relacionamento de replicação SnapMirror entre o sistema de origem e o de destino

Esta seção fornece instruções sobre como criar um relacionamento de replicação do SnapMirror entre o sistema de origem e o de destino.

Para mover um relacionamento de replicação SnapMirror existente, você deve primeiro quebrar o relacionamento de replicação SnapMirror existente antes de criar um novo relacionamento de replicação SnapMirror .

Use o ONTAP CLI para as etapas a seguir.

Passos

1. Crie um volume de dados protegido no SVM de destino.

```
dest::> vol create -volume <new_dest_vol> -vserver <dest_svm> -type DP
-size <10GB> -aggregate <aggr1>
```

2. Crie o relacionamento de replicação do SnapMirror no destino, que inclui a política do SnapMirror e o agendamento 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 o relacionamento 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 do relacionamento é `Snapmirrored` e a saúde do relacionamento é `true` .

5. Opcional: Na CLI do ONTAP , execute o seguinte comando para visualizar o histórico de ações do relacionamento 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 sendo replicado para o destino.

Administração do Google Cloud

Alterar o tipo de máquina do Google Cloud para o 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 determinar que ela é subdimensionada ou superdimensionada para suas necessidades.

Sobre esta tarefa

- O retorno automático deve ser habilitado em um par de Cloud Volumes ONTAP HA (esta é a configuração padrão). Caso contrário, a operação falhará.

["Documentação do ONTAP 9: Comandos para configurar o retorno automático"](#)

- Alterar o tipo de máquina pode afetar as cobranças do serviço do Google Cloud.
- A operação reinicia o Cloud Volumes ONTAP.

Para sistemas de nó único, a E/S é interrompida.

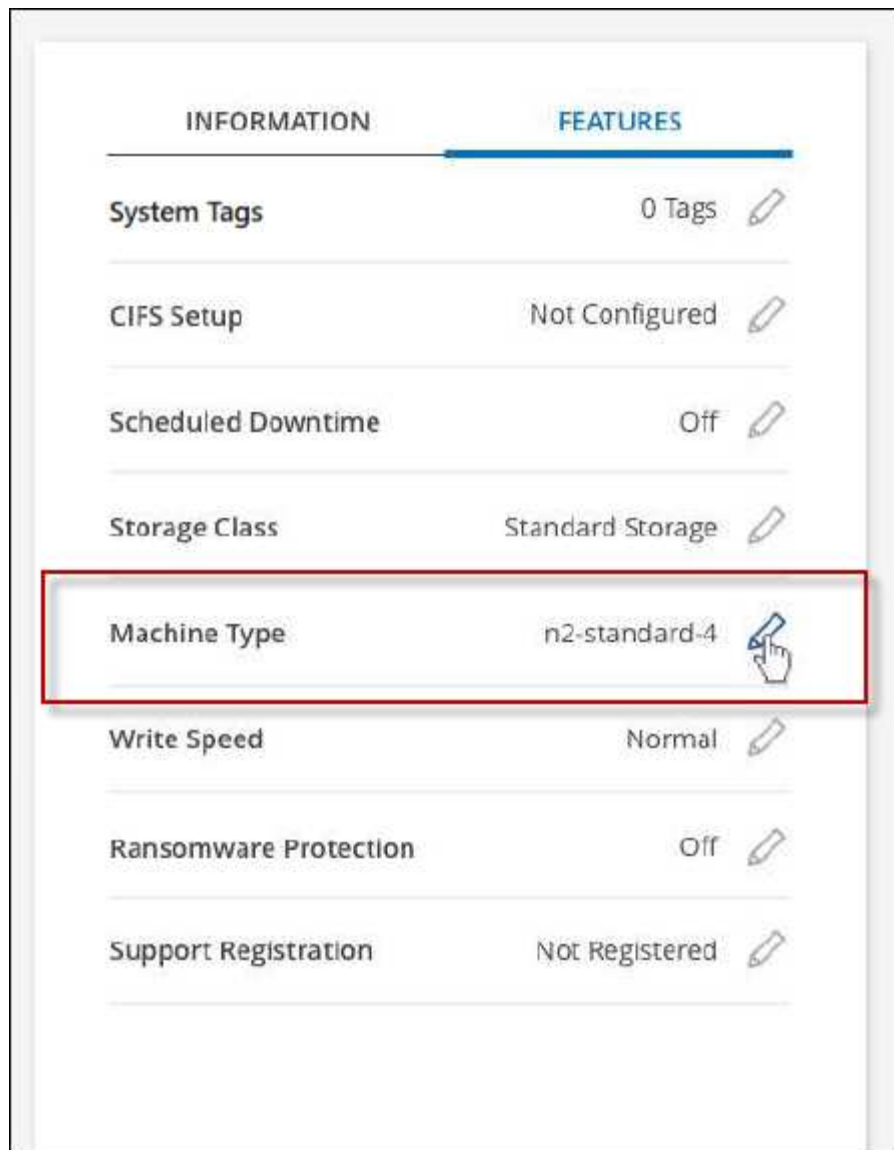
Para pares HA, a mudança não é disruptiva. Os pares HA continuam a fornecer dados.



O NetApp Console altera um nó por vez, iniciando a aquisição e aguardando o retorno. A equipe de Garantia de Qualidade da NetApp testou a gravação e a leitura de arquivos durante esse processo e não observou nenhum problema no lado do cliente. Conforme as conexões mudavam, algumas tentativas eram observadas no nível de E/S, mas a camada de aplicação superou a reconfiguração das conexões NFS/CIFS.

Passos

1. Na página **Sistemas**, selecione o sistema.
2. Na guia Visão geral, clique no painel Recursos e depois clique no ícone de lápis ao lado de **Tipo de máquina**.



Se você estiver usando uma licença de pagamento conforme o uso (PAYGO) baseada em nó, você pode escolher uma licença e um tipo de máquina diferentes 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 é reinicializado com a nova configuração.

Administrar o Cloud Volumes ONTAP usando o System Manager

Os recursos avançados de gerenciamento de armazenamento do Cloud Volumes ONTAP estão disponíveis por meio do ONTAP System Manager, uma interface de gerenciamento fornecida com os sistemas ONTAP . Você pode acessar o System Manager diretamente do NetApp Console.

Características

Você pode executar várias funções de gerenciamento de armazenamento usando o ONTAP System Manager no Console. A lista a seguir inclui algumas dessas funcionalidades, embora não seja exaustiva:

- Gerenciamento avançado de armazenamento: gerencie grupos de consistência, compartilhamentos, qtrees, cotas e VMs de armazenamento.
- Movimento de volume: "[Mover um volume para um agregado diferente.](#)"
- Gerenciamento de rede: gerencie espaços IP, interfaces de rede, conjuntos de portas e portas Ethernet.
- Gerenciar volumes FlexGroup : Você pode criar e gerenciar volumes FlexGroup somente por meio do Gerenciador de Sistemas. O Console não suporta a criação de volumes FlexGroup .
- Eventos e trabalhos: visualize logs de eventos, alertas do sistema, trabalhos e logs de auditoria.
- Proteção avançada de dados: proteja VMs de armazenamento, LUNs e grupos de consistência.
- Gerenciamento de host: configure grupos de iniciadores SAN e clientes NFS.
- Gerenciamento de armazenamento de objetos S3: os recursos de gerenciamento de armazenamento S3 no Cloud Volumes ONTAP estão disponíveis somente no Gerenciador do Sistema e não no Console.

Configurações suportadas

- O gerenciamento avançado de armazenamento por meio do ONTAP System Manager está disponível no Cloud Volumes ONTAP 9.10.0 e posteriores em regiões de nuvem padrão.
- A integração do System Manager não é suportada em regiões GovCloud ou em regiões que não têm acesso de saída à Internet.

Limitações

Alguns recursos que aparecem na interface do System Manager não são suportados pelo Cloud Volumes ONTAP:

- NetApp Cloud Tiering: O Cloud Volumes ONTAP não oferece suporte ao Cloud Tiering. Você deve configurar o armazenamento de dados em camadas para objetos diretamente na Exibição Padrão ao criar volumes.
- Níveis: O gerenciamento de agregados (incluindo níveis locais e níveis de nuvem) não é compatível com o Gerenciador de Sistemas. Você deve gerenciar agregados diretamente da Exibição Padrão.
- Atualizações de firmware: O Cloud Volumes ONTAP não oferece suporte a atualizações automáticas de firmware na página **Cluster > Configurações** do Gerenciador do Sistema.
- Controle de acesso baseado em função: o controle de acesso baseado em função do Gerenciador do Sistema não é suportado.
- Disponibilidade Contínua (CA) para SMB: O Cloud Volumes ONTAP não oferece suporte "[ações SMB continuamente disponíveis](#)" para operações não disruptivas.

Configurar autenticação para acessar o System Manager

Como administrador, você pode ativar a autenticação para usuários que acessam o ONTAP System Manager pelo Console. Você pode determinar o nível correto de permissões de acesso com base nas funções do usuário do ONTAP e habilitar ou desabilitar a autenticação conforme necessário. Se você habilitar a autenticação, os usuários precisarão inserir suas credenciais de usuário do ONTAP sempre que acessarem o System Manager pelo Console ou quando a página for recarregada, porque o Console não armazena as credenciais internamente. Se você desabilitar a autenticação, os usuários poderão acessar o Gerenciador do

Sistema usando as credenciais de administrador.



Esta configuração é aplicável a cada agente do Console para os usuários do ONTAP na sua organização ou conta, independentemente do sistema Cloud Volumes ONTAP .

Permissões necessárias

Você precisa ter privilégios de administrador da organização ou da conta para modificar as configurações do agente do Console para autenticação de usuário do Cloud Volumes ONTAP .

Passos

1. No painel de navegação esquerdo, acesse **Administração > Agentes**.
2. Clique no ícone para o agente do Console necessário e selecione **Editar agente do Console**.
3. Em **Forçar credenciais de usuário**, marque a caixa de seleção **Ativar/Desativar**. Por padrão, a autenticação está desabilitada.



Se você definir esse valor como **Ativar**, a autenticação será redefinida e você terá que modificar todos os fluxos de trabalho existentes para acomodar essa alteração.

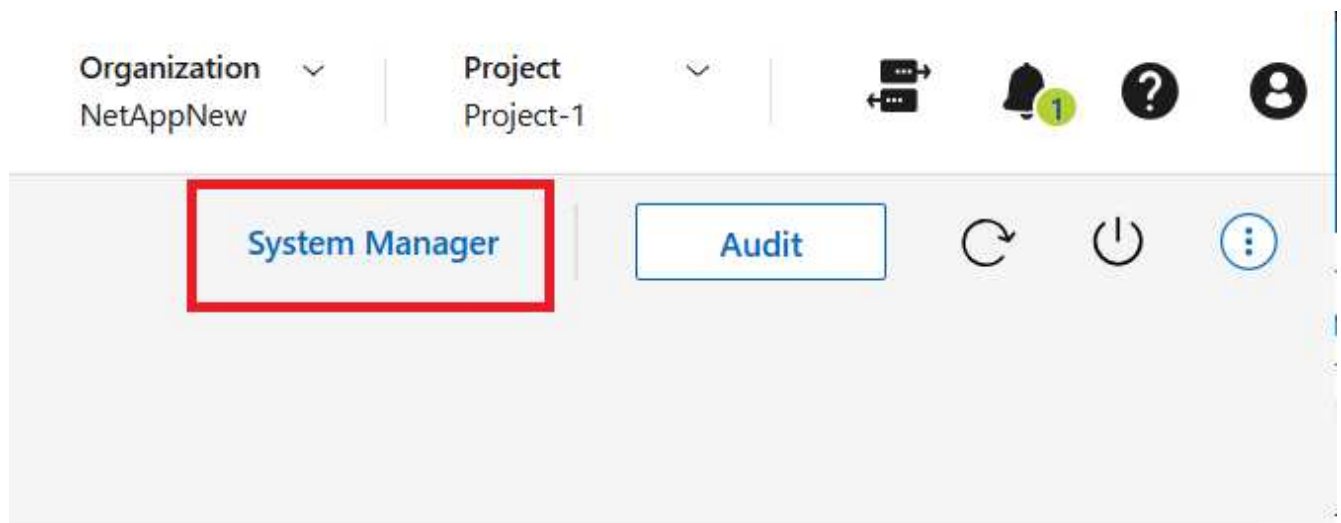
4. Clique em **Salvar**.

Comece a usar o System Manager

Você pode acessar o ONTAP System Manager a partir de um sistema Cloud Volumes ONTAP .

Passos

1. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
2. Na página **Sistemas**, clique duas vezes no sistema Cloud Volumes ONTAP necessário.
3. Clique em **Gerenciador do Sistema**.



4. Se solicitado, insira suas credenciais de usuário do ONTAP e clique em **Login**.
5. Se uma mensagem de confirmação aparecer, leia-a e clique em **Fechar**.

Use o System Manager para gerenciar seu sistema Cloud Volumes ONTAP . Você pode clicar em **Voltar** para retornar ao Console.

Ajuda com o uso do Gerenciador de Sistema

Se precisar de ajuda para usar o System Manager com o Cloud Volumes ONTAP, consulte o "[Documentação do ONTAP](#)" para obter instruções passo a passo. Aqui estão alguns links de documentação do ONTAP que podem ajudar:

- "[Funções, aplicativos e autenticação do ONTAP](#)"
- "[Use o Gerenciador de Sistema para acessar um cluster](#)" .
- "[Gerenciamento de volume e LUN](#)"
- "[Gerenciamento de rede](#)"
- "[Proteção de dados](#)"
- "[Crie compartilhamentos SMB continuamente disponíveis](#)"

Administrar o Cloud Volumes ONTAP a partir da CLI

O Cloud Volumes ONTAP CLI permite que você execute todos os comandos administrativos e é uma boa escolha para tarefas avançadas ou se você se sentir mais confortável usando o CLI. Você pode se conectar à CLI usando Secure Shell (SSH).

Antes de começar

O host 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 fazer SSH de um host de salto que esteja na rede do seu provedor de nuvem.



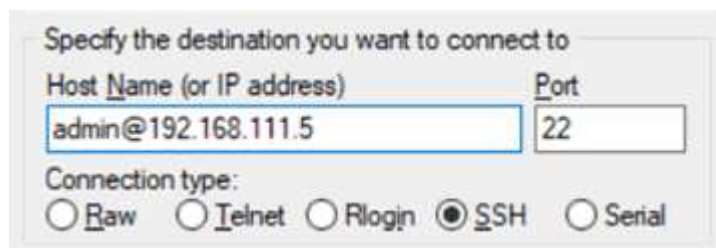
Quando implantadas em várias AZs, as configurações de HA do Cloud Volumes ONTAP usam um endereço IP flutuante para a interface de gerenciamento do cluster, o que significa que o roteamento externo não está disponível. Você deve se conectar de um host que faça parte do mesmo domínio de roteamento.

Passos

1. No NetApp Console, identifique o endereço IP da interface de gerenciamento do cluster:
 - a. No menu de navegação à esquerda, selecione **Armazenamento > Gerenciamento**.
 - b. Na página **Sistemas**, selecione o sistema Cloud Volumes ONTAP .
 - c. Copie o endereço IP de gerenciamento do cluster que aparece no painel direito.
2. Use SSH para se conectar ao endereço IP da interface de gerenciamento do cluster usando a conta de administrador.

Exemplo

A imagem a seguir mostra um exemplo usando PuTTY:



3. No prompt de login, digite a senha da conta de administrador.

Exemplo

```
Password: *****  
COT2::>
```

Saúde e eventos do sistema

Verifique a configuração do AutoSupport para o Cloud Volumes ONTAP

O AutoSupport monitora proativamente a integridade do seu sistema e envia mensagens ao suporte técnico da NetApp . Por padrão, o AutoSupport é habilitado em cada nó para enviar mensagens ao 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 com a Internet. Para obter detalhes, consulte os requisitos de rede do seu provedor de nuvem.

Requisitos do AutoSupport

Os nós do Cloud Volumes ONTAP exigem acesso de saída à Internet para o NetApp AutoSupport, que monitora proativamente a integridade do seu sistema e envia mensagens ao suporte técnico da NetApp .

As políticas de roteamento e firewall devem permitir tráfego HTTPS para os seguintes endpoints para que o Cloud Volumes ONTAP possa enviar mensagens de AutoSupport :

- \ <https://mysupport.netapp.com/aods/asupmessage>
- \ <https://mysupport.netapp.com/asupprod/post/1.0/postAsup>

Se uma conexão de saída com a Internet não estiver disponível para enviar mensagens do AutoSupport , o NetApp Console configurará automaticamente seus sistemas Cloud Volumes ONTAP para usar o agente do Console como um servidor proxy. O único requisito é garantir que o grupo de segurança do agente do Console permita conexões *de entrada* pela porta 3128. Você precisará abrir esta porta depois de implantar o agente do Console.

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.



Se você estiver usando um par HA, o mediador HA não exigirá acesso de saída à Internet.

Depois de verificar se o acesso de saída à Internet está disponível, você pode testar o AutoSupport para garantir que ele pode enviar mensagens. Para obter instruções, consulte o "[Documentação do ONTAP : Configurar o AutoSupport](#)" .

Solucionar problemas de configuração do AutoSupport

Se uma conexão de saída não estiver disponível e o Console não puder configurar seu sistema Cloud Volumes ONTAP para usar o agente do Console como um servidor proxy, você receberá uma notificação do

Console intitulada "<nome do sistema> não consegue enviar mensagens do AutoSupport ".

Provavelmente você está recebendo esta mensagem devido a problemas de rede.

Siga estas etapas para resolver esse problema.

Passos

1. Conecte-se por SSH ao sistema Cloud Volumes ONTAP para que você possa administrar o sistema a partir da CLI do ONTAP .

["Aprenda como usar SSH para Cloud Volumes ONTAP"](#) .

2. Exibir o status 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 a URL do proxy para cada nó do Cloud Volumes ONTAP :

```
autosupport show -fields proxy-url
```

4. Se o parâmetro de URL do proxy estiver vazio, configure o Cloud Volumes ONTAP para usar o agente do Console como um proxy:

```
autosupport modify -proxy-url http://<console agent private ip>:3128
```

5. Verifique novamente o status do AutoSupport :

```
autosupport check show-details
```

6. Se o status ainda for falha, valide se há conectividade entre o Cloud Volumes ONTAP e o agente do Console pela porta 3128.
7. Se o ID de status ainda falhar após verificar se há conectividade, faça SSH para o agente do Console.

["Saiba mais sobre como conectar-se à VM Linux para o agente do console"](#)

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 `localnet src` 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 maneira:

```
acl cvonet src <cidr>
```

Se você adicionar esta nova entrada, não se esqueça de adicionar também uma entrada de permissão:

```
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. Após editar o arquivo de configuração, reinicie o contêiner 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 de AutoSupport :

```
autosupport check show-details
```

Configurar o EMS para sistemas Cloud Volumes ONTAP

O Sistema de Gerenciamento de Eventos (EMS) coleta e exibe 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 interceptação SNMP ou servidores syslog) e rotas de eventos para uma gravidade de evento específica.

Você pode configurar o EMS usando a CLI. Para obter instruções, consulte o ["Documentação do ONTAP : Visão geral da configuração do EMS"](#) .

Conceitos

Licenciamento

Licenciamento para 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 seguintes opções de licenciamento estão disponíveis para novos clientes.

Licenciamento baseado em capacidade

Pague por vários sistemas Cloud Volumes ONTAP na sua conta NetApp por capacidade provisionada. Inclui a capacidade de adquirir serviços de dados em nuvem adicionais. Para obter mais informações sobre modelos de consumo em licenças baseadas em capacidade, consulte ["Saiba mais sobre licenças baseadas em capacidade"](#).

Assinatura Keystone

Um serviço baseado em assinatura com pagamento conforme o crescimento que oferece uma experiência de nuvem híbrida perfeita para pares de alta disponibilidade (HA).

As seções a seguir fornecem mais detalhes sobre cada uma dessas opções.



Não há suporte 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 pelo Cloud Volumes ONTAP por TiB de capacidade. A licença está associada à sua conta NetApp e permite que você cobre vários sistemas pela licença, desde que haja capacidade suficiente disponível por meio da licença.

Por exemplo, você pode comprar uma única licença de 20 TiB, implantar quatro sistemas Cloud Volumes ONTAP e, em seguida, alocar um volume de 5 TiB 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 do seu negócio.



Embora o uso real e a medição dos produtos e serviços gerenciados no NetApp Console sejam sempre calculados em GiB e TiB, os termos GB/GiB e TB/TiB são usados de forma intercambiável. Isso se reflete nas listagens do mercado de nuvem, cotações de preços, descrições de listagens e em outra documentação de suporte.

Pacotes

Os seguintes pacotes baseados em capacidade estão disponíveis para o Cloud Volumes ONTAP. Para obter mais informações sobre pacotes de licenças baseados em capacidade, consulte ["Saiba mais sobre licenças"](#)

[baseadas em capacidade](#)" .

Para obter uma lista de tipos de VM suportados com os seguintes pacotes baseados em capacidade, consulte:

- ["Configurações com suporte no Azure"](#)
- ["Configurações suportadas no Google Cloud"](#)

Freemium

Fornece todos os recursos do Cloud Volumes ONTAP gratuitamente da NetApp (as taxas do provedor de nuvem ainda se aplicam). Um pacote Freemium tem estas características:

- Não é necessária nenhuma licença ou contrato.
- O suporte da 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 , para qualquer provedor de nuvem.
- Se a capacidade provisionada para um sistema Cloud Volumes ONTAP exceder 500 GiB, o Console converterá o sistema em um pacote Essentials.

Assim que um sistema é convertido para o pacote Essentials, ["carga mínima"](#) aplica-se a ele.

Um sistema Cloud Volumes ONTAP que foi convertido em um pacote Essentials não pode ser alternado de volta para Freemium, mesmo que a capacidade provisionada seja reduzida para menos de 500 GiB. Outros sistemas com menos de 500 GiB de capacidade provisionada permanecem no Freemium (desde que tenham sido implantados usando a oferta Freemium).

Essenciais

Você pode pagar por capacidade em diversas configurações diferentes:

- Escolha sua configuração do Cloud Volumes ONTAP :
 - Um único nó ou sistema HA
 - Armazenamento de arquivos e blocos ou dados secundários para recuperação de desastres (DR)
- Adicione qualquer um dos serviços de dados em nuvem da NetApp por um custo extra

Profissional

Pague por capacidade para qualquer tipo de configuração do Cloud Volumes ONTAP com backups ilimitados.

- Fornece licenciamento para qualquer configuração do Cloud Volumes ONTAP

Nó único ou HA com capacidade de cobrança para volumes primários e secundários na mesma taxa

- Inclui backups de volume ilimitados usando o NetApp Backup and Recovery, mas apenas para sistemas Cloud Volumes ONTAP que usam o pacote Profissional.



É necessária uma assinatura pré-paga (PAYGO) para Backup e Recuperação, porém não haverá cobranças pelo uso deste serviço. Para obter mais informações sobre como configurar o licenciamento para Backup e Recuperação, consulte ["Configurar licenciamento para backup e recuperação"](#) .

- Adicione qualquer um dos serviços de dados em nuvem da NetApp por um custo extra

Disponibilidade de licenças baseadas em capacidade

A disponibilidade das licenças PAYGO e BYOL para sistemas Cloud Volumes ONTAP exige que o agente do Console esteja ativo e em execução.

["Saiba mais sobre os agentes do Console"](#) .



A NetApp restringiu a compra, extensão e renovação de licenças BYOL. Para obter mais informações, consulte ["Disponibilidade restrita de licenciamento BYOL para Cloud Volumes ONTAP"](#) .

Como começar

Saiba como começar a usar o licenciamento baseado em capacidade:

- ["Configurar licenciamento para Cloud Volumes ONTAP na AWS"](#)
- ["Configurar o licenciamento do Cloud Volumes ONTAP no Azure"](#)
- ["Configurar o licenciamento do Cloud Volumes ONTAP no Google Cloud"](#)

Assinatura Keystone

Um serviço baseado em assinatura com pagamento conforme o crescimento que oferece uma experiência de nuvem híbrida perfeita para aqueles que preferem modelos de consumo de OpEx ao CapEx inicial ou leasing.

A cobrança é baseada no tamanho da sua capacidade comprometida para um ou mais pares de Cloud Volumes ONTAP HA na sua assinatura Keystone .

A capacidade provisionada para cada volume é agregada e comparada periodicamente à capacidade comprometida em sua Assinatura Keystone , e quaisquer excedentes são cobrados como pico em sua Assinatura Keystone .

["Saiba mais sobre o NetApp Keystone"](#) .

Configurações suportadas

Assinaturas Keystone são suportadas com pares HA. Esta opção de licenciamento não é suportada com sistemas de nó único no momento.

Limite de capacidade

No modelo de licenciamento baseado em capacidade, cada sistema Cloud Volumes ONTAP oferece suporte à hierarquização para armazenamento de objetos, e a capacidade total em camadas pode ser ampliada até o limite de bucket do provedor de nuvem. Embora a licença não imponha restrições de capacidade, siga as ["Melhores práticas do FabricPool"](#) para garantir desempenho ideal, confiabilidade e eficiência de custos ao configurar e gerenciar camadas.

Para obter informações sobre os limites de capacidade de cada provedor de nuvem, consulte sua documentação:

- ["Documentação do AWS"](#)
- ["Documentação do Azure para discos gerenciados"](#) e ["Documentação do Azure para armazenamento de blobs"](#)
- ["Documentação do Google Cloud"](#)

Como começar

Saiba como começar com uma assinatura Keystone :

- ["Configurar licenciamento para Cloud Volumes ONTAP na AWS"](#)
- ["Configurar o licenciamento do Cloud Volumes ONTAP no Azure"](#)
- ["Configurar o licenciamento do Cloud Volumes ONTAP no Google Cloud"](#)

Licenciamento baseado em nó

O licenciamento baseado em nó é o modelo de licenciamento da geração anterior que permitia 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 descritos acima.

A NetApp planejou o fim da disponibilidade (EOA) e do suporte (EOS) do licenciamento baseado em nós. Após o EOA e o EOS, as licenças baseadas em nós precisarão ser convertidas em licenças baseadas em capacidade.

Para obter informações, consulte ["Comunicado ao cliente: CPC-00589"](#) .

Fim 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 nó que se estenda além da data do EOA, poderá continuar a usar a licença até que o contrato expire. Após o término do contrato, será necessário fazer a transição para o modelo de licenciamento baseado em capacidade. Se você não tiver um contrato de longo prazo para um nó Cloud Volumes ONTAP , é importante planejar sua conversão antes da data de EOS.

Saiba mais sobre cada tipo de licença e o impacto do EOA sobre ele nesta tabela:

Tipo de licença	Impacto após o EOA
Licença válida baseada em nó adquirida por meio de traga sua própria licença (BYOL)	A licença permanece válida até o vencimento. Licenças baseadas em nós não utilizadas existentes podem ser usadas para implantar novos sistemas Cloud Volumes ONTAP .

Tipo de licença	Impacto após o EOA
Licença baseada em nó expirada adquirida por meio de BYOL	Você não terá direito de implantar novos sistemas Cloud Volumes ONTAP usando esta licença. Os sistemas existentes podem continuar funcionando, mas você não receberá nenhum suporte ou atualizações para seus sistemas após a data do EOS.
Licença válida baseada em nó com assinatura PAYGO	Deixará de receber suporte da NetApp após a data de EOS, até que você faça a transição para uma licença baseada em capacidade.

Exclusões

A NetApp reconhece que certas situações exigem consideração especial, e o EOA e o EOS do licenciamento baseado em nó não se aplicarão aos seguintes casos:

- Clientes do setor público dos EUA
- Implantações em modo privado
- Implantações 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 necessidades operacionais.



Mesmo nesses cenários, novas licenças baseadas em nós e renovações de licenças são válidas por no máximo um ano a partir da data de aprovação.

Conversão de licença

O Console permite uma conversão perfeita de licenças baseadas em nós para licenças baseadas em capacidade por meio da ferramenta de conversão de licenças. Para obter informações sobre o EOA do licenciamento baseado em nós, consulte ["Fim da disponibilidade de licenças baseadas em nós"](#).

Antes de fazer a 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 ONTAP, o que pode restringir a flexibilidade. O licenciamento baseado em capacidade, por outro lado, permite um pool compartilhado de armazenamento entre 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 na capacidade se ajusta perfeitamente às mudanças nos requisitos de armazenamento.

Para saber como você pode realizar essa conversão, consulte ["Converter uma licença baseada em nó do Cloud Volumes ONTAP em uma licença baseada em capacidade"](#).



A conversão de um sistema de licenciamento baseado em capacidade para baseado em nó não é suportada.

Saiba mais sobre licenças baseadas em capacidade para o Cloud Volumes ONTAP

Você deve estar familiarizado com o uso de capacidade e cobrança 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 carteira de motorista (BYOL). Uma licença adquirida da NetApp que pode ser usada para implantar o Cloud Volumes ONTAP em qualquer provedor de nuvem.



A NetApp restringiu a compra, extensão e renovação de licenças BYOL. Para obter mais informações, consulte ["Disponibilidade restrita de licenciamento BYOL para Cloud Volumes ONTAP"](#).

- **PAYGO:** Uma assinatura de pagamento conforme o uso (PAYGO) é uma assinatura por hora do mercado do seu provedor de nuvem.
- **Anual:** Um contrato anual do marketplace do seu provedor de nuvem.

Observe o seguinte:

- Se você adquirir uma licença da NetApp (BYOL), também precisará assinar a oferta PAYGO no marketplace do seu provedor de nuvem. A NetApp possui licenciamento BYOL restrito. Quando suas licenças BYOL expirarem, você deverá substituí-las por assinaturas do marketplace de nuvem.

Sua licença é sempre cobrada primeiro, mas você será cobrado pela taxa horária do mercado nestes casos:

- Se você exceder sua capacidade licenciada
- Se o prazo da sua licença expirar
- Se você tiver um contrato anual de um marketplace, *todos* os sistemas Cloud Volumes ONTAP que você implantar serão cobrados desse contrato. Você não pode misturar e combinar um contrato de mercado anual com BYOL.
- Somente sistemas de nó único com BYOL são suportados nas regiões da China. As implantações na região da China estão isentas das restrições de licenciamento BYOL.

Alterando pacotes

Após a implantação, você pode alterar o pacote para 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 caso suas necessidades comerciais mudem.

["Aprenda como alterar os métodos de cobrança"](#).

Para obter informações sobre a conversão de licenças baseadas em nó em licenças baseadas em capacidade, consulte

Preços e configurações suportadas

Para obter detalhes sobre preços, acesse o ["Site do console NetApp"](#).

Pacotes de licenciamento baseados em capacidade estão disponíveis com o Cloud Volumes ONTAP 9.7 e posteriores.

VMs de armazenamento

- Não há custos extras de licenciamento para VMs de armazenamento de dados adicionais (SVMs), mas há uma cobrança de capacidade mínima de 4 TiB por SVM de serviço de dados.
- Os SVMs de recuperação de desastres são cobrados de acordo com a capacidade provisionada.

Pares HA

Para pares de HA, você só é cobrado pela capacidade provisionada em um nó. Você não é cobrado pelos dados espelhados de forma síncrona no nó parceiro.

Volumes FlexClone e FlexCache

- Você não será cobrado pela capacidade usada pelos volumes FlexClone .
- Os volumes FlexCache de origem e destino são considerados dados primários e cobrados de acordo com o espaço provisionado.

Limite de capacidade

No modelo de licenciamento baseado em capacidade, cada sistema Cloud Volumes ONTAP oferece suporte à hierarquização para armazenamento de objetos, e a capacidade total em camadas pode ser ampliada até o limite de bucket do provedor de nuvem. Embora a licença não imponha restrições de capacidade, siga as ["Melhores práticas do FabricPool"](#) para garantir desempenho ideal, confiabilidade e eficiência de custos ao configurar e gerenciar camadas.

Para obter informações sobre os limites de capacidade de cada provedor de nuvem, consulte sua documentação:

- ["Documentação do AWS"](#)
- ["Documentação do Azure para discos gerenciados"](#) e ["Documentação do Azure para armazenamento de blobs"](#)
- ["Documentação do Google Cloud"](#)

Número máximo de sistemas

Com o licenciamento baseado em capacidade, o número máximo de sistemas Cloud Volumes ONTAP é limitado a 24 por conta do NetApp Console. Um *sistema* é um par de Cloud Volumes ONTAP HA, um sistema de nó único do Cloud Volumes ONTAP ou quaisquer VMs de armazenamento adicionais que você criar. A VM de armazenamento padrão não conta para o limite. Este limite se aplica a todos os modelos de licenciamento.

Por exemplo, digamos que você tenha três sistemas:

- Um sistema Cloud Volumes ONTAP de nó único com uma VM de armazenamento (esta é a VM de armazenamento padrão criada quando você implanta o Cloud Volumes ONTAP)

Este sistema conta como um sistema.

- Um sistema Cloud Volumes ONTAP de nó único com duas VMs de armazenamento (a VM de armazenamento padrão, mais uma VM de armazenamento adicional que você criou)

Este sistema conta como dois sistemas: um para o sistema de nó único e um para a VM de armazenamento adicional.

- Um par de Cloud Volumes ONTAP HA com três VMs de armazenamento (a VM de armazenamento padrão, mais duas VMs de armazenamento adicionais que você criou)

Este sistema conta como três sistemas: um para o par HA e dois para as VMs de armazenamento adicionais.

São seis sistemas no total. Você teria então espaço para mais 14 sistemas em sua conta.

Se você tiver uma implantação grande que exija mais de 24 sistemas, entre em contato com seu representante de conta ou equipe de vendas.

["Saiba mais sobre contas do Console"](#) .

["Saiba mais sobre os limites de armazenamento para AWS, Azure e Google Cloud"](#) .

Notas sobre o carregamento

Os detalhes a seguir podem ajudar você a entender como a cobrança funciona com o licenciamento baseado em capacidade.

Carga mínima

Há uma cobrança mínima de 4 TiB para cada VM de armazenamento de dados que tenha pelo menos um volume primário (leitura e gravação). Se a soma dos volumes primários for menor que 4 TiB, o Console aplicará a cobrança mínima de 4 TiB àquela VM de armazenamento.

Se você ainda não provisionou nenhum volume, a cobrança mínima não se aplica.

Para o pacote Essentials, a cobrança 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 armazenamento com 1 TiB de dados secundários, você será cobrado apenas por esse 1 TiB de dados. Com o tipo de pacote Profissional, a capacidade mínima de carregamento de 4 TiB se aplica independentemente do tipo de volume.

Excedentes

Se você exceder sua capacidade BYOL, será cobrado pelo excedente com base nas taxas horárias da sua assinatura do marketplace. O excedente é cobrado com base nas taxas do marketplace, com preferência pelo uso da capacidade disponível de outras licenças primeiro. Se sua licença BYOL expirar, você precisará migrar para um modelo de licenciamento baseado em capacidade por meio de marketplaces na nuvem.

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, do maior para o menor, 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 implantação ou tipo de volume.

O licenciamento é baseado inteiramente no tipo de volume criado nos sistemas Cloud Volumes ONTAP :

- Essentials Single Node: 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 ONTAP que podem fazer failover entre si

para acesso de dados sem interrupções.

- Nó único secundário essencial: volumes do tipo Proteção de Dados (DP) (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 Console o considerará como dados primários e os custos de cobrança serão calculados com base no tempo em que o volume esteve no modo de leitura/gravação. Quando o volume é novamente tornado somente leitura/DP, ele o considera como dados secundários novamente e cobra de acordo usando a melhor licença correspondente no Console.

- HA secundário essencial: volumes do tipo Proteção de Dados (DP) (normalmente volumes de destino SnapMirror ou SnapVault que são somente leitura) criados em um sistema Cloud Volumes ONTAP usando dois nós ONTAP que podem fazer failover um para o outro para acesso de dados sem interrupções.

Traga sua própria bebida

Se você adquiriu uma licença Essentials da NetApp (BYOL) e excedeu a capacidade licenciada para essa implantação e tipo de volume, o Console cobrará excedentes em 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 de acordo com as 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 *Essentials Secondary HA* de 500 TiB com 500 TiB de capacidade comprometida
- Uma licença *Essentials Single Node* de 500 TiB que tem apenas 100 TiB de capacidade comprometida

Outros 50 TiB são provisionados em um par HA com volumes secundários. Em vez de cobrar esses 50 TiB para o PAYGO, o Console cobra os 50 TiB excedentes da licença *Essentials Single Node*. Essa licença tem um preço mais alto que o *Essentials Secondary HA*, mas ela usa uma licença que você já comprou e não adicionará custos à sua fatura mensal.

Em **Administração > Licenças e assinaturas**, você pode ver 50 TiB cobrados pela licença *Essentials Single Node*.

Aqui está outro exemplo. Digamos que você tenha as seguintes licenças para o pacote Essentials:

- Uma licença *Essentials Secondary HA* de 500 TiB com 500 TiB de capacidade comprometida
- Uma licença *Essentials Single Node* de 500 TiB que tem apenas 100 TiB de capacidade comprometida

Outros 100 TiB são provisionados em um par HA com volumes primários. A licença que você comprou não tem capacidade comprometida de *Essentials Primary HA*. A licença *Essentials Primary HA* tem um preço mais alto do que as licenças *Essentials Primary Single Node* e *Essentials Secondary HA*.

Neste exemplo, o Console cobra excedentes na taxa de mercado para os 100 TiB adicionais. As cobranças excedentes aparecerão na sua fatura 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. Em seguida, você provisiona volumes de leitura e gravação (nó único primário) e volumes somente leitura (nó único secundário). Seu contrato de marketplace 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 horárias sob demanda (PAYGO) e adicionará custos à sua fatura mensal.

Armazenar

Protocolos de cliente suportados para Cloud Volumes ONTAP

O Cloud Volumes ONTAP oferece suporte aos protocolos de cliente 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 de cliente oferece um iniciador de software que é executado em uma porta Ethernet padrão.

NFS

NFS é o protocolo tradicional de acesso a arquivos 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 aos arquivos usando permissões no estilo UNIX, permissões no estilo NTFS ou uma combinação de ambos.

Os clientes podem acessar os mesmos arquivos usando os protocolos NFS e SMB.

PMEs

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 mistura de estilos de permissão é suportada.

S3

O Cloud Volumes ONTAP oferece suporte ao S3 como uma opção para armazenamento escalável. O suporte ao protocolo S3 permite que você configure o acesso do cliente S3 a objetos contidos em um bucket em uma VM de armazenamento (SVM).

["Documentação do ONTAP : Aprenda como funciona o multiprotocolo S3"](#) . ["Documentação do ONTAP : Aprenda a 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 suportado por provedores de nuvem. O NetApp Console não fornece nenhum recurso de gerenciamento para NVMe-TCP.

Para obter mais informações sobre como configurar o NVMe por meio do ONTAP, consulte o ["Documentação do ONTAP : Configurar uma VM de armazenamento para NVMe"](#) .

Discos e agregados usados para clusters Cloud Volumes ONTAP

Entender como o Cloud Volumes ONTAP usa o armazenamento em nuvem pode ajudar

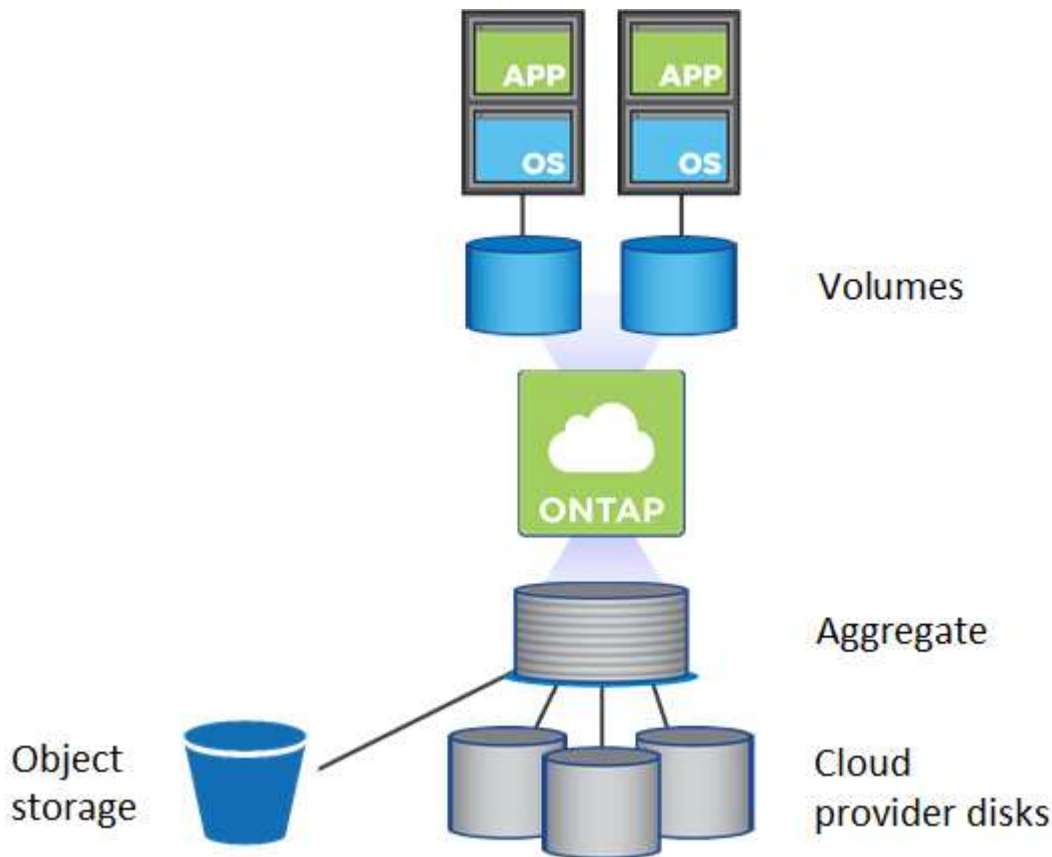
você a entender seus custos de armazenamento.



Você deve criar e excluir todos os discos e agregados do NetApp Console. Você não deve executar essas ações a partir 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

O Cloud Volumes ONTAP usa o armazenamento do provedor de nuvem como discos e os agrupa em um ou mais agregados. Agregados fornecem armazenamento 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 padrão do disco ao implantar o Cloud Volumes ONTAP.



A quantidade total de armazenamento adquirida de um provedor de nuvem é a *capacidade bruta*. A *capacidade utilizável* é menor porque aproximadamente 12 a 14 por cento é sobrecarga reservada para uso do Cloud Volumes ONTAP. Por exemplo, se o Console criar um agregado de 500 GiB, a capacidade utilizável será de 442,94 GiB.

Armazenamento AWS

Na AWS, o Cloud Volumes ONTAP usa armazenamento EBS para dados do usuário e armazenamento NVMe local como Flash Cache em alguns tipos de instância EC2.

Armazenamento EBS

Na AWS, um agregado pode conter até 6 discos, todos do mesmo tamanho. Mas se você tiver uma configuração compatível com o recurso Amazon EBS Elastic Volumes, um agregado poderá conter até 8 discos. ["Saiba mais sobre o suporte para Elastic Volumes"](#).

O tamanho máximo do disco é 16 TiB.

O tipo de disco EBS subjacente pode ser SSDs de uso geral (gp3 ou gp2), SSDs com IOPS provisionados (io1) ou HDDs com taxa de transferência otimizada (st1). Você pode emparelhar um disco EBS com o Amazon S3 para ["armazenamento de objetos de baixo custo"](#).



Não é recomendado hierarquizar dados para armazenamento de objetos ao usar HDDs com taxa de transferência otimizada (st1).

Armazenamento NVMe local

Alguns tipos de instância EC2 incluem armazenamento NVMe local, que o Cloud Volumes ONTAP usa como ["Cache Flash"](#).

Links relacionados

- ["Documentação da AWS: Tipos de volume do EBS"](#)
- ["Aprenda a escolher tipos e tamanhos de disco para seus sistemas na AWS"](#)
- ["Revisar limites de armazenamento para Cloud Volumes ONTAP na AWS"](#)
- ["Revise as configurações suportadas para o Cloud Volumes ONTAP na AWS"](#)

Armazenamento do Azure

No Azure, um agregado pode conter até 12 discos, todos do 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

Sistemas de nó único podem usar estes tipos de Azure Managed Disks:

- *Discos SSD gerenciados premium* oferecem alto desempenho para cargas de trabalho com uso intensivo de E/S a um custo mais alto.
- *Discos gerenciados SSD v2 Premium* oferecem maior desempenho com menor latência e menor custo para nós únicos e pares de HA, em comparação aos discos gerenciados SSD Premium.
- *Discos gerenciados SSD padrão* fornecem desempenho consistente para cargas de trabalho que exigem IOPS baixo.
- *Discos gerenciados de HDD padrão* são uma boa escolha se você não precisa de IOPS alto e quer reduzir seus custos.

Cada tipo de disco gerenciado tem um tamanho máximo de 32 TiB.

Você pode emparelhar um disco gerenciado com o armazenamento de Blobs do Azure para ["armazenamento de objetos de baixo custo"](#).

Pares HA

Os pares de HA usam dois tipos de discos que fornecem alto desempenho para cargas de trabalho com uso intensivo de E/S a um custo mais alto:

- *Blobs de página premium* com tamanho máximo de disco de 8 TiB
- *Discos gerenciados* com tamanho máximo de disco de 32 TiB

Links relacionados

- ["Aprenda a escolher tipos e tamanhos de disco para seus sistemas no Azure"](#)
- ["Inicie um par de Cloud Volumes ONTAP HA no Azure"](#)
- ["Documentação do Microsoft Azure: Tipos de disco gerenciado do Azure"](#)
- ["Documentação do Microsoft Azure: Visão geral dos blobs de páginas do Azure"](#)
- ["Revisar limites de armazenamento para Cloud Volumes ONTAP no Azure"](#)

Armazenamento em nuvem do Google

No Google Cloud, um agregado pode conter até 6 discos, todos do mesmo tamanho. O tamanho máximo do disco é 64 TiB.

O tipo de disco pode ser *Discos persistentes SSD zonais*, *Discos persistentes balanceados zonais* ou *Discos persistentes padrão zonais*. Você pode emparelhar discos persistentes com um bucket do Google Storage para ["armazenamento de objetos de baixo custo"](#).

Links relacionados

- ["Documentação do Google Cloud: Opções de armazenamento"](#)
- ["Revisar limites de armazenamento para o Cloud Volumes ONTAP no Google Cloud"](#)

Tipo RAID

O tipo de RAID para cada agregado do Cloud Volumes ONTAP é RAID0 (striping). O Cloud Volumes ONTAP depende do provedor de nuvem para disponibilidade e durabilidade do disco. Nenhum outro tipo de RAID é suportado.

Peças de reposição 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.

Saiba mais sobre o suporte para AWS Elastic Volumes com Cloud Volumes ONTAP

O suporte ao recurso Amazon EBS Elastic Volumes com um agregado Cloud Volumes ONTAP oferece melhor desempenho e capacidade adicional, ao mesmo tempo em que permite que o NetApp Console aumente automaticamente a capacidade do disco subjacente conforme necessário.

Benefícios

- Crescimento dinâmico do disco

O Console pode aumentar dinamicamente o tamanho dos discos enquanto o Cloud Volumes ONTAP

estiver em execução e enquanto os discos ainda estiverem conectados.

- Melhor desempenho

Agregados habilitados com Elastic Volumes podem ter até oito discos que são utilizados igualmente em dois grupos RAID. Esta configuração proporciona mais rendimento e desempenho consistente.

- Agregados maiores

O suporte para oito discos fornece 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 Elastic Volumes.

Observe que os limites de capacidade total do sistema permanecem os mesmos.

["Documentação da AWS: Saiba mais sobre Elastic Volumes da AWS"](#)

Configurações suportadas

O recurso Amazon EBS Elastic Volumes é compatível com versões específicas do Cloud Volumes ONTAP e tipos específicos de disco do EBS.

Versão Cloud Volumes ONTAP

O recurso Elastic Volumes é compatível com *novos* sistemas Cloud Volumes ONTAP criados a partir da versão 9.11.0 ou posterior. O recurso *não* é compatível com os sistemas Cloud Volumes ONTAP existentes que foram implantados antes da versão 9.11.0.

Por exemplo, o recurso Elastic Volumes não será suportado se você criou um sistema Cloud Volumes ONTAP 9.9.0 e depois 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 Elastic Volumes é habilitado automaticamente no nível agregado ao usar SSDs de uso geral (gp3) ou SSDs de IOPS provisionados (io1). O recurso Elastic Volumes não é compatível com agregados que usam qualquer outro tipo de disco.

Permissões necessárias da AWS

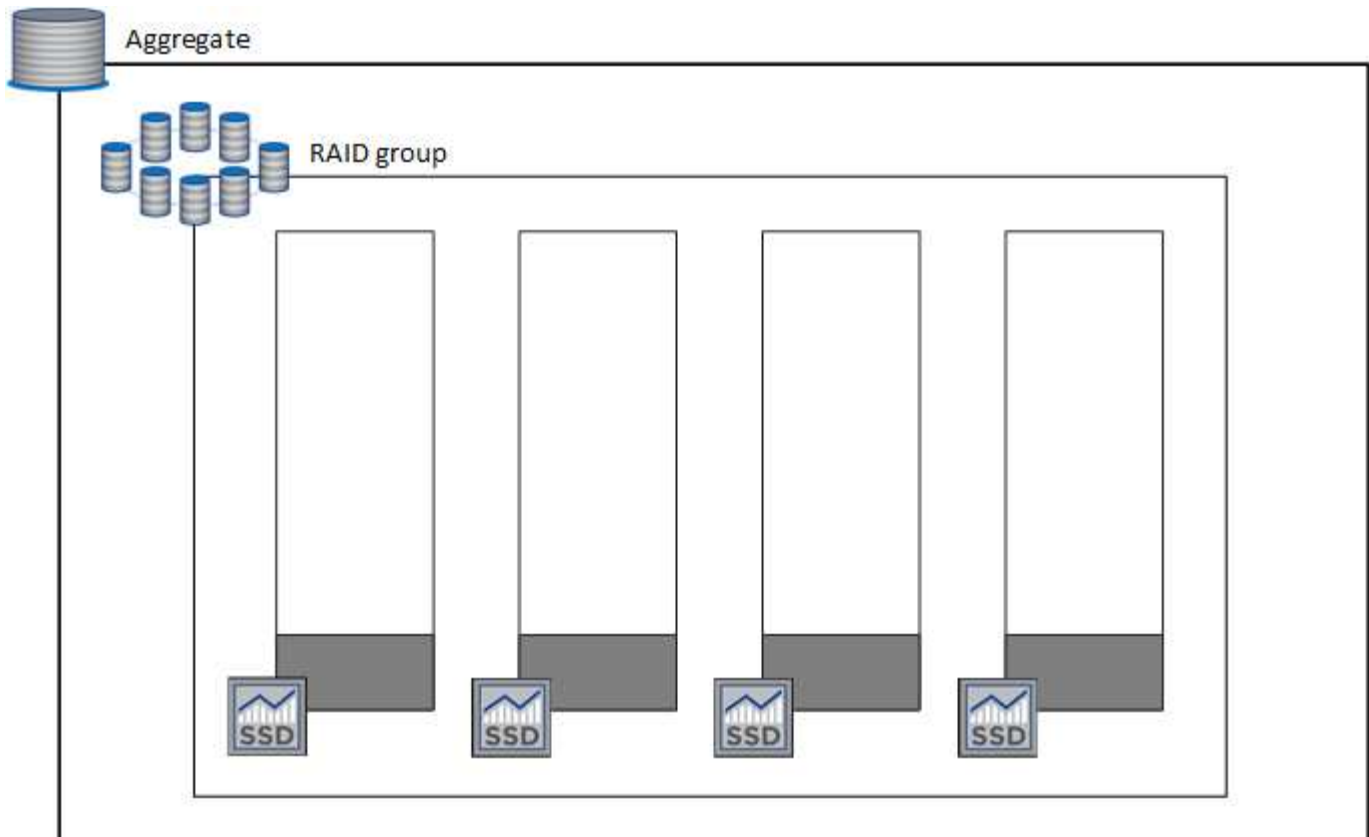
A partir da versão 3.9.19, o agente do Console requer as seguintes permissões para habilitar e gerenciar o recurso Elastic Volumes em um agregado Cloud Volumes ONTAP :

- ec2:DescribeVolumesModifications
- ec2:ModificarVolume

Essas permissões estão incluídas em ["as políticas fornecidas pela NetApp"](#)

Como funciona o suporte para Elastic Volumes

Um agregado que tem o recurso Elastic Volumes habilitado é composto por um ou dois grupos RAID. Cada grupo RAID tem quatro discos idênticos com a mesma capacidade. Aqui está um exemplo de um agregado de 10 TiB que tem quatro discos de 2,5 TiB cada:



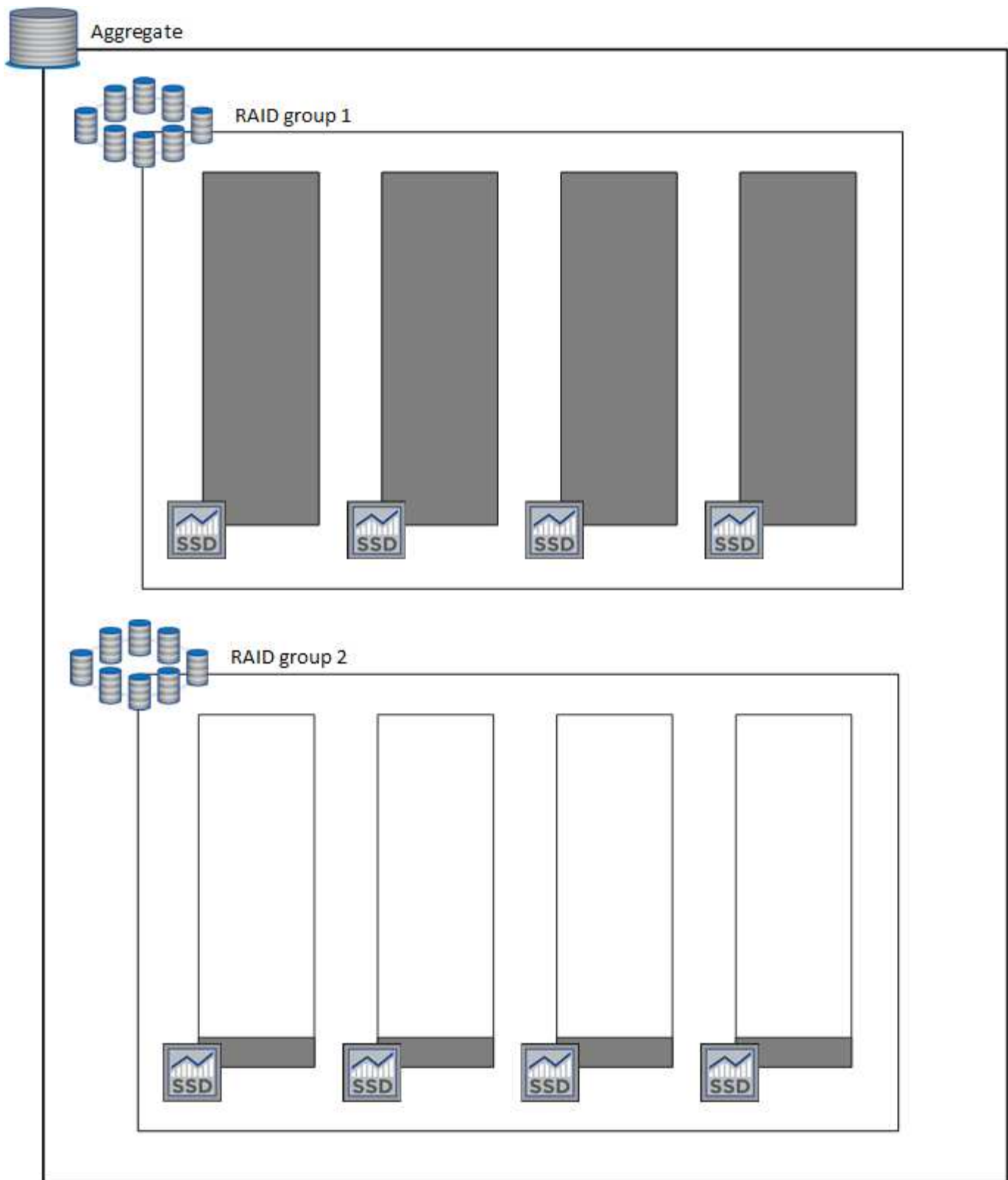
Quando o Console cria um agregado, ele começa com um grupo RAID. Se for necessária capacidade adicional, o agregado será aumentado aumentando a capacidade de todos os discos no grupo RAID na mesma quantidade. O aumento de capacidade é de no mínimo 256 GiB ou 10% do tamanho do agregado.

Por exemplo, se você tiver um agregado de 1 TiB, cada disco terá 250 GiB. 10% da capacidade do agregado é de 100 GiB. Isso é menor que 256 GiB, então o tamanho do agregado é aumentado pelo mínimo de 256 GiB (ou 64 GiB para cada disco).

O Console aumenta o tamanho dos discos enquanto o sistema Cloud Volumes ONTAP está em execução e enquanto os discos ainda estão conectados. A mudança não é disruptiva.

Se um agregado atingir 64 TiB (ou 16 TiB em cada disco), o Console criará um segundo grupo RAID para capacidade adicional. Este segundo grupo RAID funciona exatamente como o primeiro: ele tem quatro discos com exatamente 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 usa discos gp3 ou io1, o Console criará o volume em um agregado da seguinte maneira:

- Se houver um agregado gp3 ou io1 existente com Elastic Volumes habilitados, o Console criará o volume nesse agregado.

- Se houver vários agregados gp3 ou io1 com Volumes Elásticos habilitados, o Console criará o volume no agregado que requer a menor quantidade de recursos.
- Se o sistema tiver apenas agregados gp3 ou io1 que não estejam habilitados para Elastic Volumes, o volume será criado nesse agregado.



Embora esse cenário seja improvável, ele é possível em dois casos:

- Você desabilitou explicitamente o recurso Elastic Volumes ao criar um agregado da API.
- Você criou um novo sistema Cloud Volumes ONTAP a partir da interface do usuário. Nesse caso, o recurso Elastic Volumes é desabilitado no agregado inicial. Análise [Limitações](#) abaixo para saber mais.

- Se nenhum agregado existente tiver capacidade suficiente, o Console criará o agregado com os Volumes Elásticos habilitados 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 agente de Console funciona com Volumes Elásticos de forma semelhante a como funciona com outros tipos de agregados:

- Quando o modo Automático está ativado (esta é a configuração padrão), o Console aumenta automaticamente o tamanho dos agregados se capacidade adicional for necessária.
- Se você alterar o modo de gerenciamento de capacidade para Manual, o Console solicitará sua aprovação para comprar 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, o Console não pode solicitar nenhuma capacidade adicional para esse agregado.

Como trabalhar com volumes elásticos

Você pode executar estas tarefas com o Elastic Volumes:

- Crie um novo sistema que tenha volumes elásticos habilitados no agregado inicial ao usar discos gp3 ou io1

["Aprenda a criar um sistema Cloud Volumes ONTAP"](#)

- Crie um novo volume em um agregado que tenha Volumes Elásticos habilitados

Se você criar um volume que usa discos gp3 ou io1, o Console criará automaticamente o volume em um agregado que tenha Volumes Elásticos habilitados. Para mais detalhes, consulte [O que acontece quando você cria um volume](#) .

["Aprenda a criar volumes"](#) .

- Crie um novo agregado que tenha os Volumes Elásticos habilitados

O Elastic Volumes é habilitado 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.

Quando você cria o agregado, o Console solicita o tamanho da capacidade do agregado. Isso é diferente de outras configurações em que você escolhe o tamanho do disco e o número de discos.

A captura de tela a seguir mostra um exemplo de um novo agregado composto de discos gp3.

The screenshot shows the 'Select Disk Type' step in the AWS Management Console. At the top, there are four numbered steps: 1 Disk Type, 2 Aggregate details, 3 Tiering Data, and 4 Review. The main heading is 'Select Disk Type'. Below it, the 'Disk Type' dropdown menu is set to 'GP3 - General Purpose SSD Dynamic Performance'. A detailed box for 'General Purpose SSD (gp3) Disk Properties' is displayed, containing a description: 'General purpose SSD volume that balances price and performance (performance level is independent of storage capacity)'. It also shows two configurable fields: 'IOPS Value' set to 12000 and 'Throughput MB/s' set to 250, each with an information icon.

["Aprenda a criar agregados"](#) .

- Identificar agregados que tenham volumes elásticos habilitados

Ao acessar a página Alocação Avançada, você pode identificar se o recurso Volumes Elásticos está habilitado em um agregado. No exemplo a seguir, aggr1 tem Volumes Elásticos habilitados.

 aggr1

■ ONLINE

...

INFO

Disk Type

GP3 3000 IOPS

Disks

4

Volumes

2

Elastic Volumes

Enabled

S3 Tiering

Enabled

CAPACITY

Provisioned size

907.12 GiB

EBS Used

1.13 GiB

S3 Used

0 GiB

- Adicionar capacidade a um agregado

Embora o Console adicione capacidade automaticamente aos agregados conforme necessário, você pode aumentar a capacidade manualmente.

["Aprenda como aumentar a capacidade agregada"](#) .

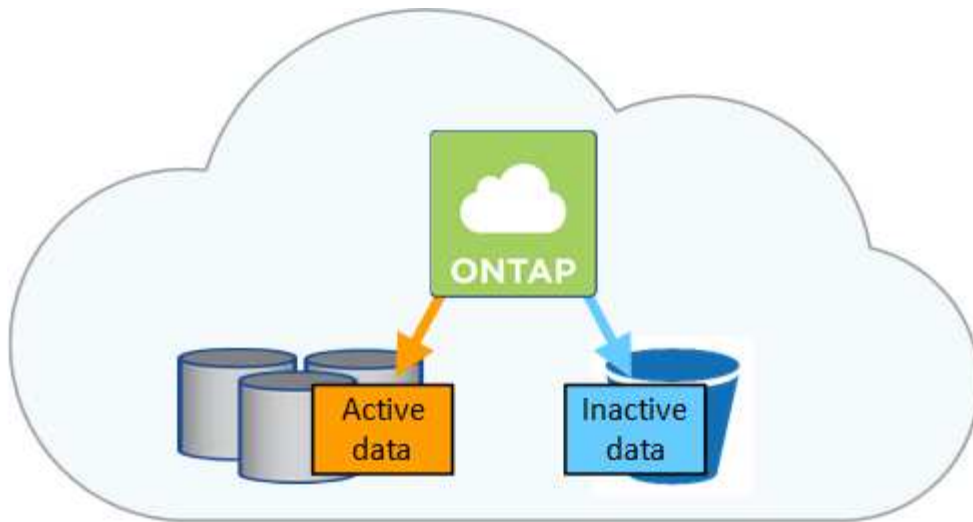
- Replique dados para um agregado que tenha Elastic Volumes habilitado

Se o sistema Cloud Volumes ONTAP de destino for compatível com Elastic Volumes, um volume de destino será colocado em um agregado que tenha Elastic Volumes habilitado (contanto que você escolha um disco gp3 ou io1).

["Aprenda a configurar a replicação de dados"](#)

Saiba mais sobre camadas de dados com o Cloud Volumes ONTAP na AWS, Azure ou Google Cloud

Reduza seus custos de armazenamento habilitando a hierarquização automatizada de dados inativos para armazenamento de objetos de baixo custo. Os dados ativos permanecem em SSDs ou HDDs de alto desempenho, enquanto os dados inativos são alocados em camadas para armazenamento de objetos de baixo custo. Isso permite que você recupere espaço no seu armazenamento primário e reduza o armazenamento secundário.



A hierarquização de dados é alimentada pela tecnologia FabricPool . O Cloud Volumes ONTAP fornece camadas de dados para todos os clusters do Cloud Volumes ONTAP sem uma licença adicional. Quando você habilita a hierarquização de dados, os dados hierarquizados para armazenamento de objetos incorrem em cobranças. Consulte a documentação do seu provedor de nuvem para obter detalhes sobre os custos de armazenamento de objetos.

Camadas de dados na AWS

Quando você habilita a hierarquização de dados 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.

Nível de desempenho

O nível de desempenho pode ser SSDs de uso geral (gp3 ou gp2) ou SSDs de IOPS provisionados (io1).

Não é recomendado hierarquizar dados para armazenamento de objetos ao usar HDDs com taxa de transferência otimizada (st1).

Nível de capacidade

Um sistema Cloud Volumes ONTAP organiza dados inativos em um único bucket S3.

O NetApp Console cria um único bucket S3 para cada sistema e o nomeia *fabric-pool-cluster unique identifier*. Um bucket S3 diferente não é criado para cada volume.

Quando o Console cria o bucket S3, ele usa as seguintes configurações padrão:

- Classe de armazenamento: Padrão
- Criptografia padrão: Desativada
- Bloquear acesso público: bloquear todo o acesso público
- Propriedade do objeto: ACLs habilitadas
- Controle de versão de bucket: Desativado
- Bloqueio de objeto: Desativado

Classes de armazenamento

A classe de armazenamento padrão para dados em camadas na AWS é *Standard*. Padrão é ideal para dados acessados com frequência armazenados em várias Zonas de Disponibilidade.

Se você não planeja acessar os dados inativos, pode reduzir seus custos de armazenamento alterando a classe de armazenamento para uma das seguintes: *Intelligent Tiering*, *One-Zone Infrequent Access*, *Standard-Infrequent 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 serão maiores se você acessar os dados, então considere isso antes de alterar a classe de armazenamento. ["Documentação do Amazon S3: Saiba mais sobre as classes de armazenamento do Amazon S3"](#) .

Você pode selecionar uma classe de armazenamento ao criar o sistema e pode alterá-la a qualquer momento depois. Para obter instruções sobre como alterar a classe de armazenamento, consulte ["Dados inativos em camadas para armazenamento de objetos de baixo custo"](#) .

A classe de armazenamento para camadas de dados abrange todo o sistema, não é por volume.

Camadas de dados no Azure

Quando você habilita a hierarquização de dados no Azure, o Cloud Volumes ONTAP usa discos gerenciados do Azure como uma camada de desempenho para dados ativos e o armazenamento de Blobs do Azure como uma camada de capacidade para dados inativos.

Nível de desempenho

O nível de desempenho pode ser SSDs ou HDDs.

Nível de capacidade

Um sistema Cloud Volumes ONTAP organiza dados inativos em um único contêiner Blob.

O Console cria uma nova conta de armazenamento com um contêiner para cada sistema Cloud Volumes ONTAP . O nome da conta de armazenamento é aleatório. Um contêiner diferente não é criado para cada volume.

O Console cria a conta de armazenamento com as seguintes configurações:

- Nível de acesso: Quente
- Desempenho: Padrão
- Redundância: De acordo com a implantação do Cloud Volume ONTAP
 - Zona de disponibilidade única: Armazenamento localmente redundante (LRS)
 - Zona de disponibilidade múltipla: Armazenamento redundante de zona (ZRS)
- Conta: StorageV2 (uso geral v2)
- Exigir transferência segura para operações da API REST: Habilitado
- Acesso à chave da conta de armazenamento: habilitado
- Versão mínima do TLS: Versão 1.2
- Criptografia de infraestrutura: Desativada

Níveis de acesso ao armazenamento

O nível de acesso de armazenamento padrão para dados em camadas no Azure é o nível *ativo*. A camada ativa é ideal para dados acessados com frequência na camada de capacidade.

Se você não planeja acessar os dados inativos na camada de capacidade, pode escolher a camada de

armazenamento *cool*, onde os dados inativos são retidos por no mínimo 30 dias. Você também pode optar pelo nível *frio*, onde os dados inativos são armazenados por no mínimo 90 dias. Com base em seus requisitos de armazenamento e considerações de custo, você pode selecionar o nível que melhor atende às suas necessidades. Quando você altera o nível de armazenamento para *frio* ou *frio*, os dados do nível de capacidade inativo são movidos diretamente para o nível de armazenamento frio ou frio. Os níveis frio e frio oferecem custos de armazenamento mais baixos em comparação ao nível quente, mas vêm com custos de acesso mais altos, então leve isso em consideração antes de alterar o nível de armazenamento. Consulte "[Documentação do Microsoft Azure: Saiba mais sobre os níveis de acesso ao armazenamento de Blobs do Azure](#)".

Você pode selecionar um nível de armazenamento ao adicionar um sistema Cloud Volumes ONTAP e pode alterá-lo a qualquer momento depois. Para obter detalhes sobre como alterar o nível de armazenamento, consulte "[Dados inativos em camadas para armazenamento de objetos de baixo custo](#)".

O nível de acesso ao armazenamento para hierarquização de dados abrange todo o sistema, não é por volume.

Camadas de dados no Google Cloud

Quando você habilita a hierarquização de dados no Google Cloud, o Cloud Volumes ONTAP usa discos persistentes como uma camada de desempenho para dados ativos e um bucket do Google Cloud Storage como uma camada de capacidade para dados inativos.

Nível de desempenho

O nível de desempenho pode ser discos persistentes SSD, discos persistentes balanceados ou discos persistentes padrão.

Nível de capacidade

Um sistema Cloud Volumes ONTAP organiza dados inativos em um único bucket do Google Cloud Storage.

O Console cria um bucket para cada sistema e o nomeia *fabric-pool-cluster unique identifier*. Um bucket diferente não é criado para cada volume.

Quando o Console cria o bucket, ele usa as seguintes configurações padrão:

- Tipo de localização: Região
- Classe de armazenamento: Padrão
- Acesso público: sujeito a ACLs de objetos
- 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 pode reduzir seus custos de armazenamento mudando para *Armazenamento Nearline* ou *Armazenamento Coldline*. 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 armazenamento de dados inativos existentes, você deve executar a designação manualmente.

Os custos de acesso serão maiores se você acessar os dados, então leve isso em consideração antes de alterar a classe de armazenamento. Para saber mais, consulte o ["Documentação do Google Cloud: Classes de armazenamento"](#).

Você pode selecionar um nível de armazenamento ao criar o sistema e pode alterá-lo a qualquer momento depois. Para obter detalhes sobre como alterar a classe de armazenamento, consulte ["Dados inativos em camadas para armazenamento de objetos de baixo custo"](#).

A classe de armazenamento para camadas de dados abrange todo o sistema, não é por volume.

Camadas de dados e limites de capacidade

Se você habilitar a hierarquização de dados, o limite de capacidade do sistema permanecerá o mesmo. O limite é distribuído entre o nível de desempenho e o nível de capacidade.

Políticas de níveis de volume

Para habilitar o armazenamento em camadas de dados, você deve selecionar uma política de armazenamento em camadas de volume ao criar, modificar ou replicar um volume. Você pode selecionar uma política diferente para cada volume.

Algumas políticas de hierarquização têm um período mínimo de resfriamento associado, que define o tempo que os dados do usuário em um volume devem permanecer inativos para que os dados sejam considerados "frios" e movidos para a camada 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). ["Aprenda como alterar o período de resfriamento"](#) e ["aprenda como alterar o limite"](#).

O Console permite que você escolha entre as seguintes políticas de camadas de volume ao criar ou modificar um volume:

Somente instantâneo

Depois que um agregado atinge 50% da capacidade, o Cloud Volumes ONTAP nivela os dados frios do usuário de cópias do Snapshot que não estão associadas ao sistema de arquivos ativo para o nível de capacidade. O período de resfriamento é de aproximadamente 2 dias.

Se lidos, os blocos de dados frios na camada de capacidade se tornam quentes e são movidos para a camada de desempenho.

Todos

Todos os dados (não incluindo metadados) são imediatamente marcados como frios e classificados no armazenamento de objetos o mais rápido possível. Não há necessidade de esperar 48 horas para que novos blocos em um volume esfriem. Observe que os blocos localizados no volume anterior à política Todos serem definidos levam 48 horas para esfriar.

Se lidos, os blocos de dados frios na camada de nuvem permanecem frios e não são gravados de volta na camada de desempenho. Esta política está disponível a partir do ONTAP 9.6.

Auto

Depois que um agregado atinge 50% da capacidade, o Cloud Volumes ONTAP divide os blocos de dados frios em um volume em uma camada de capacidade. Os dados frios incluem não apenas cópias de instantâneos, mas também dados frios do usuário do sistema de arquivos ativo. O período de resfriamento é de aproximadamente 31 dias.

Esta política é compatível a partir do Cloud Volumes ONTAP 9.4.

Se lidos aleatoriamente, os blocos de dados frios na camada de capacidade se tornam quentes e passam para a camada de desempenho. Se lidos por leituras sequenciais, como aquelas associadas a índices e verificações antivírus, os blocos de dados frios permanecem frios e não passam para a camada de desempenho.

Nenhum

Mantém os dados de um volume na camada de desempenho, impedindo que sejam movidos para a camada de capacidade.

Ao replicar um volume, você pode escolher se deseja hierarquizar os dados no armazenamento de objetos. Se fizer isso, o Console aplicará a política de **Backup** ao volume de proteção de dados. A partir do Cloud Volumes ONTAP 9.6, a política de camadas **All** substitui a política de backup.

Desativar o Cloud Volumes ONTAP afeta o período de resfriamento

Blocos de dados são resfriados por varreduras de resfriamento. Durante esse processo, os blocos que não foram utilizados têm sua temperatura movida (resfriada) para o próximo valor mais baixo. O tempo de resfriamento padrão depende da política de níveis de volume:

- Automático: 31 dias
- Somente instantâneo: 2 dias

O Cloud Volumes ONTAP deve estar em execução para que a verificação de resfriamento funcione. Se o Cloud Volumes ONTAP estiver desativado, o resfriamento também será interrompido. Como resultado, você pode experimentar tempos de resfriamento mais longos.



Quando o Cloud Volumes ONTAP é desativado, 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.

Configurando a hierarquização de dados

Para obter instruções e uma lista de configurações suportadas, consulte ["Dados inativos em camadas para armazenamento de objetos de baixo custo"](#).

Gerenciamento de armazenamento Cloud Volumes ONTAP

O NetApp Console fornece gerenciamento simplificado e avançado do armazenamento Cloud Volumes ONTAP.



Você deve criar e excluir todos os discos e agregados diretamente do Console. Você não deve executar essas ações a partir 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 armazenamento

O Console facilita o provisionamento de armazenamento para o Cloud Volumes ONTAP comprando discos e gerenciando agregados para você. Você só precisa criar volumes. Você pode usar uma opção de alocação avançada para provisionar agregados por conta própria, se desejar.

Provisionamento simplificado

Agregados fornecem armazenamento em nuvem para volumes. O Console cria agregados para você quando você inicia uma instância e quando provisiona volumes adicionais.

Quando você cria um volume, o Console faz uma das 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 suporta Volumes Elásticos, ele também aumenta o tamanho dos discos em um grupo RAID. ["Saiba mais sobre o suporte para Elastic Volumes"](#).

- Ele compra discos para um novo agregado e coloca o volume nesse agregado.

O Console determina onde colocar um novo volume observando vários fatores: o tamanho máximo de um agregado, se o provisionamento fino está habilitado e os limites de espaço livre para agregados.

Seleção de tamanho de disco para agregados na AWS

Quando o Console cria novos agregados para o Cloud Volumes ONTAP na AWS, ele aumenta gradualmente os tamanhos dos discos conforme o número de agregados aumenta para maximizar a capacidade do sistema antes de atingir os limites do disco de dados da AWS.

Por exemplo, o Console pode escolher os seguintes tamanhos de disco:

Número agregado	Tamanho do disco	Capacidade máxima agregada
1	500 GiB	3 TiB
4	1 TiB	6 TiB
6	2 TiB	12 TiB



Esse comportamento não se aplica a agregados que oferecem suporte ao recurso Amazon EBS Elastic Volumes. Agregados que têm Volumes Elásticos habilitados são compostos de um ou dois grupos RAID. Cada grupo RAID tem quatro discos idênticos com a mesma capacidade. ["Saiba mais sobre o suporte para Elastic Volumes"](#).

Você pode escolher o tamanho do disco usando a opção de alocação avançada.

Alocação avançada

Você também pode gerenciar agregados. ["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.

Gestão de capacidade

O administrador da organização ou da conta pode configurar o Console para notificá-lo sobre decisões de capacidade de armazenamento ou se deseja gerenciar automaticamente os requisitos de capacidade para você.

Esse comportamento é determinado pelo *Modo de Gerenciamento de Capacidade* em um agente de Console. O Modo de Gerenciamento de Capacidade afeta todos os sistemas Cloud Volumes ONTAP gerenciados por esse agente do Console. Se você tiver outro agente do Console, ele poderá ser configurado de forma diferente.

Gerenciamento automático de capacidade

O Modo de Gerenciamento de Capacidade é definido como automático por padrão. Neste modo, o Console verifica a proporção de espaço livre a cada 15 minutos para determinar se ela fica abaixo do limite especificado. Se for necessária mais capacidade, ele inicia a compra de novos discos, exclui coleções de discos não utilizadas (agregados), move volumes entre agregados conforme necessário e tenta 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, o Console comprará automaticamente novos discos para esse agregado para que os volumes possam continuar a crescer.

No caso de um agregado na AWS que suporta Volumes Elásticos, ele também aumenta o tamanho dos discos em um grupo RAID. ["Saiba mais sobre o suporte para Elastic Volumes"](#) .

+ * Se um agregado atingir o limite de capacidade e não puder suportar nenhum disco adicional, o Console moverá automaticamente um volume desse agregado para um agregado com capacidade disponível ou para um novo agregado.

+ Se o Console criar um novo agregado para o volume, ele escolherá um tamanho de disco que acomode o tamanho desse volume.

+ Observe que agora há espaço livre disponível no agregado original. Volumes existentes ou novos volumes podem usar esse espaço. O espaço não pode ser devolvido ao provedor de nuvem neste cenário.

- Se um agregado não contiver volumes por mais de 12 horas, o Console o excluirá.

Gerenciamento de LUNs com gerenciamento automático de capacidade

O gerenciamento automático de capacidade do Console não se aplica a LUNs. Ao criar um LUN, ele desabilita o recurso de crescimento automático.

Gerenciamento de capacidade manual

Se a organização ou o administrador da conta definir o Modo de Gerenciamento de Capacidade como manual, o Console informará você para tomar as ações apropriadas para decisões de capacidade. Os mesmos exemplos descritos no modo automático se aplicam ao modo manual, mas cabe a você aceitar as ações.

Saber mais

["Aprenda a modificar o modo de gerenciamento de capacidade"](#) .

Velocidade de gravação

O NetApp Console 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, bem como 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-se a probabilidade de perda de dados no caso de uma interrupção não planejada do sistema ou de 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, há potencial para perda de dados caso ocorra uma interrupção não planejada do sistema.

A quantidade de dados que podem ser perdidos no caso de uma interrupção não planejada do sistema é o intervalo 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 armazenamento fornecido pelo seu provedor de nuvem pode afetar o tempo de processamento do ponto de consistência.

Quando usar alta velocidade de gravação

Alta velocidade de gravação é uma boa escolha se um desempenho de gravação rápido for necessário para sua carga de trabalho e você puder suportar o 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 alta velocidade de gravação, deverá garantir proteção contra gravação na camada do aplicativo ou que os aplicativos possam tolerar perda de dados, caso isso ocorra.

Alta velocidade de gravação com um par HA na AWS

Se você planeja habilitar alta velocidade de gravação em um par de HA na AWS, deve entender a diferença nos níveis de proteção entre uma implantação de várias Zonas de Disponibilidade (AZ) e uma implantação de uma única AZ. A implantação de um par de HA em várias AZs oferece mais resiliência e pode ajudar a reduzir a chance de perda de dados.

["Saiba mais sobre pares de HA na AWS"](#) .

Configurações que suportam alta velocidade de gravação

Nem todas as configurações do Cloud Volumes ONTAP oferecem suporte a 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 a alta velocidade de gravação com todos os tipos de instância.

A partir da versão 9.8, o Cloud Volumes ONTAP oferece suporte à alta velocidade de gravação com pares HA ao usar quase todos os tipos de instância EC2 suportados, exceto m5.xlarge e r5.xlarge.

["Saiba mais sobre as instâncias do Amazon EC2 compatíveis com o Cloud Volumes ONTAP"](#) .

Azul

Se você usar um sistema de nó único, o Cloud Volumes ONTAP oferece suporte a alta velocidade de gravação com todos os tipos de VM.

Se você usar um par de HA, o Cloud Volumes ONTAP oferece suporte a alta velocidade de gravação com vários tipos de VM, a partir da versão 9.8. Vá para o ["Notas de versão do Cloud Volumes ONTAP"](#) para visualizar 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 com todos os tipos de máquina.

Se você usar um par de HA, o Cloud Volumes ONTAP oferecerá suporte a alta velocidade de gravação com vários tipos de VM, a partir da versão 9.13.0. Vá para o ["Notas de versão do Cloud Volumes ONTAP"](#) para visualizar os tipos de VM que suportam alta velocidade de gravação.

["Saiba mais sobre os tipos de máquinas do Google Cloud compatíveis com o Cloud Volumes ONTAP"](#) .

Como selecionar uma velocidade de gravação

Você pode escolher uma velocidade de gravação ao adicionar um novo sistema Cloud Volumes ONTAP e pode ["alterar 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 conseguir inicializar e continuar a fornecer dados sem intervenção do usuário.

Como interromper o acesso aos dados em caso de perda de dados

Se você estiver preocupado com a perda de dados, quiser que os aplicativos parem de ser executados após a perda de dados e que o acesso aos dados seja retomado após o problema de perda de dados ser resolvido adequadamente, você pode usar a opção NVFAIL da CLI para atingir esse objetivo.

Para habilitar a opção NVFAIL

```
vol modify -volume <vol-name> -nvfail on
```

Para verificar as configurações NVFAIL

```
vol show -volume <vol-name> -fields nvfail
```

Para desabilitar a opção NVFAIL

```
vol modify -volume <vol-name> -nvfail off
```

Quando ocorre perda de dados, um volume NFS ou iSCSI com NVFAIL habilitado deve parar de fornecer dados (não há impacto no CIFS, que é um protocolo sem estado). Para mais detalhes, consulte ["Como o NVFAIL afeta o acesso a volumes NFS ou LUNs"](#).

Para verificar o estado NVFAIL

```
vol show -fields in-nvfailed-state
```

Depois que o problema de perda de dados for resolvido adequadamente, você poderá 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
```

Cache Flash

Algumas configurações do Cloud Volumes ONTAP incluem armazenamento 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 cache inteligente em tempo real de dados de usuários lidos recentemente e metadados do NetApp . É eficaz para cargas de trabalho aleatórias com uso intensivo de leitura, incluindo bancos de dados, e-mail e serviços de arquivo.

Configurações suportadas

O Flash Cache é compatível com configurações específicas do Cloud Volumes ONTAP . Veja as configurações suportadas no ["Notas de versão do Cloud Volumes ONTAP"](#)

Limitações

- Ao configurar o Flash Cache para o Cloud Volumes ONTAP 9.12.0 ou anterior na AWS, a compactação deve ser desabilitada 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 desabilitar a compactação.

Pule a seleção das configurações de eficiência de armazenamento ao criar um volume no NetApp Console ou crie um volume e, em seguida, ["desabilitar a compactação de dados usando a CLI"](#) .

- O reaquecimento do cache após uma reinicialização não é suportado com o Cloud Volumes ONTAP.

Saiba mais sobre o armazenamento WORM no Cloud Volumes ONTAP

Você pode ativar o armazenamento WORM (gravação única e leitura múltipla) em um sistema Cloud Volumes ONTAP para reter arquivos em formato inalterado por um período de retenção especificado. O armazenamento WORM na nuvem é alimentado pela tecnologia SnapLock , o que significa que os arquivos WORM são protegidos no nível do arquivo.

O recurso WORM está disponível para uso com assinaturas de traga sua própria licença (BYOL) e de mercado para suas licenças, sem custo adicional. Entre em contato com seu representante de vendas da NetApp para adicionar o WORM à sua licença atual.

Como funciona o armazenamento WORM

Depois que um arquivo é enviado para o armazenamento WORM, ele não pode ser modificado, mesmo após o período de retenção ter expirado. Um relógio à prova de violação determina quando o período de retenção de um arquivo WORM expirou.

Após o término do período de retenção, você será responsável por excluir todos os arquivos dos quais não precisa mais.

Ativando o armazenamento WORM

A maneira como você ativa o armazenamento 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 habilitar ou desabilitar o WORM no nível do volume.

Ao adicionar um sistema Cloud Volumes ONTAP , você será solicitado a habilitar ou desabilitar o armazenamento WORM:

- Se você habilitar o armazenamento WORM ao adicionar um sistema, cada volume criado no NetApp Console terá o WORM habilitado. Mas você pode usar o ONTAP System Manager ou o ONTAP CLI para criar volumes que tenham o WORM desabilitado.
- Se você desabilitar o armazenamento WORM ao adicionar um sistema, todos os volumes criados no Console, no ONTAP System Manager ou no ONTAP CLI terão o WORM desabilitado.

Versão 9.10.0 e anteriores

Você pode ativar o armazenamento WORM em um sistema Cloud Volumes ONTAP ao adicionar um novo sistema. Cada volume criado no Console tem o WORM habilitado. Não é possível desabilitar o armazenamento WORM em volumes individuais.

Enviando arquivos para WORM

Você pode usar um aplicativo para confirmar arquivos no WORM por NFS ou CIFS, ou usar o ONTAP CLI para confirmar arquivos no WORM automaticamente. Você também pode usar um arquivo WORM anexável para reter dados que são gravados incrementalmente, como informações de log.

Depois de ativar o armazenamento WORM em um sistema Cloud Volumes ONTAP , você deve usar a CLI do ONTAP para todo o gerenciamento do armazenamento WORM. Para obter instruções, consulte o ["Documentação ONTAP sobre SnapLock"](#) .

Habilitando WORM em um sistema Cloud Volumes ONTAP

Você pode habilitar o armazenamento WORM ao criar um sistema Cloud Volumes ONTAP no Console. Você também pode habilitar o WORM em um sistema se o WORM não estiver habilitado nele durante a criação. Após habilitá-lo, você não poderá desabilitar o WORM.

Sobre esta tarefa

- O WORM é compatível com o ONTAP 9.10.1 e posteriores.
- WORM com backup é suportado no ONTAP 9.11.1 e posteriores.

Passos

1. Na página **Sistemas**, clique duas vezes no nome do sistema no qual você deseja habilitar o WORM.
2. Na guia Visão geral, clique no painel Recursos e depois clique no ícone de lápis ao lado de **WORM**.

Se o WORM já estiver habilitado no sistema, o ícone de lápis será desabilitado.

3. Na página **WORM**, defina o período de retenção para o relógio de conformidade do cluster.

Para mais informações, consulte o ["Documentação do ONTAP : Inicializar o Relógio de Conformidade"](#) .

4. Clique em **Definir**.

Depois que você terminar

Você pode verificar o status do **WORM** no painel Recursos. Após o WORM ser habilitado, a licença SnapLock é instalada automaticamente no cluster. Você pode visualizar a licença do SnapLock no ONTAP System Manager.

Excluindo arquivos WORM

Você pode excluir arquivos WORM durante o período de retenção usando o recurso de exclusão privilegiada.

Para obter instruções, consulte o ["Documentação do ONTAP"](#) .

WORM e hierarquização de dados

Ao criar um novo sistema Cloud Volumes ONTAP 9.8 ou posterior, você pode habilitar a hierarquização de dados e o armazenamento WORM juntos. Habilitar o armazenamento em camadas de dados com WORM permite que você organize os dados em camadas em um armazenamento de objetos na nuvem.

Você deve entender o seguinte sobre como habilitar a hierarquização de dados e o armazenamento WORM:

- Os dados em camadas no armazenamento de objetos não incluem a funcionalidade ONTAP WORM. Para garantir a capacidade WORM de ponta a ponta, você precisará configurar as permissões do bucket corretamente.
- Os dados em camadas no armazenamento de objetos não carregam a funcionalidade WORM, o que significa que tecnicamente qualquer pessoa com acesso total aos buckets e contêineres pode ir e excluir os objetos em camadas pelo ONTAP.
- A reversão ou o downgrade para o Cloud Volumes ONTAP 9.8 é bloqueado após a ativação do WORM e da hierarquização.

Limitações

- O armazenamento WORM no Cloud Volumes ONTAP opera sob um modelo de "administrador de armazenamento confiável". Embora os arquivos WORM sejam protegidos contra alterações ou modificações, os volumes podem ser excluídos por um administrador de cluster, mesmo que contenham dados WORM não expirados.
- Além do modelo de administrador de armazenamento confiável, o armazenamento WORM no Cloud Volumes ONTAP também opera implicitamente sob um modelo de "administrador de nuvem confiável". Um administrador de nuvem pode excluir dados WORM antes da data de expiração removendo ou editando o armazenamento em nuvem diretamente do provedor de nuvem.

Link relacionado

- ["Crie cópias de Snapshot invioláveis para armazenamento WORM"](#)

Pares de alta disponibilidade

Saiba mais sobre pares de alta disponibilidade do Cloud Volumes ONTAP na AWS

Uma configuração de alta disponibilidade (HA) do Cloud Volumes ONTAP fornece operações ininterruptas e tolerância a falhas. Na AWS, os dados são espelhados de

forma síncrona entre os dois nós.

Componentes HA

Na AWS, as configurações de HA do Cloud Volumes ONTAP incluem os seguintes componentes:

- Dois nós Cloud Volumes ONTAP cujos dados são espelhados de forma síncrona entre si.
- Uma instância mediadora que fornece um canal de comunicação entre os nós para auxiliar nos processos de aquisição e devolução de armazenamento.

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 anteriores, o Debian 10 foi instalado no mediador.

Atualizações

Quando você atualiza o Cloud Volumes ONTAP, o NetApp Console também atualiza a instância do mediador conforme necessário.

Acesso à instância

Ao criar um par de Cloud Volumes ONTAP HA no Console, você 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 terceirizados

Agentes de terceiros ou extensões de VM não são suportados na instância do mediador.

Aquisição e devolução de armazenamento

Se um nó cair, o outro nó pode fornecer dados para seu parceiro para fornecer serviço de dados contínuo. Os clientes podem acessar os mesmos dados do nó do parceiro porque os dados foram espelhados de forma síncrona para o parceiro.

Após a reinicialização do nó, o parceiro deve ressincronizar os dados antes de poder retornar o armazenamento. O tempo que leva para ressincronizar os dados depende de quantos dados foram alterados enquanto o nó estava inativo.

A aquisição, a ressincronização e a devolução do armazenamento são todas automáticas por padrão. Nenhuma ação do usuário é necessária.

RPO e RTO

Uma configuração de HA mantém alta disponibilidade dos seus dados da seguinte maneira:

- O objetivo do ponto de recuperação (RPO) é 0 segundos. Seus dados são transacionalmente consistentes, sem perda de dados.
- O objetivo do 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 dos seus dados implantando uma configuração de HA em várias zonas de disponibilidade (AZs) ou em uma única zona de disponibilidade (AZ). Você deve analisar mais detalhes sobre cada configuração para escolher a que melhor atende às suas necessidades.

Várias zonas de disponibilidade

A implantação de uma configuração de HA em várias zonas de disponibilidade (AZs) garante alta disponibilidade dos seus dados caso ocorra uma falha em uma AZ ou em uma instância que execute um nó do Cloud Volumes ONTAP. Você deve entender como os endereços IP do NAS afetam o acesso aos dados e o failover de armazenamento.

Acesso a dados NFS e CIFS

Quando uma configuração de HA é distribuída em várias Zonas de Disponibilidade, *endereços IP flutuantes* permitem o acesso do cliente NAS. Os endereços IP flutuantes, que devem estar fora dos blocos CIDR para todas as VPCs na região, podem migrar entre nós quando ocorrem falhas. Eles não são nativamente acessíveis a clientes que estão fora do VPC, a menos que você ["configure um gateway de trânsito da AWS"](#).

Se você não conseguir configurar um gateway de trânsito, endereços IP privados estarão disponíveis para clientes NAS que estão fora da VPC. No entanto, esses endereços IP são estáticos — eles não podem fazer failover entre nós.

Você deve revisar os requisitos para endereços IP flutuantes e tabelas de rotas 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.

Para mais informações, consulte ["Requisitos de rede da AWS para Cloud Volumes ONTAP HA em várias AZs"](#).

acesso a dados iSCSI

A comunicação de dados entre VPCs não é um problema, pois o iSCSI não usa endereços IP flutuantes.

Aquisição e devolução para iSCSI

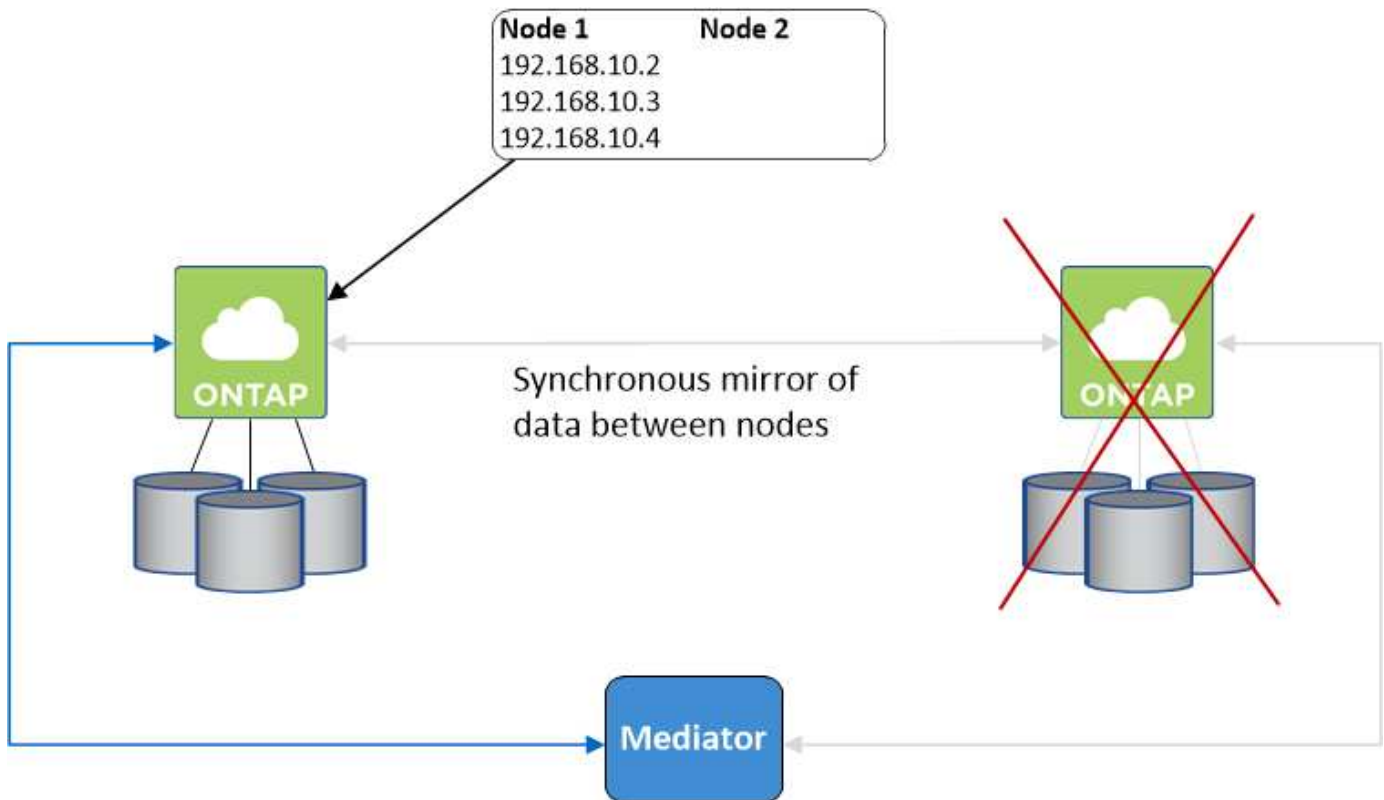
Para iSCSI, o Cloud Volumes ONTAP usa E/S multicaminho (MPIO) e Acesso de Unidade Lógica Assimétrica (ALUA) para gerenciar o failover de caminho entre os caminhos otimizados ativos e não otimizados.



Para obter informações sobre quais configurações específicas de host oferecem suporte a ALUA, consulte o ["Ferramenta de Matriz de Interoperabilidade da NetApp"](#) e o ["Guia de hosts SAN e clientes em nuvem"](#) para o seu sistema operacional host.

Aquisição e devolução para NAS

Quando ocorre a aquisição em uma configuração NAS usando IPs flutuantes, o endereço IP flutuante do nó que os clientes usam para acessar dados é movido para o outro nó. A imagem a seguir mostra a aquisição de armazenamento em uma configuração NAS usando IPs flutuantes. Se o nó 2 ficar inativo, o endereço IP flutuante do nó 2 será movido para o nó 1.



Os IPs de dados do NAS usados para acesso externo à VPC 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 a ficar online, remonte os clientes nos volumes usando o endereço IP original. Esta etapa é necessária para evitar a transferência de dados desnecessários entre dois nós de HA, o que pode causar impacto significativo no desempenho e na estabilidade.

Você pode localizar o endereço IP correto no Console 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 dos seus dados se uma instância que executa um nó do Cloud Volumes ONTAP falhar. Todos os dados são acessíveis nativamente de fora da VPC.



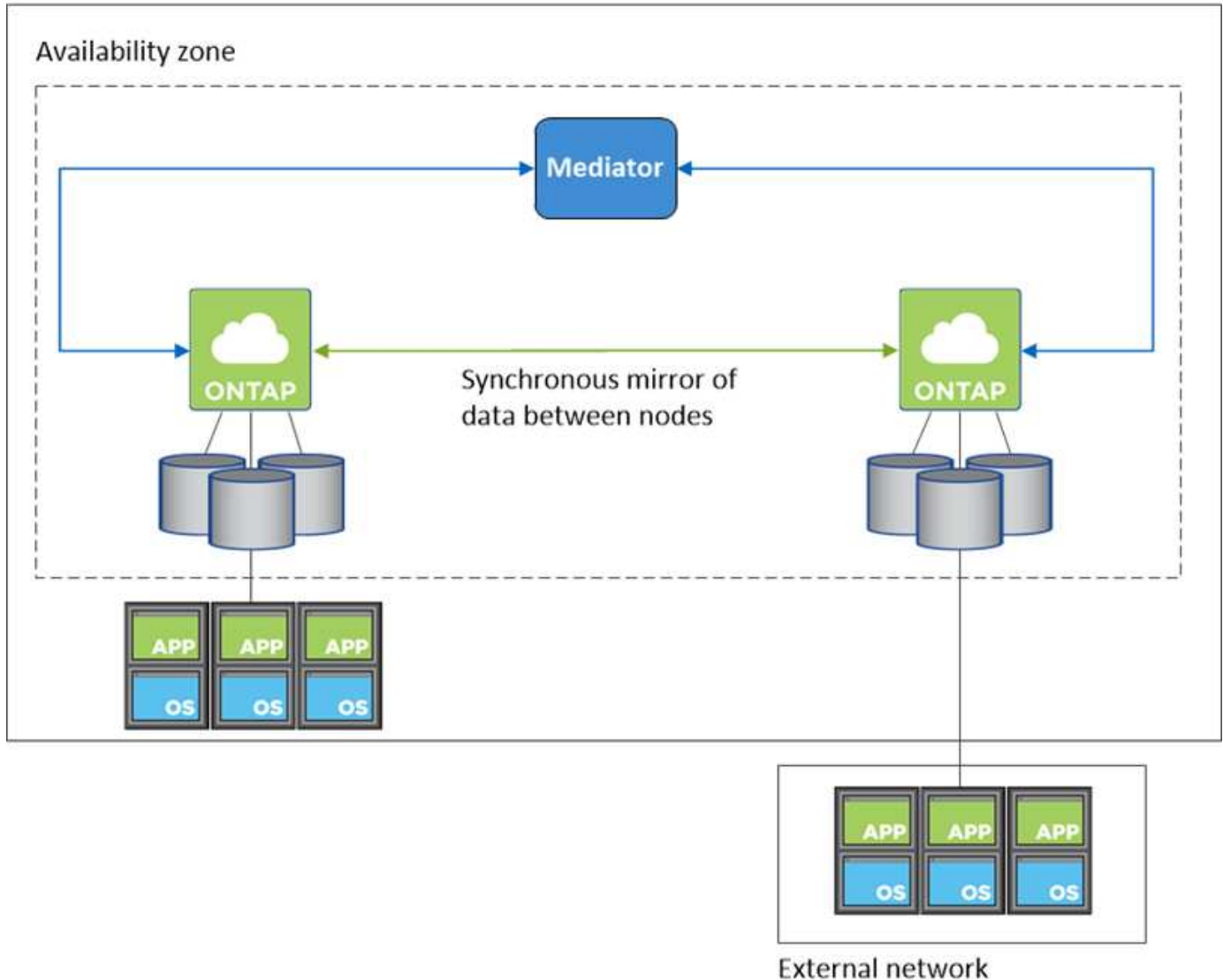
O Console cria um "[Documentação da AWS: Grupo de posicionamento de spread da AWS](#)" e inicia os dois nós HA naquele grupo de posicionamento. O grupo de posicionamento reduz o risco de falhas simultâneas ao distribuir as instâncias entre hardwares subjacentes distintos. Esse recurso melhora a redundância de uma perspectiva de computação e não de 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 de dentro da VPC e de fora dela.

A imagem a seguir mostra uma configuração de HA em uma única AZ. Os dados podem ser acessados de dentro da VPC e de fora dela.

VPC in AWS



Aquisição e devolução

Para iSCSI, o Cloud Volumes ONTAP usa E/S multicaminho (MPIO) e Acesso de Unidade Lógica Assimétrica (ALUA) para gerenciar o failover de caminho entre os caminhos otimizados ativos e não otimizados.



Para obter informações sobre quais configurações específicas de host oferecem suporte a ALUA, consulte o "[Ferramenta de Matriz de Interoperabilidade da NetApp](#)" e o "[Guia de hosts SAN e clientes em nuvem](#)" para o seu sistema operacional host.

Para configurações de 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 armazenamento, computação, banco de dados e outros serviços selecionados da AWS estão localizados perto de grandes cidades e áreas industriais. Com o AWS Local Zones, você pode trazer os serviços da AWS para mais perto de você, o que melhora a latência das suas cargas de trabalho e mantém os bancos de dados localmente. No Cloud Volumes ONTAP,

Você pode implantar uma única AZ ou várias configurações de AZ nas Zonas Locais da AWS.



As Zonas Locais da AWS são suportadas ao usar o Console nos modos padrão e privado. No momento, as Zonas Locais da AWS não são suportadas no modo restrito.

Exemplo de configurações de zona local da AWS

O Cloud Volumes ONTAP na AWS oferece suporte apenas ao modo de alta disponibilidade (HA) em uma única zona de disponibilidade. Implantações de nó único não são suportadas.

O Cloud Volumes ONTAP não oferece suporte a níveis de dados, níveis de nuvem e instâncias não qualificadas em zonas locais da AWS.

A seguir estão alguns exemplos de configurações:

- Zona de disponibilidade única: ambos os nós do cluster e o mediador estão na mesma Zona Local.
- Várias zonas de disponibilidade Em configurações de várias zonas de disponibilidade, há três instâncias, dois nós e um mediador. Uma das três instâncias deve estar em uma zona separada. Você pode escolher como configurar isso.

Aqui estão três exemplos de configurações:

- Cada nó do 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 em uma zona de disponibilidade.
- Cada nó do 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 suporta apenas essas configurações. Selecionar tipos de disco não suportados ou instâncias não qualificadas na configuração da Zona Local da AWS pode resultar em falha na implantação. A hierarquização de dados para o AWS S3 não está disponível nas Zonas Locais da AWS devido à falta de conectividade.

Como funciona o armazenamento em um par HA

Ao contrário de um cluster ONTAP , o armazenamento em um par Cloud Volumes ONTAP HA não é compartilhado entre os nós. Em vez disso, os dados são espelhados de forma síncrona entre os nós para que estejam disponíveis em caso de falha.

Alocação de armazenamento

Quando você cria um novo volume e discos adicionais são necessários, o Console aloca o mesmo número de discos para ambos os nós, cria um agregado espelhado e, em seguida, cria o novo volume. Por exemplo, se dois discos forem necessários para o volume, o Console alocará dois discos por nó, para um total de quatro discos.

Configurações de armazenamento

Você pode usar um par de HA como uma configuração ativa-ativa, na qual ambos os nós fornecem dados aos clientes, ou como uma configuração ativa-passiva, na qual o nó passivo responde às solicitações de dados somente se tiver assumido o armazenamento do nó ativo.



Você pode configurar uma configuração ativa-ativa somente ao usar o Console na Exibição do Sistema de Armazenamento.

Expectativas de desempenho

Uma configuração do Cloud Volumes ONTAP HA replica dados de forma síncrona entre nós, o que consome largura de banda da rede. Como resultado, você pode esperar o seguinte desempenho em comparação com uma configuração de nó único do Cloud Volumes ONTAP :

- Para configurações de HA que fornecem dados de apenas um nó, o desempenho de leitura é comparável ao desempenho de leitura de uma configuração de nó único, enquanto o desempenho de gravação é menor.
- Para configurações de HA que atendem dados de ambos os nós, o desempenho de leitura é maior que o desempenho de leitura de uma configuração de nó único, e o desempenho de gravação é o mesmo ou maior.

Para obter mais detalhes sobre o desempenho do Cloud Volumes ONTAP , consulte "[Desempenho](#)" .

Acesso do cliente ao armazenamento

Os clientes devem acessar os volumes NFS e CIFS usando o endereço IP de dados do nó no qual o volume reside. Se clientes NAS acessarem um volume usando o endereço IP do nó parceiro, o tráfego passará entre ambos os nós, o que reduz o desempenho.



Se você mover um volume entre nós em um par de HA, deverá remontar o volume usando o endereço IP do outro nó. Caso contrário, você poderá ter um desempenho reduzido. Se os clientes oferecerem suporte a referências NFSv4 ou redirecionamento de pasta para CIFS, você poderá habilitar esses recursos nos sistemas Cloud Volumes ONTAP para evitar a remontagem do volume. Para mais detalhes, consulte a documentação do ONTAP .

Você pode identificar facilmente o endereço IP correto por meio da opção *Mount Command* no painel de gerenciamento de volumes.

Volume Actions

View volume details

Mount command

Clone volume

Edit volume tags

Edit volume settings

Delete volume

Protection Actions

Advanced Actions

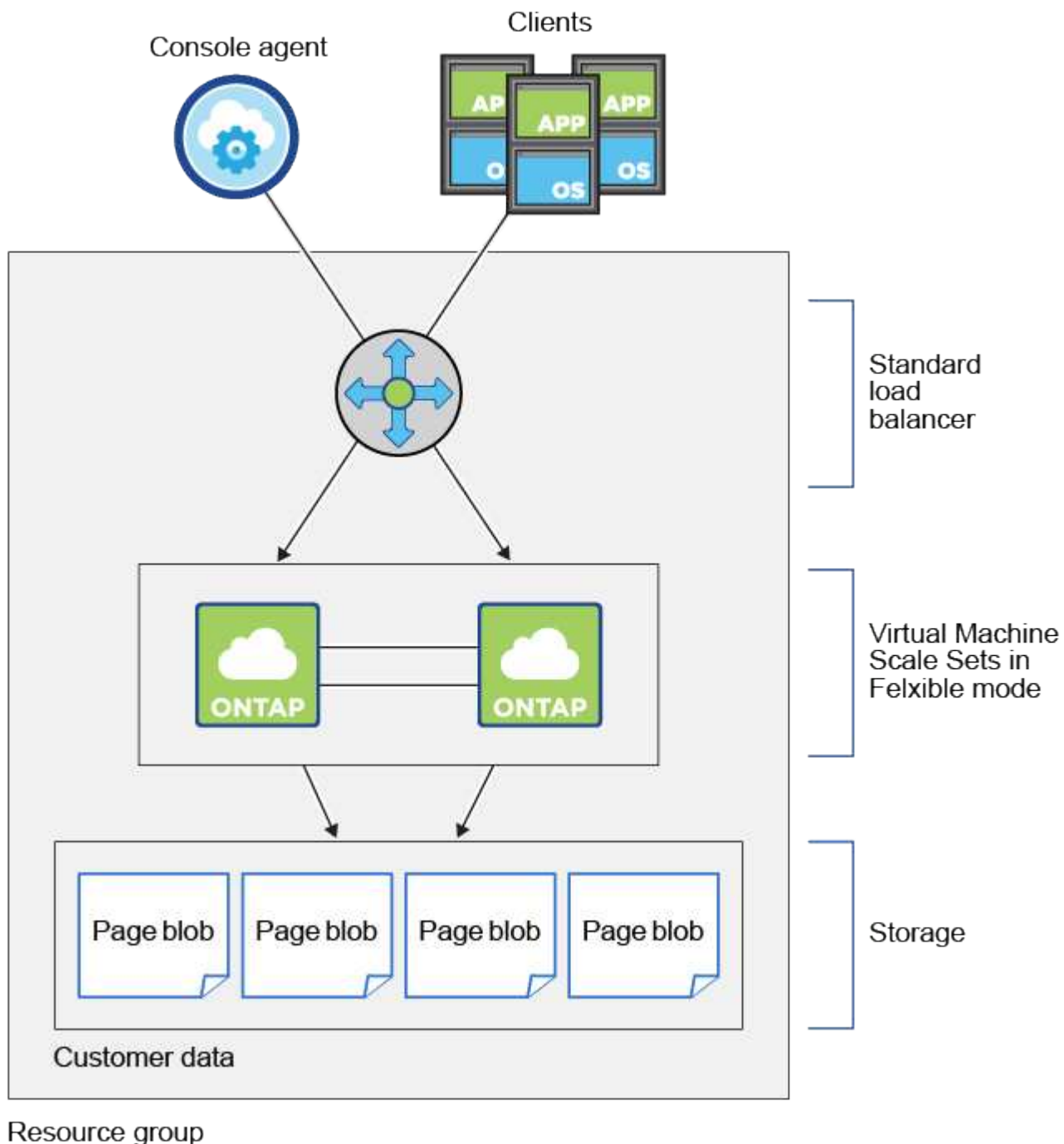
Saiba mais sobre pares de alta disponibilidade do Cloud Volumes ONTAP no Azure

Um par de alta disponibilidade (HA) do Cloud Volumes ONTAP fornece confiabilidade empresarial e operações contínuas em caso de falhas no seu ambiente de nuvem. No Azure, o armazenamento 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 NetApp Console implanta para você:

Balancedor de Carga Padrão do Azure

O balanceador de carga gerencia o tráfego de entrada para o par Cloud Volumes ONTAP HA.

VMs em zonas de disponibilidade única

A partir do Cloud Volumes ONTAP 9.15.1, você pode criar e gerenciar máquinas virtuais (VMs)

heterogêneas 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 disponibilidade ideal. Para saber mais sobre o modo de orquestração flexível que permite esse recurso, consulte o ["Documentação do Microsoft Azure: Conjuntos de dimensionamento de máquinas virtuais"](#) .

Discos

Os dados do cliente residem em blobs de páginas do Premium Storage. Cada nó tem acesso ao armazenamento do outro nó. Armazenamento adicional também é necessário para ["dados de inicialização, raiz e núcleo"](#) .

Contas de armazenamento

- Uma conta de armazenamento é necessária para discos gerenciados.
- Uma ou mais contas de armazenamento são necessárias para os blobs da página de Armazenamento Premium, pois o limite de capacidade de disco por conta de armazenamento é atingido.

["Documentação do Microsoft Azure: metas de escalabilidade e desempenho do Azure Storage para contas de armazenamento"](#) .

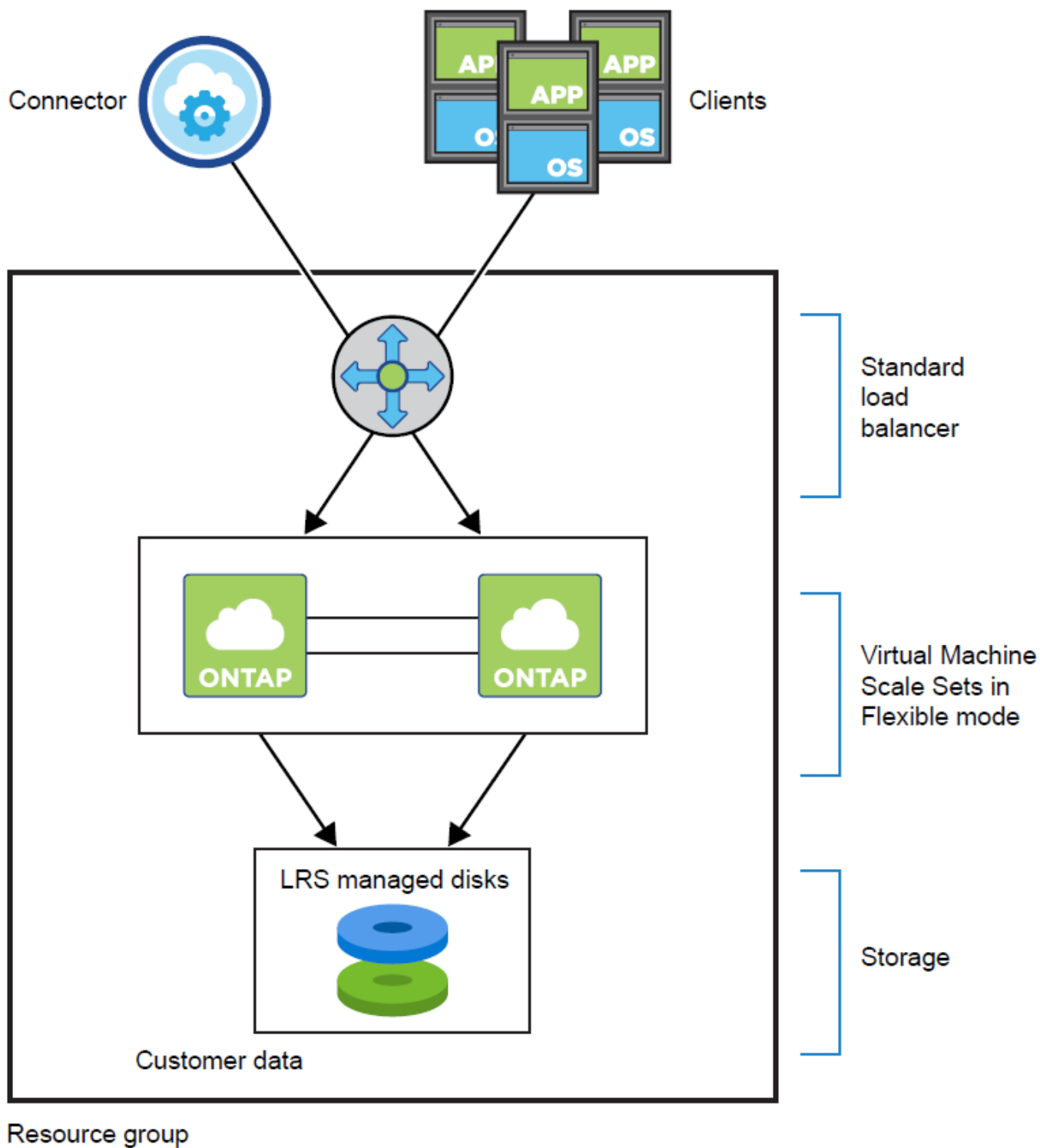
- Uma conta de armazenamento é necessária para o armazenamento de dados em camadas no armazenamento de Blobs do Azure.
- A partir do Cloud Volumes ONTAP 9.7, as contas de armazenamento que o Console cria para pares de HA são contas de armazenamento v2 de uso geral.
- Você pode habilitar uma conexão HTTPS de um par de HA do Cloud Volumes ONTAP 9.7 para contas de armazenamento do Azure ao adicionar um sistema Cloud Volumes ONTAP . Observe que habilitar esta opção pode afetar o desempenho da gravação. Você não pode alterar a configuração depois de criar o sistema.



A partir do Cloud Volumes ONTAP 9.15.0P1, os blobs de páginas do Azure não têm mais suporte para novas implantações de pares de alta disponibilidade. Se você atualmente usa blobs de páginas do Azure em implantações de pares de alta disponibilidade existentes, pode migrar para tipos de instância de VM mais recentes nas VMs das séries Edsv4 e Edsv5. ["Saiba mais sobre as configurações com suporte no Azure"](#) .

Configuração de zona de disponibilidade única de HA com discos gerenciados compartilhados

Uma configuração de zona de disponibilidade única do Cloud Volumes ONTAP HA em execução no disco gerenciado compartilhado inclui os seguintes componentes:



Observe o seguinte sobre os componentes do Azure que o Console implanta para você:

Balancedador de Carga Padrão do Azure

O balanceador de carga gerencia o tráfego de entrada para o par Cloud Volumes ONTAP HA.

VMs em zonas de disponibilidade única

A partir do Cloud Volumes ONTAP 9.15.1, você pode criar e gerenciar máquinas virtuais (VMs) heterogêneas 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 disponibilidade ideal. Para saber mais sobre o modo de orquestração flexível que permite esse recurso, consulte o ["Documentação do](#)

A implantação zonal usa discos gerenciados Premium SSD 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 oferecem suporte a discos gerenciados Premium SSD v2. Para obter informações sobre as regiões suportadas, consulte ["Site do Microsoft Azure: Produtos disponíveis por região"](#) .
- A assinatura é registrada para a Microsoft ["Recurso Microsoft.Compute/VMOrchestratorZonalMultiFD"](#) .

Discos

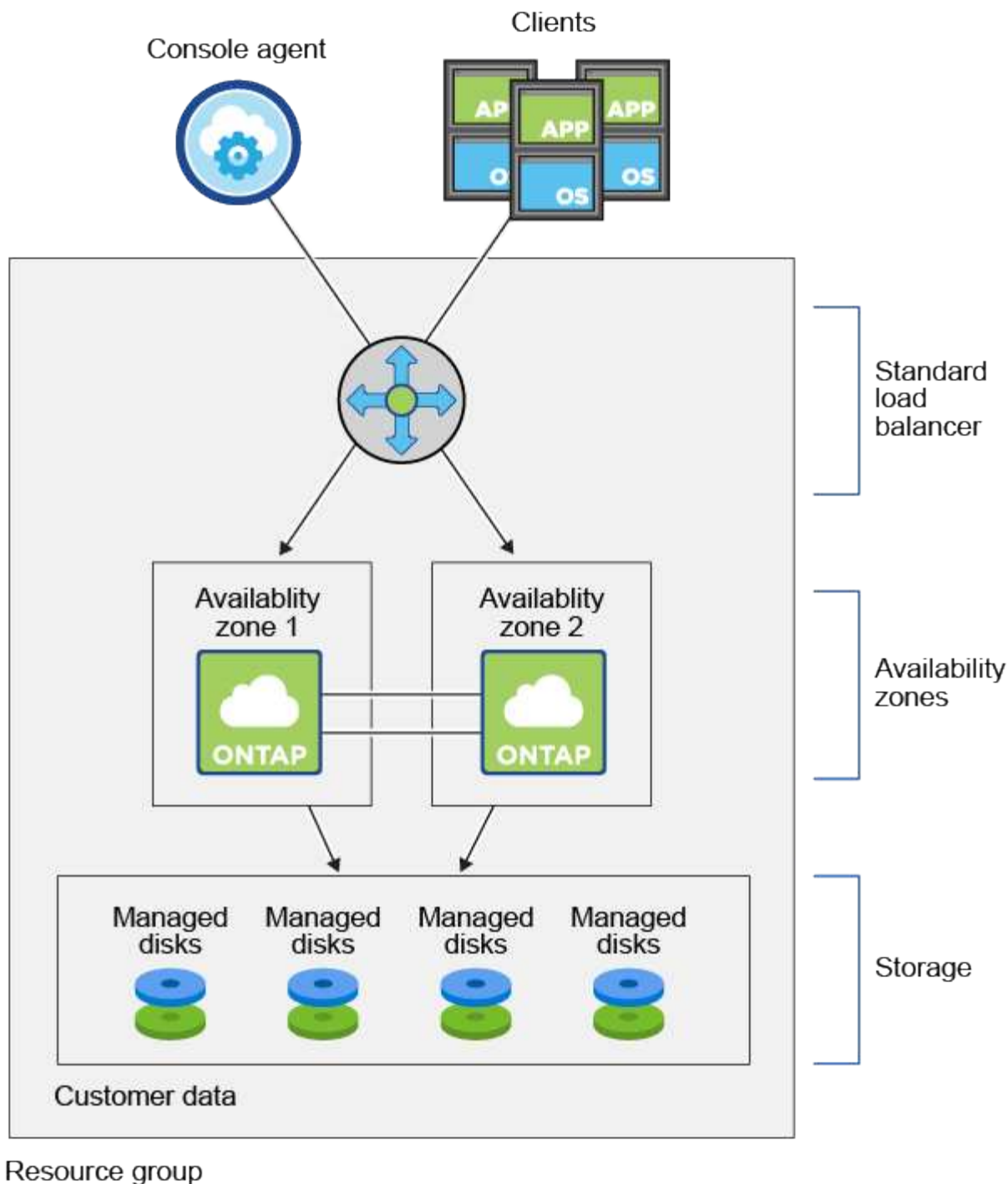
Os dados do cliente residem em discos gerenciados por armazenamento redundante local (LRS). Cada nó tem acesso ao armazenamento do outro nó. Armazenamento adicional também é necessário para ["dados de inicialização, raiz, raiz do parceiro, núcleo e NVRAM"](#) .

Contas de armazenamento

Contas de armazenamento são usadas para implantações baseadas em disco gerenciado para manipular logs de diagnóstico e camadas para armazenamento de blobs.

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 Console implanta para você:

Balancedor de Carga Padrão do Azure

O balanceador de carga gerencia o tráfego de entrada para o par Cloud Volumes ONTAP HA.

Zonas de disponibilidade

A configuração de várias zonas de disponibilidade do HA utiliza um modelo de implantação em que dois nós do 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 dimensionamento de máquinas virtuais no modo de orquestração flexível podem usar zonas de disponibilidade no Azure, consulte o ["Documentação do Microsoft Azure: Criar um conjunto](#)

de dimensionamento de máquina virtual que usa zonas de disponibilidade" .

Discos

Os dados do cliente residem em discos gerenciados de armazenamento redundante de zona (ZRS). Cada nó tem acesso ao armazenamento do outro nó. Armazenamento adicional também é necessário para "dados de inicialização, raiz, raiz do parceiro e núcleo" .

Contas de armazenamento

Contas de armazenamento são usadas para implantações baseadas em disco gerenciado para manipular logs de diagnóstico e camadas para armazenamento de blobs.

RPO e RTO

Uma configuração de HA mantém alta disponibilidade dos seus dados da seguinte maneira:

- O objetivo do ponto de recuperação (RPO) é 0 segundos. Seus dados são transacionalmente consistentes, sem perda de dados.
- O objetivo do tempo de recuperação (RTO) é de 120 segundos. Em caso de interrupção, os dados devem estar disponíveis em 120 segundos ou menos.

Aquisição e devolução de armazenamento

Semelhante a um cluster ONTAP físico, o armazenamento 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 uma *aquisição*. Os mecanismos de failover do caminho de rede garantem que clientes e hosts continuem a se comunicar com o nó sobrevivente. O parceiro *devolve* o armazenamento quando o nó é reativado.

Para configurações de NAS, os endereços IP de dados migram automaticamente entre nós de HA se ocorrerem falhas.

Para iSCSI, o Cloud Volumes ONTAP usa E/S multicaminho (MPIO) e Acesso de Unidade Lógica Assimétrica (ALUA) para gerenciar o failover de caminho entre os caminhos otimizados ativos e não otimizados.



Para obter informações sobre quais configurações específicas de host oferecem suporte a ALUA, consulte o "[Ferramenta de Matriz de Interoperabilidade da NetApp](#)" e o "[Guia de hosts SAN e clientes em nuvem](#)" para o seu sistema operacional host.

A aquisição, a ressincronização e a devolução do armazenamento são todas automáticas por padrão. Nenhuma ação do usuário é necessária.

Configurações de armazenamento

Você pode usar um par HA como uma configuração ativa-ativa, na qual ambos os nós fornecem dados aos clientes, ou como uma configuração ativa-passiva, na qual o nó passivo responde às solicitações de dados somente se tiver assumido o armazenamento do nó ativo.

Saiba mais sobre pares de alta disponibilidade do Cloud Volumes ONTAP no Google Cloud

Uma configuração de alta disponibilidade (HA) do Cloud Volumes ONTAP fornece operações ininterruptas e tolerância a falhas. No Google Cloud, os dados são

espelhados de forma síncrona entre os dois nós.

Componentes HA

As configurações de alta disponibilidade do Cloud Volumes ONTAP no Google Cloud incluem os seguintes componentes:

- Dois nós Cloud Volumes ONTAP cujos dados são espelhados de forma síncrona entre si.
- Uma instância mediadora que fornece um canal de comunicação entre os nós para auxiliar nos processos de aquisição e devolução de armazenamento.
- Uma zona ou três zonas (recomendado).

Se você escolher três zonas, os dois nós e o mediador estarão em zonas separadas do Google Cloud.

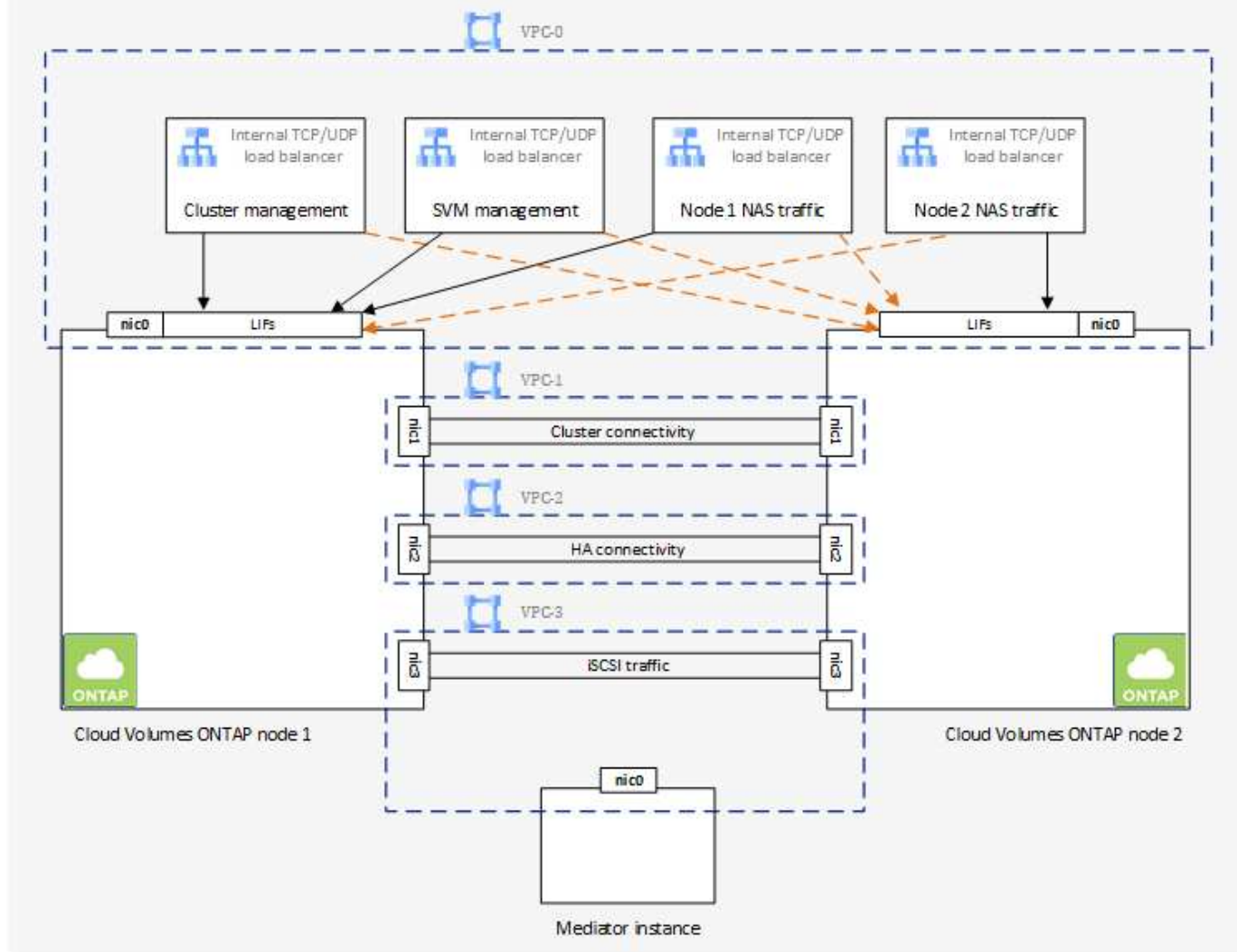
- Quatro Nuvens Privadas Virtuais (VPCs).

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 Cloud Volumes ONTAP HA.

["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 Cloud Volumes ONTAP HA e seus componentes:



Mediador

Aqui estão alguns detalhes importantes sobre a instância do mediador no Google Cloud:

Tipo de instância

e2-micro (uma instância f1-micro foi usada anteriormente)

Discos

Dois discos persistentes padrão de 10 GiB cada

Sistema operacional

Debian 11



Para o Cloud Volumes ONTAP 9.10.0 e anteriores, o Debian 10 foi instalado no mediador.

Atualizações

Quando você atualiza o Cloud Volumes ONTAP, o NetApp Console 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 certificados para o `admin` usuário quando o acesso SSH é solicitado por meio do console do Google Cloud ou da linha de comando do `gcloud`. Você pode especificar `sudo` para obter privilégios de root.

Agentes terceirizados

Agentes de terceiros ou extensões de VM não são suportados na instância do mediador.

Aquisição e devolução de armazenamento

Se um nó cair, o outro nó pode fornecer dados para seu parceiro para fornecer serviço de dados contínuo. Os clientes podem acessar os mesmos dados do nó do parceiro porque os dados foram espelhados de forma síncrona para o parceiro.

Após a reinicialização do nó, o parceiro deve ressincronizar os dados antes de poder retornar o armazenamento. O tempo que leva para ressincronizar os dados depende de quantos dados foram alterados enquanto o nó estava inativo.

A aquisição, a ressincronização e a devolução do armazenamento são todas automáticas por padrão. Nenhuma ação do usuário é necessária.

RPO e RTO

Uma configuração de HA mantém alta disponibilidade dos seus dados da seguinte maneira:

- O objetivo do ponto de recuperação (RPO) é 0 segundos.

Seus dados são transacionalmente consistentes, sem perda de dados.

- O objetivo do 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 dos 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 disponibilidade contínua de dados caso ocorra uma falha em uma zona. Observe que o desempenho de gravação é um pouco menor quando comparado ao 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 espalhado. Esta política garante que uma configuração de HA seja protegida de um único ponto de falha dentro da zona, sem precisar usar zonas separadas para obter isolamento de falhas.

Este modelo de implantação reduz seus custos porque não há cobranças de saída de dados entre zonas.

Como funciona o armazenamento em um par HA

Ao contrário de um cluster ONTAP, o armazenamento em um par Cloud Volumes ONTAP HA no GCP não é

compartilhado entre nós. Em vez disso, os dados são espelhados de forma síncrona entre os nós para que estejam disponíveis em caso de falha.

Alocação de armazenamento

Quando você cria um novo volume e discos adicionais são necessários, o Console aloca o mesmo número de discos para ambos os nós, cria um agregado espelhado e, em seguida, cria o novo volume. Por exemplo, se dois discos forem necessários para o volume, o Console alocará dois discos por nó, para um total de quatro discos.

Configurações de armazenamento

Você pode usar um par de HA como uma configuração ativa-ativa, na qual ambos os nós fornecem dados aos clientes, ou como uma configuração ativa-passiva, na qual o nó passivo responde às solicitações de dados somente se tiver assumido o armazenamento do nó ativo.

Expectativas de desempenho para uma configuração de HA

Uma configuração do Cloud Volumes ONTAP HA replica dados de forma síncrona entre nós, o que consome largura de banda da rede. Como resultado, você pode esperar o seguinte desempenho em comparação com uma configuração de nó único do Cloud Volumes ONTAP :

- Para configurações de HA que fornecem dados de apenas um nó, o desempenho de leitura é comparável ao desempenho de leitura de uma configuração de nó único, enquanto o desempenho de gravação é menor.
- Para configurações de HA que atendem dados de ambos os nós, o desempenho de leitura é maior que o desempenho de leitura de uma configuração de nó único, e o desempenho de gravação é o mesmo ou maior.

Para obter mais detalhes sobre o desempenho do Cloud Volumes ONTAP , consulte "[Desempenho](#)" .

Acesso do cliente ao armazenamento

Os clientes devem acessar os volumes NFS e CIFS usando o endereço IP de dados do nó no qual o volume reside. Se clientes NAS acessarem um volume usando o endereço IP do nó parceiro, o tráfego passará entre ambos os nós, o que reduz o desempenho.



Se você mover um volume entre nós em um par de HA, deverá remontar o volume usando o endereço IP do outro nó. Caso contrário, você poderá ter um desempenho reduzido. Se os clientes oferecerem suporte a referências NFSv4 ou redirecionamento de pasta para CIFS, você poderá habilitar esses recursos nos sistemas Cloud Volumes ONTAP para evitar a remontagem do volume. Para mais detalhes, consulte a documentação do ONTAP .

Você pode localizar o endereço IP correto no Console selecionando o volume e clicando em **Comando de montagem**.

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"](#)
- ["Aprenda como começar no GCP"](#)

Operações indisponíveis quando um nó no par Cloud Volumes ONTAP HA está offline

Quando um nó em um par HA não está disponível, o outro nó fornece dados para seu parceiro para fornecer serviço de dados contínuo. Isso é chamado de *aquisição de*

armazenamento. Várias ações ficarão indisponíveis até que a devolução no armazenamento seja concluída.



Quando um nó em um par de HA não está disponível, o estado do sistema no NetApp Console é *Degradado*.

As seguintes ações não estão disponíveis na aquisição de armazenamento:

- Registro de suporte
- Alterações de licença
- Alterações no tipo de instância ou VM
- Alterações na velocidade de gravação
- Configuração CIFS
- Alterando o local dos backups de configuração
- Definindo a senha do cluster
- Gerenciamento de discos e agregados (alocação avançada)

Essas ações estarão disponíveis novamente após a conclusão da devolução do armazenamento e o estado do sistema voltar ao normal.

Saiba mais sobre a criptografia de dados Cloud Volumes ONTAP e a proteção contra ransomware

O Cloud Volumes ONTAP oferece suporte à criptografia de dados e 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)
- Serviço de gerenciamento de chaves da AWS
- Criptografia do Serviço de Armazenamento do Azure
- Criptografia padrão do Google Cloud Platform

Você pode usar soluções de criptografia da NetApp com criptografia nativa do seu provedor de nuvem, que criptografa dados no nível do hipervisor. Isso forneceria criptografia dupla, o que pode ser desejado para dados muito confidenciais. Quando os dados criptografados são acessados, eles são descriptografados duas vezes: uma vez no nível do hipervisor (usando chaves do provedor de nuvem) e novamente usando soluções de criptografia da NetApp (usando chaves de um gerenciador de chaves externo).

Soluções de criptografia NetApp (NVE e NAE)

O Cloud Volumes ONTAP oferece suporte ["Criptografia de volume NetApp \(NVE\) e criptografia agregada NetApp \(NAE\)"](#). NVE e NAE são soluções baseadas em software que permitem a criptografia de dados em repouso de volumes compatível com (FIPS) 140-2. Tanto o NVE quanto o NAE usam criptografia AES de 256 bits.

- O NVE criptografa dados em repouso, um volume por vez. Cada volume de dados tem sua própria chave de criptografia exclusiva.
- NAE é uma extensão do NVE: ele criptografa dados para cada volume, e os volumes compartilham uma chave no agregado. O NAE também permite que blocos comuns em todos os volumes no agregado sejam desduplicados.

O Cloud Volumes ONTAP oferece suporte a NVE e NAE com serviços externos de gerenciamento de chaves (EKMs) fornecidos pela AWS, Azure e Google Cloud, incluindo soluções de terceiros, como Fortanix. Ao contrário do ONTAP, para o Cloud Volumes ONTAP, as chaves de criptografia são geradas no lado do provedor de nuvem, não no ONTAP.

O Cloud Volumes ONTAP usa os serviços padrão do Key Management Interoperability Protocol (KMIP) que o ONTAP utiliza. Para obter mais informações sobre os serviços suportados, consulte o ["Ferramenta de Matriz de Interoperabilidade"](#).

Se você usar o NVE, terá a opção de usar o cofre de chaves do seu provedor de nuvem para proteger as chaves de criptografia ONTAP :

- Serviço de gerenciamento de chaves da AWS (KMS)
- Cofre de Chaves do Azure (AKV)
- Serviço de gerenciamento de chaves do Google Cloud

Os novos agregados têm o NetApp Aggregate Encryption (NAE) habilitado por padrão após você configurar um gerenciador de chaves externo. Novos volumes que não fazem parte de um agregado NAE têm o NVE habilitado por padrão (por exemplo, se você tiver agregados existentes que foram criados antes de configurar um gerenciador de chaves externo).

A única etapa necessária é configurar um gerenciador de chaves compatível. Para obter instruções de configuração, consulte ["Criptografe volumes com soluções de criptografia NetApp"](#).

Serviço de gerenciamento de chaves da AWS

Ao iniciar um sistema Cloud Volumes ONTAP na AWS, você pode habilitar a criptografia de dados usando o ["Serviço de gerenciamento de chaves da AWS \(KMS\)"](#). O NetApp Console 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, deverá garantir que o AWS KMS esteja configurado corretamente. Para obter informações, consulte ["Configurando o AWS KMS"](#).

Criptografia do Serviço de Armazenamento do Azure

Os dados são criptografados automaticamente no Cloud Volumes ONTAP no Azure usando ["Criptografia do Serviço de Armazenamento do Azure"](#) com uma chave gerenciada pela Microsoft.

Você pode usar suas próprias chaves de criptografia, se preferir. ["Aprenda a 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 habilitado por padrão para Cloud Volumes ONTAP. Nenhuma configuração é necessária.

Embora o Google Cloud Storage sempre criptografe seus dados antes de gravá-los no disco, você pode usar as APIs do Console para criar um sistema Cloud Volumes ONTAP que usa *chaves de criptografia gerenciadas pelo cliente*. Essas são chaves que você gera e gerencia no GCP usando o Cloud Key Management Service. "[Saber mais](#)".

Verificação de vírus ONTAP

Você pode usar a funcionalidade antivírus integrada em sistemas ONTAP para proteger dados de serem comprometidos por vírus ou outros códigos maliciosos.

A verificação de vírus ONTAP, chamada *Vscan*, combina o melhor software antivírus de terceiros com recursos ONTAP que oferecem a flexibilidade necessária para controlar quais arquivos serão verificados e quando.

Para obter informações sobre os fornecedores, software e versões suportadas pelo Vscan, consulte o "[Matriz de interoperabilidade da NetApp](#)".

Para obter informações sobre como configurar e gerenciar a funcionalidade antivírus em sistemas ONTAP, consulte o "[Guia de configuração do antivírus ONTAP 9](#)".

Proteção contra ransomware

Ataques de ransomware podem custar tempo, recursos e reputação a uma empresa. O Console permite que você implemente a solução NetApp para ransomware, que fornece ferramentas eficazes para visibilidade, detecção e correção.

- O Console identifica volumes que não são protegidos por uma política de Snapshot e permite que você ative a política de Snapshot padrão nesses volumes.

As cópias de instantâneos são somente leitura, o que evita a corrupção por 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 Console também permite que você bloqueie extensões de arquivo comuns de ransomware 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

"Aprenda a implementar a solução NetApp para ransomware" .

Saiba mais sobre o monitoramento de desempenho para cargas de trabalho do Cloud Volumes ONTAP

Você pode revisar os resultados de desempenho para ajudar a decidir quais cargas de trabalho são apropriadas para o Cloud Volumes ONTAP.

Relatórios técnicos de desempenho

- Cloud Volumes ONTAP para AWS

["Relatório Técnico NetApp 4383: Caracterização de Desempenho de Cloud Volumes ONTAP na Amazon Web Services 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 aplicativos"](#)

- Cloud Volumes ONTAP para Google Cloud

["Relatório técnico da NetApp 4816: Caracterização de desempenho do Cloud Volumes ONTAP para Google Cloud"](#)

Desempenho da CPU

Os nós do Cloud Volumes ONTAP aparecem como altamente utilizados (mais de 90%) nas ferramentas de monitoramento do seu provedor de nuvem. Isso ocorre porque o ONTAP reserva todas as vCPUs apresentadas à máquina virtual para que estejam disponíveis quando necessário.

Para obter informações, consulte o ["Artigo da base de conhecimento da NetApp sobre como monitorar a utilização da CPU do ONTAP usando a CLI"](#)

Gerenciamento de licenças para BYOL baseado em nó

Cada sistema Cloud Volumes ONTAP que tem uma licença "traga sua própria licença" (BYOL) baseada em nó deve ter uma licença de sistema instalada com uma assinatura ativa. O NetApp Console simplifica o processo gerenciando licenças para você e exibindo um aviso antes que elas expirem.



Uma licença baseada em nó é a licença da geração anterior para o Cloud Volumes ONTAP. Uma licença baseada em nó pode ser adquirida da NetApp (BYOL) e está disponível para renovações de licença apenas em casos específicos.

["Saiba mais sobre as opções de licenciamento do Cloud Volumes ONTAP"](#) .

["Saiba mais sobre como gerenciar licenças baseadas em nós"](#) .

Licenças do sistema BYOL

Licenças baseadas em nós podem ser adquiridas da NetApp. O número de licenças que você pode adquirir para um único sistema de nó ou par de HA é ilimitado.



A NetApp restringiu a compra, extensão e renovação de licenças BYOL. Para obter mais informações, consulte ["Disponibilidade restrita de licenciamento BYOL para Cloud Volumes ONTAP"](#) .

Uma licença baseada em nó fornece até 368 TiB de capacidade para um único nó ou par de HA. Você pode ter adquirido várias licenças para um sistema Cloud Volumes ONTAP BYOL para alocar mais de 368 TiB de capacidade. Por exemplo, você pode ter duas licenças para alocar até 736 TiB de capacidade para o Cloud Volumes ONTAP. Ou você pode ter quatro licenças para obter até 1,4 PiB.

Esteja ciente de que os limites do disco podem impedir que você atinja o limite de capacidade usando apenas discos. Você pode ir além do limite do disco por ["hierarquização de dados inativos para armazenamento de objetos"](#) . Para obter informações sobre limites de disco, consulte ["limites de armazenamento nas notas de versão do Cloud Volumes ONTAP"](#) .

Gerenciamento de licenças para um novo sistema

Ao criar um sistema BYOL baseado em nó, o Console solicita o número de série da sua licença e sua conta do Site de Suporte da NetApp . O Console usa a conta para baixar o arquivo de licença do NetApp e instalá-lo no sistema Cloud Volumes ONTAP .

["Aprenda como adicionar contas do site de suporte da NetApp ao console"](#) .

Se o Console não puder acessar o arquivo de licença por meio de uma conexão segura com a Internet, você poderá ["obtenha o arquivo você mesmo e então carregue-o manualmente no Console"](#) .

Expiração da licença

O Console exibe um aviso 30 dias antes da expiração de uma licença baseada em nó e novamente quando a licença expira. A imagem a seguir mostra um aviso de expiração de 30 dias que aparece na interface do usuário:



Você pode selecionar o sistema para revisar a mensagem.

O Console inclui um aviso de expiração de licença no relatório do Cloud Volumes ONTAP que é enviado a você por e-mail, se você for uma organização ou administrador de conta e tiver habilitado a opção. O relatório enviado por e-mail inclui o aviso de expiração da licença a cada 2 semanas.

Se você não renovar a licença a tempo, o sistema Cloud Volumes ONTAP será desligado. Se você reiniciá-lo, ele será desligado novamente.

Renovação de licença

Se você renovar uma assinatura BYOL baseada em nó entrando em contato com um representante da NetApp, o Console obterá automaticamente a nova licença da NetApp e a instalará no sistema Cloud Volumes ONTAP.

Se o Console não puder acessar o arquivo de licença por meio de uma conexão segura com a Internet, você poderá ["obtenha o arquivo você mesmo e então carregue-o manualmente no Console"](#).

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 usar a licença com um novo sistema BYOL em uma VPC/VNet ou provedor de nuvem diferente. Observe que somente números de série *independentes de nuvem* funcionam em qualquer provedor de nuvem. Os números de série independentes de nuvem começam com o prefixo 908xxxx.

É importante observar que sua licença BYOL está vinculada à sua empresa e a um conjunto específico de credenciais do site de suporte da NetApp.

Aprenda como o AutoSupport e o Digital Advisor são usados no Cloud Volumes ONTAP

O componente AutoSupport do ONTAP coleta telemetria e a envia para análise. O Active IQ Digital Advisor (também conhecido como Digital Advisor) analisa os dados do AutoSupport e fornece atendimento proativo e otimização. Usando inteligência artificial, o Digital Advisor pode identificar problemas potenciais e ajudar você a resolvê-los antes que eles afetem seus negócios.

O Digital Advisor permite que você otimize sua infraestrutura de dados em sua nuvem híbrida global, fornecendo análises preditivas acionáveis e suporte proativo por meio de um portal baseado em nuvem e aplicativo móvel. Insights e recomendações baseados em dados do Digital Advisor estão disponíveis para todos os clientes da NetApp com um contrato ativo do SupportEdge (os recursos variam de acordo com o

produto e o nível de suporte).

Aqui estão algumas coisas que você pode fazer com o Digital Advisor:

- Planeje atualizações.

O Digital Advisor identifica problemas no seu ambiente que podem ser resolvidos com a atualização para uma versão mais recente do ONTAP , e o componente Upgrade Advisor ajuda você a planejar uma atualização bem-sucedida.

- Visualizar o bem-estar do sistema.

O painel do seu Digital Advisor relata quaisquer problemas com bem-estar e ajuda você a corrigi-los. Monitore a capacidade do sistema para garantir que você nunca fique sem espaço de armazenamento. Veja casos de suporte para seu sistema.

- Gerenciar desempenho.

O Digital Advisor mostra o desempenho do sistema por um período mais longo do que você pode ver no ONTAP System Manager. Identifique problemas de configuração e sistema que estão afetando seu desempenho. Maximize a eficiência. Visualize métricas de eficiência de armazenamento e identifique maneiras de armazenar mais dados em menos espaço.

- Ver inventário e configuração.

O Digital Advisor exibe informações completas de inventário e configuração de software e hardware. Veja quando os contratos de serviço estão expirando e renove-os para garantir que você continue com suporte.

Links relacionados

- ["Documentação da NetApp : Digital Advisor"](#)
- ["Lançamento do Digital Advisor"](#)
- ["Serviços SupportEdge"](#)

Configurações padrão suportadas para Cloud Volumes ONTAP

Entender como o Cloud Volumes ONTAP é configurado por padrão pode ajudar você 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 padrão

- O NetApp Console cria uma VM de armazenamento de serviço de dados ao implantar o Cloud Volumes ONTAP. Algumas configurações oferecem suporte a VMs de armazenamento adicionais. ["Saiba mais sobre o gerenciamento de VMs de armazenamento"](#) .

A partir da versão 3.9.5, o relatório de espaço lógico é habilitado na VM de armazenamento inicial. Quando o espaço é relatado logicamente, o ONTAP relata o espaço do volume de forma que todo o espaço físico economizado pelos recursos de eficiência de armazenamento também seja relatado como usado. Para obter informações sobre recursos de eficiência de armazenamento em linha, consulte o artigo

da base de conhecimento "[KB: Quais recursos de eficiência de armazenamento em linha são suportados pelo CVO?](#)"

- O Console instala automaticamente as seguintes licenças de recursos ONTAP no Cloud Volumes ONTAP:
 - CIFS
 - FlexCache
 - FlexClone
 - iSCSI
 - Gerenciamento de chaves de criptografia multilocatário (MTEKM), começando com o Cloud Volumes ONTAP 9.12.1 GA
 - NetApp Volume Encryption (somente para sistemas BYOL (traga sua própria licença) ou sistemas PAYGO (pague conforme o uso) registrados)
 - 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 cluster
 - Um LIF interaglomerado
 - Um LIF de gerenciamento de SVM em sistemas HA no Azure
 - Um LIF de gerenciamento de SVM em sistemas HA no Google Cloud
 - Um 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 intercluster.
- Um LIF de dados iSCSI
 - Um LIF de dados CIFS e NFS



O failover do LIF é desabilitado por padrão para o Cloud Volumes ONTAP devido aos requisitos do provedor de nuvem. Migrar um LIF para uma porta diferente quebra 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 agente do Console usando HTTP.

Os backups podem ser acessados em `http://ipaddress/occm/offboxconfig/`, onde *ipaddress* é o endereço IP do host do agente do Console.

Você pode usar os backups para reconfigurar seu sistema Cloud Volumes ONTAP . Para obter mais informações sobre backups de configuração, consulte o "[Documentação do ONTAP](#)" .

- O Console define alguns atributos de volume de forma diferente de outras ferramentas de gerenciamento (ONTAP System Manager ou ONTAP CLI, por exemplo).

A tabela a seguir lista os atributos de volume definidos de forma diferente dos padrões:

Atributo	Valor que o Console configura
Modo de dimensionamento automático	crescer
Tamanho automático máximo	1.000 por cento  O administrador da organização ou da conta pode modificar esse valor na 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, consulte ["Página de manual do ONTAP volume create"](#).

Discos internos para dados do sistema

Além do armazenamento para dados do usuário, o Console também adquire armazenamento em nuvem para dados do sistema.

AWS

- Três discos por nó para dados de inicialização, raiz e núcleo:
 - Disco io1 de 47 GiB para dados de inicialização
 - Disco gp3 de 140 GiB para dados raiz
 - Disco gp2 de 540 GiB para dados principais
- Para pares HA:
 - Dois volumes EBS st1 para a instância do mediador, um de aproximadamente 8 GiB como disco raiz e um de 4 GiB como disco de dados
 - Um disco gp3 de 140 GiB 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 do EBS para cada disco de inicialização e disco raiz



Os instantâneos são criados automaticamente na reinicialização.

- Quando você habilita a criptografia de dados na AWS usando o Key Management Service (KMS), os discos de inicialização e raiz do Cloud Volumes ONTAP também são criptografados. Isso inclui o disco de

inicialização para a instância do mediador em um par HA. Os discos são criptografados usando a CMK que você seleciona ao adicionar um sistema Cloud Volumes ONTAP .



Na AWS, a NVRAM está no disco de inicialização.

Azure (nó único)

- Três discos SSD Premium:
 - Um disco de 10 GiB para dados de inicialização
 - Um disco de 140 GiB para dados raiz
 - Um disco de 512 GiB para NVRAM

Se a máquina virtual que você escolheu para o Cloud Volumes ONTAP for compatível com Ultra SSDs, o sistema usará um Ultra SSD de 32 GiB para NVRAM, em vez de um SSD Premium.

- Um disco HDD padrão de 1024 GiB para economizar núcleos
- Um instantâneo 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 Premium SSD v2 Managed Disk como discos de dados, o sistema usará um Premium SSD v2 Managed Disk de 32 GiB para NVRAM e outro como disco raiz.

Azure (par HA)

Pares HA 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 instantâneo do Azure para cada disco de inicialização e disco raiz



Os instantâneos são criados automaticamente na 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 instantâneo do Azure para cada disco de inicialização e disco raiz



Os instantâneos são criados automaticamente na 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 SSD Premium compartilhados gerenciados 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 gerenciados de 512 GiB para NVRAM (um por nó)

Se sua máquina virtual oferecer suporte a discos gerenciados Premium SSD v2 como discos de dados, ela usará discos gerenciados Premium SSD v2 de 32 GiB para NVRAM e discos gerenciados compartilhados Premium SSD v2 de 512 GiB para o volume raiz.

Você pode implantar pares de HA em uma única zona de disponibilidade e usar discos gerenciados Premium SSD v2 quando as seguintes condições forem atendidas:

- A versão do Cloud Volumes ONTAP é 9.15.1 ou posterior.
- A região e a zona selecionadas oferecem suporte a discos gerenciados Premium SSD v2. Para obter informações sobre as regiões suportadas, consulte ["Site do Microsoft Azure: Produtos disponíveis por região"](#).
- A assinatura é registrada 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 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 root



Os instantâneos são criados automaticamente na reinicialização.

- Os discos de inicialização e raiz são criptografados por padrão.

Google Cloud (par HA)

- Dois discos persistentes SSD de 10 GiB para dados de inicialização
- Quatro discos persistentes SSD de 64 GiB para dados 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 do mediador
- Um disco persistente padrão de 10 GiB para dados de inicialização do mediador
- Snapshots para dados de inicialização e root



Os instantâneos são criados automaticamente na reinicialização.

- Os discos de inicialização e raiz são criptografados por padrão.

Onde os discos residem

Layout de armazenamento:

- Os dados de inicialização residem em um disco conectado à instância ou máquina virtual.

Este disco, que contém a imagem de inicialização, não está disponível para o Cloud Volumes ONTAP.

- Os dados raiz, que contêm a configuração do sistema e os logs, residem em aggr0.
- O volume raiz da máquina virtual de armazenamento (SVM) reside em aggr1.
- Os volumes de dados também residem em aggr1.

Conhecimento e suporte

Registre-se para obter suporte

O registro de suporte é necessário para receber suporte técnico específico para o BlueXP e suas soluções e serviços de armazenamento. O registro de suporte também é necessário para habilitar fluxos de trabalho importantes para sistemas Cloud Volumes ONTAP .

O registro para suporte não habilita o suporte da NetApp para um serviço de arquivo do provedor de nuvem. Para obter suporte técnico relacionado a um serviço de arquivo do provedor de nuvem, sua infraestrutura ou qualquer solução que use o serviço, consulte "Obter ajuda" na documentação do BlueXP para esse produto.

- ["Amazon FSx para ONTAP"](#)
- ["Azure NetApp Files"](#)
- ["Google Cloud NetApp Volumes"](#)

Visão geral do registro de suporte

Existem duas formas de registro para ativar o direito ao suporte:

- Registrando o número de série da sua conta BlueXP (seu número de série 960xxxxxxxxx de 20 dígitos localizado na página Recursos de suporte no BlueXP).

Isso serve como seu único ID de assinatura de suporte para qualquer serviço dentro do BlueXP. Cada assinatura de suporte em nível de conta BlueXP deve ser registrada.

- Registrando os números de série do Cloud Volumes ONTAP associados a uma assinatura no marketplace do seu provedor de nuvem (são números de série 909201xxxxxxxx de 20 dígitos).

Esses números de série são comumente chamados de *números de série PAYGO* e são gerados pelo BlueXP no momento da implantação do Cloud Volumes ONTAP .

Registrar ambos os tipos de números de série habilita recursos como abertura de tickets de suporte e geração automática de casos. O registro é concluído adicionando contas do NetApp Support Site (NSS) ao BlueXP , conforme descrito abaixo.

Registre o BlueXP para suporte da NetApp

Para se registrar para obter suporte e ativar o direito ao suporte, um usuário na sua organização BlueXP (ou conta) deve associar uma conta do Site de Suporte da NetApp ao seu login BlueXP . A maneira como você se registra para o suporte da NetApp depende se você já tem uma conta no NetApp Support Site (NSS).

Cliente existente com uma conta NSS

Se você for um cliente da NetApp com uma conta NSS, basta se registrar para obter suporte pelo 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 NetApp Support Site (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 BlueXP está registrada para suporte.



Observe que outros usuários do BlueXP não verão o 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 BlueXP não esteja registrada para suporte. Desde que um usuário na organização tenha seguido essas etapas, sua organização foi registrada.

Cliente existente, mas sem conta NSS

Se você já é cliente da NetApp com licenças e números de série, mas *nenhuma* conta NSS, precisa criar uma conta NSS e associá-la ao seu login do BlueXP.

Passos

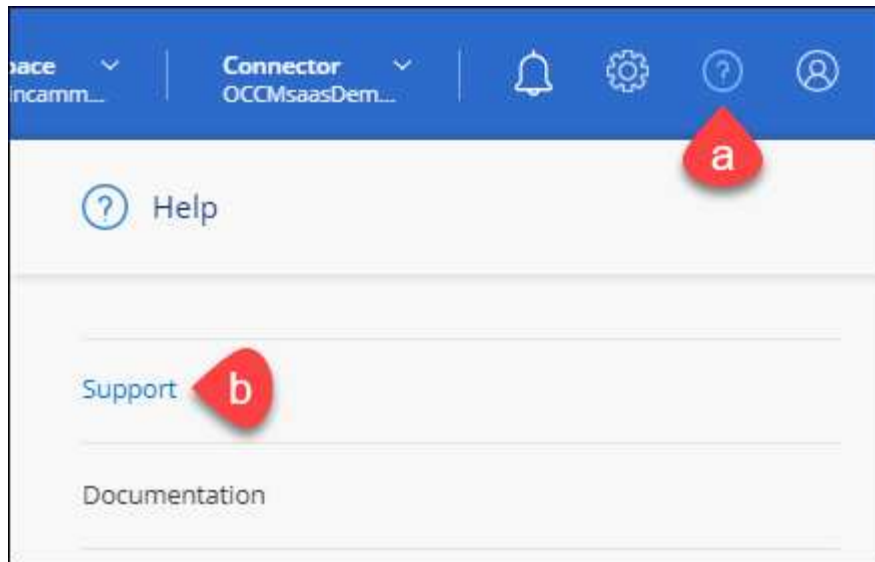
1. Crie uma conta no site de suporte da NetApp preenchendo o ["Formulário de registro de usuário do site de suporte da NetApp"](#)
 - a. Certifique-se de selecionar o Nível de usuário apropriado, que normalmente é * Cliente/Usuário final da NetApp *.
 - b. Certifique-se de copiar o número de série da conta BlueXP (960xxxx) usado acima para o campo de número de série. Isso acelerará o processamento da conta.
2. Associe sua nova conta NSS ao seu login BlueXP concluindo as etapas abaixo [Cliente existente com uma conta NSS](#).

Novidade na NetApp

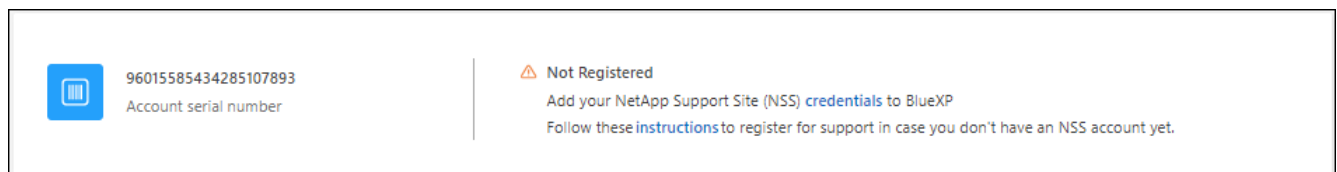
Se você é novo na NetApp e não tem uma conta NSS, siga cada etapa abaixo.

Passos

1. No canto superior direito do console BlueXP, selecione o ícone Ajuda e selecione **Suporte**.



2. Localize o número de série do seu ID de conta na página de Registro de Suporte.



3. Navegar para "[Site de registro de suporte da NetApp](#)" e selecione *Não sou um cliente registrado da NetApp*.
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 da etapa 2 acima, conclua a verificação de segurança e confirme que você leu a Política Global de Privacidade de Dados da NetApp.

Um e-mail é enviado imediatamente para a caixa de correio fornecida para finalizar esta transação segura. Não deixe de verificar sua caixa de spam caso o e-mail de validação não chegue em alguns minutos.

7. Confirme a ação no e-mail.

A confirmação envia sua solicitação à NetApp e recomenda que você crie uma conta no site de suporte da NetApp.

8. Crie uma conta no site de suporte da NetApp preenchendo o "[Formulário de registro de usuário do site de suporte da NetApp](#)"
 - a. Certifique-se de selecionar o Nível de usuário apropriado, que normalmente é * Cliente/Usuário final da NetApp*.
 - b. Certifique-se de copiar o número de série da conta (960xxxx) usado acima para o campo de número de série. Isso acelerará o processamento.

Depois que você terminar

A NetApp entrará em contato com você durante esse processo. Este é um exercício de integração único para novos usuários.

Depois de ter sua conta no site de suporte da NetApp , associe a conta ao seu login BlueXP concluindo as etapas em [Cliente existente com uma conta NSS](#) .

Credenciais associadas do NSS para suporte do Cloud Volumes ONTAP

A associação das credenciais do NetApp Support Site à sua organização BlueXP é necessária para habilitar os seguintes fluxos de trabalho principais para o Cloud Volumes ONTAP:

- Registrando sistemas Cloud Volumes ONTAP de pagamento conforme o uso para suporte

É necessário fornecer sua conta NSS para ativar o suporte para seu sistema e obter acesso aos recursos de suporte técnico da NetApp .

- Implantando o Cloud Volumes ONTAP quando você traz sua própria licença (BYOL)

É necessário fornecer sua conta NSS para que o BlueXP possa carregar sua chave de licença e habilitar a assinatura para o período que você adquiriu. Isso inclui atualizações automáticas para renovações de prazo.

- Atualizando o software Cloud Volumes ONTAP para a versão mais recente

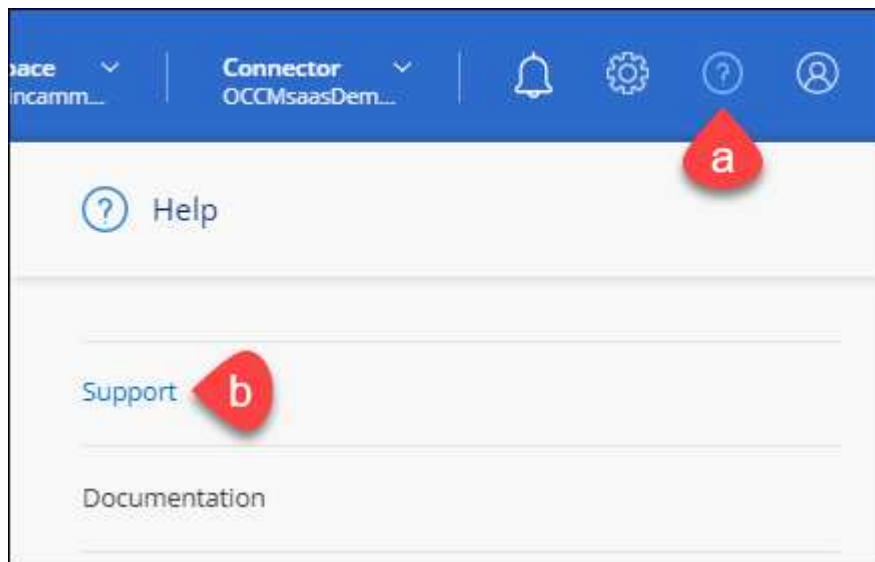
Associar credenciais do NSS à sua organização BlueXP é diferente da conta do NSS associada a um login de usuário do BlueXP .

Essas credenciais NSS estão associadas ao seu ID de organização BlueXP específico. Usuários que pertencem à organização BlueXP podem acessar essas credenciais em **Suporte > Gerenciamento NSS**.

- Se você tiver uma conta de nível de cliente, poderá adicionar uma ou mais contas NSS.
- Se você tiver uma conta de parceiro ou revendedor, poderá adicionar uma ou mais contas NSS, mas elas não poderão ser adicionadas junto com contas de nível de cliente.

Passos

1. No canto superior direito do console BlueXP , selecione o ícone Ajuda e selecione **Suporte**.



2. Selecione **Gerenciamento NSS > Adicionar conta NSS**.
3. Quando solicitado, selecione **Continuar** para ser redirecionado para uma página de login da Microsoft.

A 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 realizar o processo de autenticação.

Essas ações permitem que o BlueXP use sua conta NSS para coisas como downloads de licenças, verificação de atualização de software e registros de suporte futuros.

Observe o seguinte:

- A conta NSS deve ser uma conta de nível de cliente (não uma conta de convidado ou temporária). Você pode ter várias contas NSS em nível de cliente.
- Só pode haver uma conta NSS se essa conta for uma conta de nível de parceiro. Se você tentar adicionar contas NSS em nível de cliente e existir uma conta em nível de parceiro, você receberá a seguinte mensagem de erro:

"O tipo de cliente NSS não é permitido para esta conta, pois já existem usuários NSS de tipos diferentes."

O mesmo é verdadeiro se você tiver contas NSS pré-existentes em nível de cliente e tentar adicionar uma conta em nível de 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 seu e-mail. Na página **NSS Management**, você pode exibir seu e-mail do **...** menu.

- Se você precisar atualizar seus tokens de credenciais de login, também há uma opção **Atualizar credenciais** no **...** menu.

Usar esta opção solicitará que você faça login novamente. Observe que o token para essas contas expira após 90 dias. Uma notificação será publicada para alertá-lo sobre isso.

Obter ajuda

A NetApp oferece suporte para o BlueXP e seus serviços de nuvem de diversas maneiras. Oferecemos amplas opções gratuitas de autossuporte 24 horas por dia, 7 dias por semana, como artigos da base de conhecimento (KB) e um fórum da comunidade. Seu cadastro no suporte inclui suporte técnico remoto por meio de tickets online.

Obtenha suporte para um serviço de arquivo de provedor de nuvem

Para obter suporte técnico relacionado a um serviço de arquivo do provedor de nuvem, sua infraestrutura ou qualquer solução que use o serviço, consulte "Obter ajuda" na documentação do BlueXP para esse produto.

- ["Amazon FSx para ONTAP"](#)
- ["Azure NetApp Files"](#)
- ["Google Cloud NetApp Volumes"](#)

Para receber suporte técnico específico para o BlueXP e suas soluções e serviços de armazenamento, use as opções de suporte descritas abaixo.

Use opções de autoapoio

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 acompanhar discussões em andamento ou criar novas.

Crie um caso com o suporte da NetApp

Além das opções de autossuporte acima, você pode trabalhar com um especialista em suporte da NetApp para resolver quaisquer problemas após ativar o suporte.

Antes de começar

- Para usar o recurso **Criar um caso**, você deve primeiro associar suas credenciais do site de suporte da NetApp ao seu login do BlueXP . ["Aprenda a gerenciar credenciais associadas ao seu login BlueXP"](#) .
- Se você estiver abrindo um caso para um sistema ONTAP que tenha um número de série, sua conta NSS deverá 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 por telefone. Você será direcionado para uma página no netapp.com que lista os números de telefone para os quais você pode ligar.
 - b. Selecione **Criar um caso** para abrir um tíquete com um especialista de 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 **On-Prem** e, em seguida, o ambiente de trabalho associado.

A lista de ambientes de trabalho está dentro do escopo da organização BlueXP (ou conta), projeto (ou espaço de trabalho) e Conector que você selecionou no banner superior do serviço.
 - **Prioridade do caso**: escolha a prioridade do 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 quiser informar outra

pessoa sobre esse problema.

- **Anexo (Opcional):** Carregue até cinco anexos, um de cada vez.

Os anexos são limitados a 25 MB por arquivo. As seguintes extensões de arquivo são suportadas: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.

ntapitdemo 

NetApp Support Site Account

Service

Select ▼

Working Enviroment

Select ▼

Case Priority 

Low - General guidance ▼

Issue Description

Provide detailed description of problem, applicable error messages and troubleshooting steps taken.

Additional Email Addresses (Optional) 

Type here

Attachment (Optional)

No files selected

 Upload 

Depois que você terminar

Um pop-up aparecerá com o número do seu caso de suporte. Um especialista em suporte da NetApp analisará seu caso e entrará em contato com você em breve.

Para obter um histórico dos seus casos de suporte, você pode selecionar **Configurações > Linha do tempo** e procurar por ações chamadas "criar caso de suporte". Um botão na extrema 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 registrada à qual ela está associada não são a mesma empresa registrada para o número de série da conta BlueXP (por exemplo, 960xxxx) ou o número de

série do ambiente de trabalho. Você pode buscar assistência usando uma das seguintes opções:

- Use o chat do produto
- Envie um caso não técnico em <https://mysupport.netapp.com/site/help>

Gerencie seus casos de suporte (visualização)

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 em versões futuras. Envie-nos seu feedback usando o chat do produto.

Observe o seguinte:

- O painel de gerenciamento de casos na parte superior da página oferece duas visualizações:
 - A visualização à esquerda mostra o total de casos abertos nos últimos 3 meses pela conta NSS do usuário que você forneceu.
 - A visualização à direita mostra o total de casos abertos nos últimos 3 meses no nível da sua empresa com base na sua conta de usuário NSS.

Os resultados na tabela refletem os casos relacionados à exibição que você selecionou.

- Você pode adicionar ou remover colunas de interesse e filtrar o conteúdo de colunas como Prioridade e Status. Outras colunas fornecem apenas recursos de classificação.

Veja as etapas abaixo para mais detalhes.

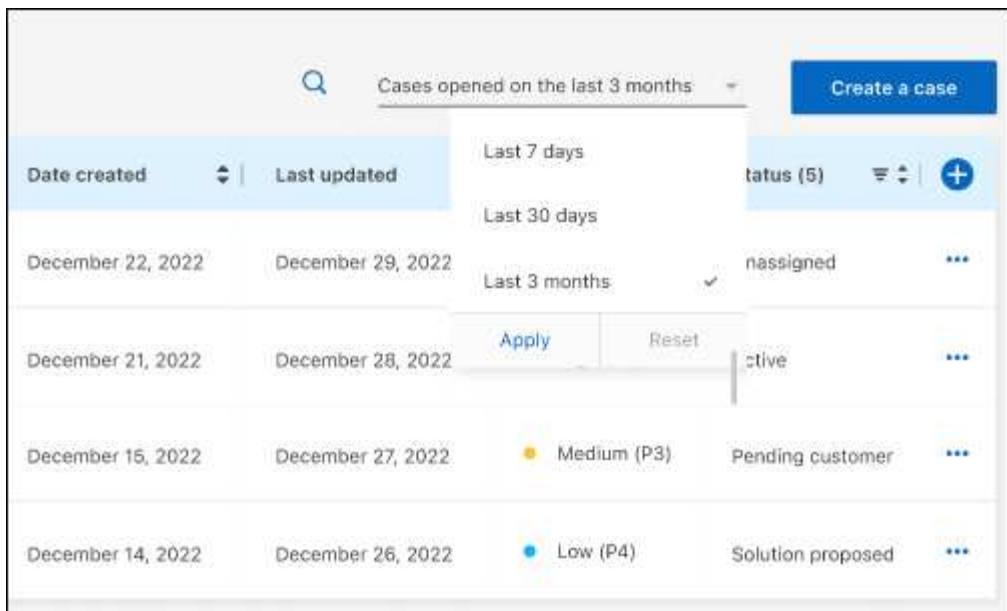
- Em cada caso, oferecemos a possibilidade de atualizar notas do caso ou fechar um caso que ainda não esteja no status Fechado ou Pendente Fechado.

Passos

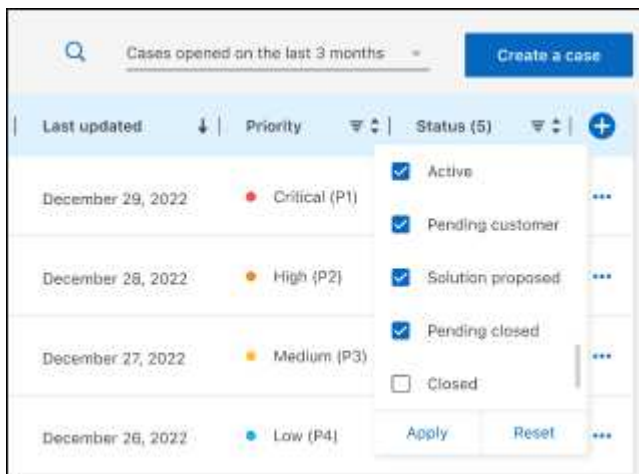
1. No BlueXP, selecione **Ajuda > Suporte**.
2. Selecione **Gerenciamento de casos** e, se solicitado, adicione sua conta NSS ao BlueXP.

A página **Gerenciamento de casos** mostra casos abertos relacionados à conta NSS associada à sua conta de usuário BlueXP. Esta é a mesma conta NSS que aparece no topo da página **Gerenciamento NSS**.

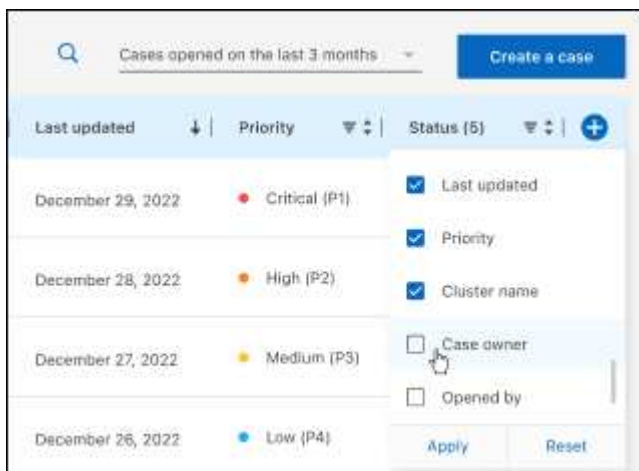
3. Modifique opcionalmente as informações exibidas na tabela:
 - Em **Casos da organização**, selecione **Exibir** para visualizar todos os casos associados à sua empresa.
 - Modifique o intervalo de datas escolhendo um intervalo de datas exato ou escolhendo um período de tempo diferente.



- Filtrar o conteúdo das colunas.



- Altere as colunas que aparecem na tabela selecionando  e então escolher as colunas que você gostaria de exibir.

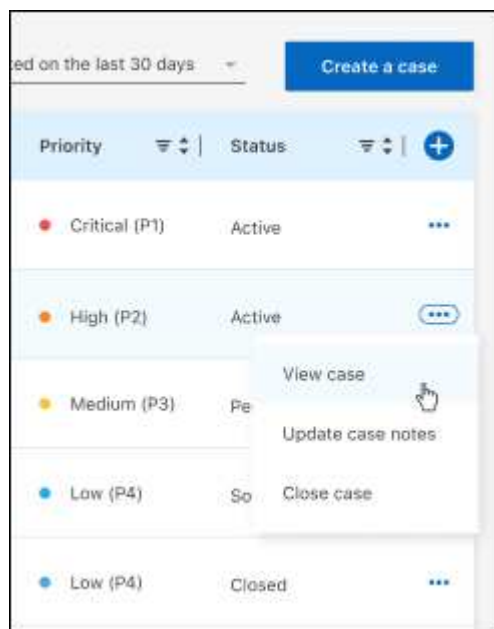


4. Gerencie um caso existente selecionando... e selecionando uma das opções disponíveis:

- **Ver caso:** Veja detalhes completos sobre um caso específico.
- **Atualizar notas do caso:** Forneça detalhes adicionais sobre seu problema ou selecione **Carregar arquivos** para anexar até no máximo cinco arquivos.

Os anexos são limitados a 25 MB por arquivo. As seguintes extensões de arquivo são suportadas: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.

- **Fechar caso:** Forneça detalhes sobre o motivo pelo qual 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 autorais

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marcas Registradas

NETAPP, o logotipo da NETAPP e as marcas listadas na página de Marcas Registradas da NetApp são marcas registradas da NetApp, Inc. Outros nomes de empresas e produtos podem ser marcas registradas 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 e licenças de terceiros usados no software NetApp .

- ["Aviso para o NetApp Console"](#)
- ["Aviso para o Cloud Volumes ONTAP"](#)
- ["Aviso para ONTAP"](#)

Informações sobre direitos autorais

Copyright © 2025 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.