Documentação do Cloud Manager e do Cloud Volumes ONTAP

Cloud Manager 3.8

NetApp
October 22, 2024

Índice

Documentação do Cloud Manager e do Cloud Volumes ONTAP

O Cloud Manager permite que especialistas DE TI e arquitetos de nuvem gerenciem centralmente sua infraestrutura multicloud híbrida usando as soluções de nuvem da NetApp.

BlueXP

O NetApp BlueXP estende e aprimora as funcionalidades fornecidas pelo Cloud Manager.

"Vá para a documentação do BlueXP "

Descubra as novidades

- "Mudanças importantes no Cloud Manager"
- "Novidades no Cloud Manager"
- "O que há de novo no Cloud Volumes ONTAP"

Comece agora

- "Cloud Manager"
- "Definições de conta"
- "Cloud Volumes ONTAP para AWS"
- "Cloud Volumes ONTAP para Azure"
- "Cloud Volumes ONTAP para Google Cloud"
- "Azure NetApp Files"
- "Cloud Volumes Service para AWS"
- "Cloud Volumes Service para Google Cloud"
- "Conformidade com a nuvem"
- "Cache de arquivos global"
- "Backup na nuvem"
- "Cloud Insights"

Automatize com APIs

- "Guia do desenvolvedor de API"
- "Amostras de automação"

Conete-se com colegas, obtenha ajuda e encontre mais informações

- "Comunidade NetApp: Serviços de dados em nuvem"

- "Suporte à NetApp Cloud Volumes ONTAP"
- "Onde obter ajuda e encontrar mais informações"

Notas de lançamento

Cloud Manager

Novidades do Cloud Manager 3,8

O Cloud Manager normalmente apresenta uma nova versão todos os meses para oferecer novos recursos, melhorias e correções de bugs.

Procurando um lançamento anterior? "Novidades em 3,7" "Novidades em 3,6" "Novidades em 3,5"

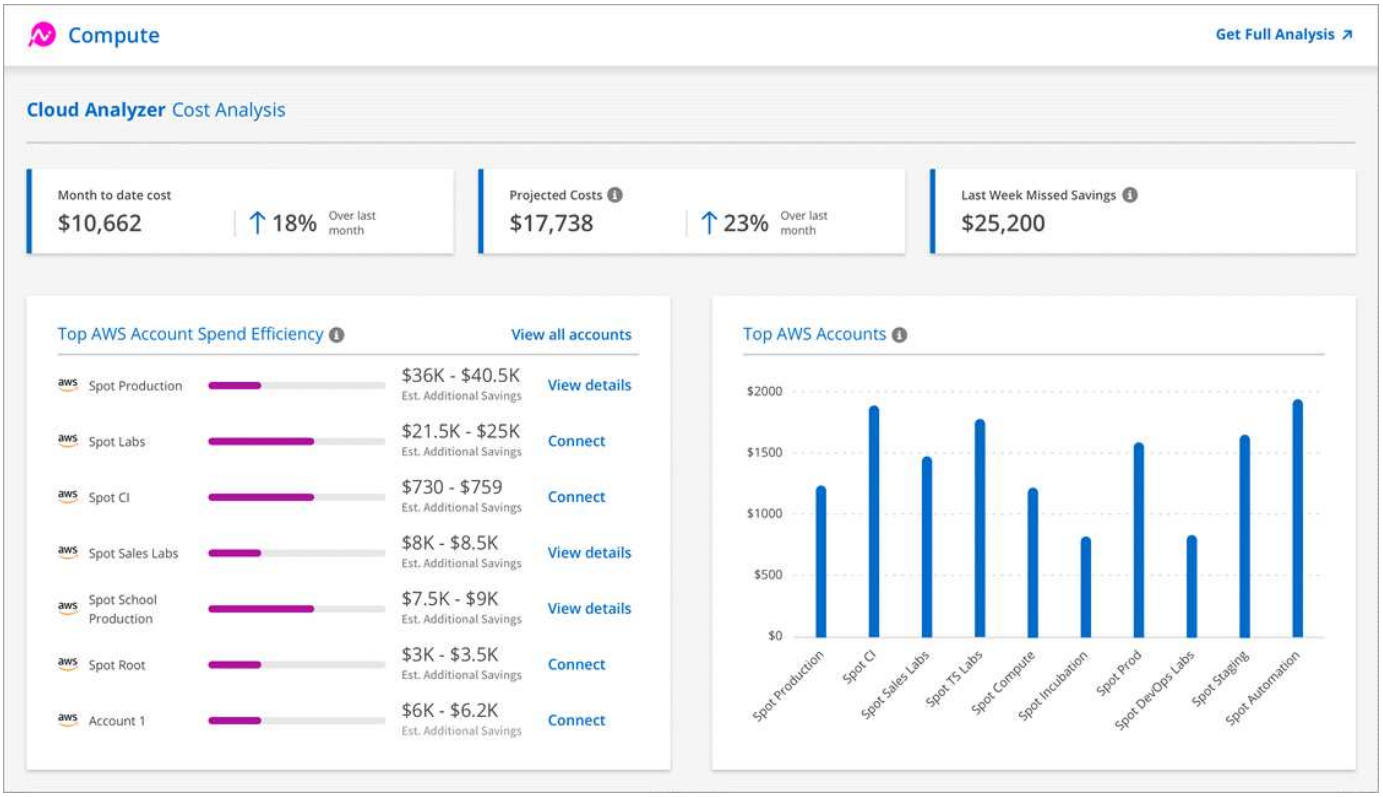
Novo provedor Terraform (19 de outubro de 2020)

Desenvolvemos um novo fornecedor Terraform que as equipes de DevOps podem usar com o Cloud Manager para automatizar e integrar o Cloud Volumes ONTAP à infraestrutura como código.

"Veja o fornecedor do NetApp-cloudmanager".

Atualização do Cloud Manager 3.8.9 (18 out 2020)

Ao aproveitar "Spot's Cloud Analyzer"o , o Cloud Manager agora pode fornecer uma análise de custos de alto nível dos seus gastos com computação em nuvem e identificar possíveis economias. Essas informações estão disponíveis no serviço **Compute** no Cloud Manager. "Saiba mais".



Atualização do Cloud Manager 3.8.9 (13 out 2020)

Lançamos duas atualizações do Cloud Tiering:

- O licenciamento para o Cloud Tiering agora está disponível no Cloud Manager.

  Pague pela disposição de dados em categorias de um cluster do ONTAP no local para a nuvem por meio de uma assinatura com pagamento conforme o uso, uma licença de disposição em camadas do ONTAP chamada *FabricPool* ou uma combinação de ambos.

- O serviço autônomo de disposição em camadas na nuvem foi desativado. Agora você deve acessar o Cloud Tiering diretamente no Cloud Manager, onde todos os mesmos recursos e funcionalidades estão disponíveis.

Cloud Manager 3.8.9 (4 de outubro de 2020)

- Melhorias de conformidade com a nuvem
- Aprimoramentos do Cloud Volumes Service para AWS
- Integração com Cloud Sync
- Melhorias no gerenciamento de contas
- Mudanças para regiões governamentais

Melhorias de conformidade com a nuvem

- Uma nova função **Cloud Compliance Viewer** está disponível no Cloud Manager.

  Os usuários que recebem essa função só podem exibir informações de conformidade e gerar relatórios para workspaces que eles têm permissão para acessar. Eles não podem gerenciar as configurações de conformidade da nuvem e não podem acessar outros recursos e serviços do Cloud Manager. Essa pode ser a função perfeita para sua equipe jurídica, para que ela possa monitorar os resultados da verificação de conformidade com a nuvem. "funções de utilizador"Consulte para obter detalhes.

- Adicionado suporte para verificar esquemas de banco de dados MongoDB e PostgreSQL. Consulte "digitalização de esquemas de banco de dados" para obter mais informações.
- O preço do Cloud Compliance muda a partir de outubro de 7th.

  Os primeiros 1 TB de dados verificados pelo Cloud Compliance em um espaço de trabalho do Cloud Manager são gratuitos. Isso inclui dados do Cloud Volumes ONTAP volumes, do Azure NetApp Files volumes, buckets do Amazon S3 e esquemas de banco de dados. É necessária uma subscrição para verificar quaisquer dados adicionais depois de atingir os 1 TB. "preços"Consulte para obter detalhes.

Aprimoramentos do Cloud Volumes Service para AWS

Ao criar um novo volume, você pode optar por basear esse volume em uma cópia Snapshot existente de outro volume.

Integração com Cloud Sync

O serviço Cloud Sync da NetApp agora está disponível no Cloud Manager. O Cloud Sync oferece uma maneira simples, segura e automatizada de migrar seus dados de qualquer destino de origem para qualquer destino, na nuvem ou no local. "Saiba mais".

Melhorias no gerenciamento de contas

Adicionámos mais formas de gerir a sua conta.

- Uma visão geral dos recursos da sua conta já está disponível.

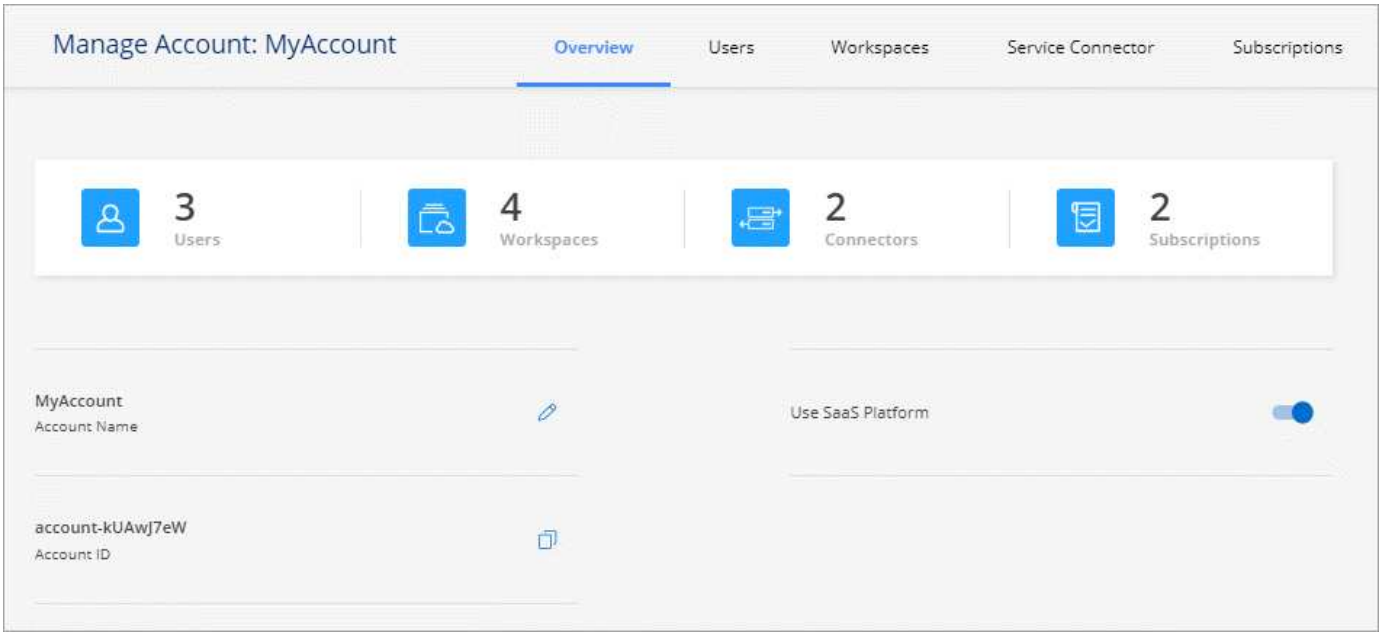
  Você pode visualizar rapidamente o número de usuários, espaços de trabalho, conetores e assinaturas na sua conta.

- Você pode alterar o nome da sua conta.
- Você pode copiar o ID da conta, o ID do workspace ou o ID do conetor.

  Copiar esses IDs ajudará com recursos de automação que estamos planejando.

- Você pode desativar o uso da plataforma SaaS.

  Não recomendamos desativar a plataforma SaaS a menos que você precise para cumprir com as políticas de segurança da sua empresa. Desativar a plataforma SaaS limita sua capacidade de usar os serviços de nuvem integrados da NetApp. "Saiba mais".



Mudanças para regiões governamentais

Se você implantar um conetor em uma região do AWS GovCloud, uma região do Azure Gov ou uma região do Azure DoD, o acesso ao Cloud Manager agora estará disponível somente por meio do endereço IP do host de um conetor. O acesso à plataforma SaaS está desativado para toda a conta.

Isso significa que somente usuários privilegiados que podem acessar a VPC/VNet interna do usuário final podem usar a IU ou API do Cloud Manager.

"Saiba mais sobre esta limitação".

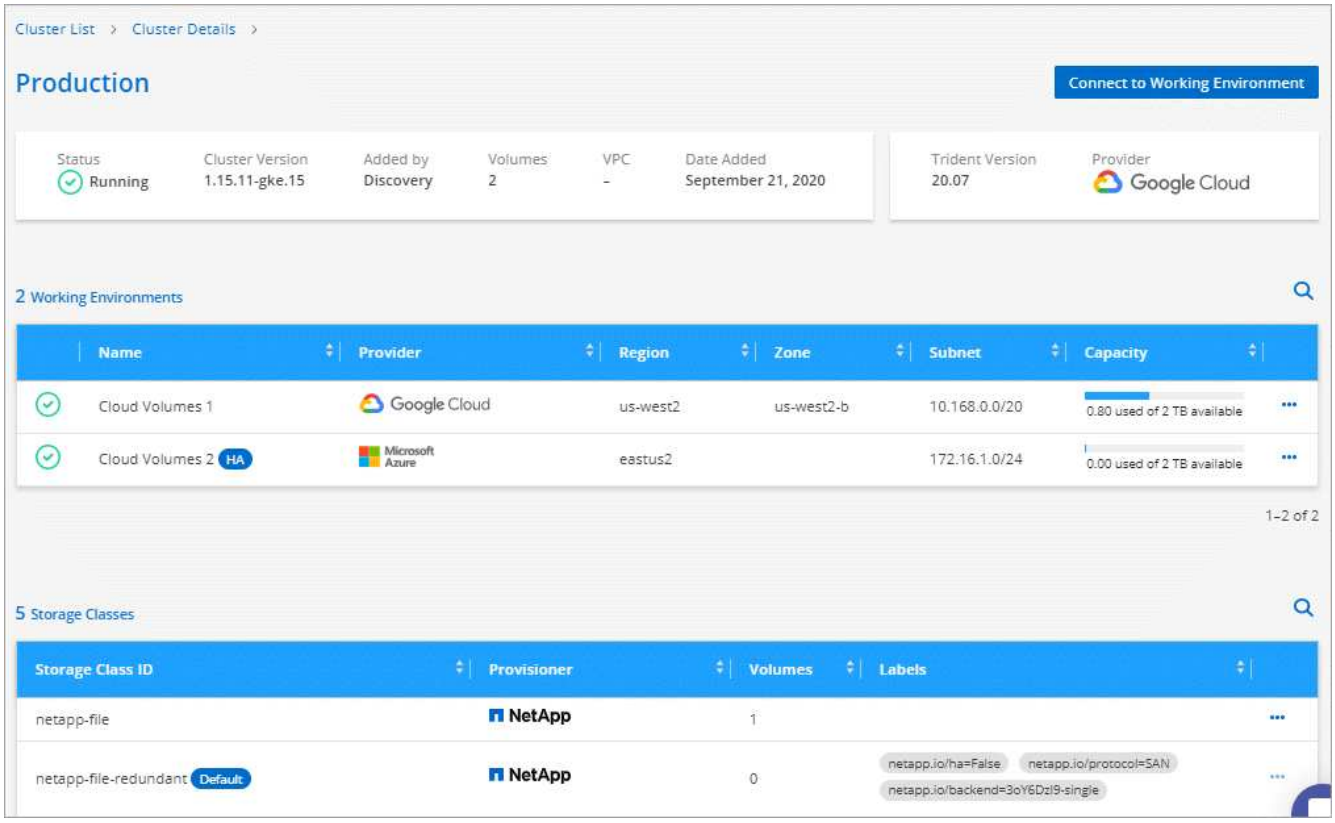
Atualização do Cloud Manager 3.8.8 (22 de setembro de 2020)

Aprimoramos o serviço Kubernetes para facilitar o uso e fornecer recursos adicionais:

- Facilitamos a descoberta dos clusters de Kubernetes executados no serviço Kubernetes gerenciado do seu fornecedor de nuvem.

  Basta clicar em **Discover clusters** e o Cloud Manager descobrirá seus clusters gerenciados usando as permissões de provedor de nuvem que você já forneceu.

- Agora, você pode ver mais informações sobre um cluster do Kubernetes descoberto, incluindo seu estado, o número de volumes, classes de armazenamento e muito mais.



- Adicionamos a verificação de recursos e erros para garantir que a comunicação esteja disponível entre o cluster e o Cloud Volumes ONTAP. E se não for, então vamos informá-lo.

"Saiba como começar".

Observe que a conta de serviço de um conetor requer as seguintes permissões para descobrir e gerenciar clusters do Kubernetes executados no Google Kubernetes Engine (GKE):

```
- container.*
```

Atualização do Cloud Manager 3.8.8 (10 de setembro de 2020)

Os seguintes aprimoramentos estão disponíveis ao implantar o Global File Cache por meio do Cloud Manager:

- Um par de HA da Cloud Volumes ONTAP na AWS agora é compatível como a plataforma de storage de back-end para seu storage central.
- Várias instâncias do Global File Cache Core podem ser implantadas em um design Load Distributed.

"Saiba mais sobre o Global File Cache".

Cloud Manager 3.8.8 (9 de setembro de 2020)

- Suporte ao Cloud Volumes Service para Google Cloud
- O backup na nuvem agora é compatível com clusters ONTAP no local
- Aprimoramentos do backup na nuvem
- Melhorias de conformidade com a nuvem
- Navegação atualizada
- Melhorias na administração

Suporte ao Cloud Volumes Service para Google Cloud

- Adicione um ambiente de trabalho para gerenciar o Cloud Volumes Service existente para volumes do GCP e para criar novos volumes. "Saiba como".
- Crie e gerencie volumes NFSv3 e NFSv4,1 para clientes Linux e UNIX e volumes SMB 3.x para clientes Windows.
- Criar, excluir e restaurar snapshots de volume.

O backup na nuvem agora é compatível com clusters ONTAP no local

Comece a fazer backup dos dados dos sistemas ONTAP no local para a nuvem. Habilite o backup na nuvem em seus ambientes de trabalho no local para fazer backup de volumes para storage Azure Blob. "Saiba mais".

Aprimoramentos do backup na nuvem

Revisamos a interface do usuário para melhor usabilidade:

- Página de lista de volumes para ver facilmente os volumes que estão sendo copiados, juntamente com os backups disponíveis
- Página de definições de cópia de segurança para ver as definições de cópia de segurança para cada ambiente de trabalho

Melhorias de conformidade com a nuvem

- Capacidade de digitalizar dados de bancos de dados

  Analise seus bancos de dados para identificar os dados pessoais e confidenciais que residem em cada esquema. Os bancos de dados compatíveis incluem Oracle, SAP HANA e SQL Server (MSSQL). "Saiba mais sobre como digitalizar bancos de dados".

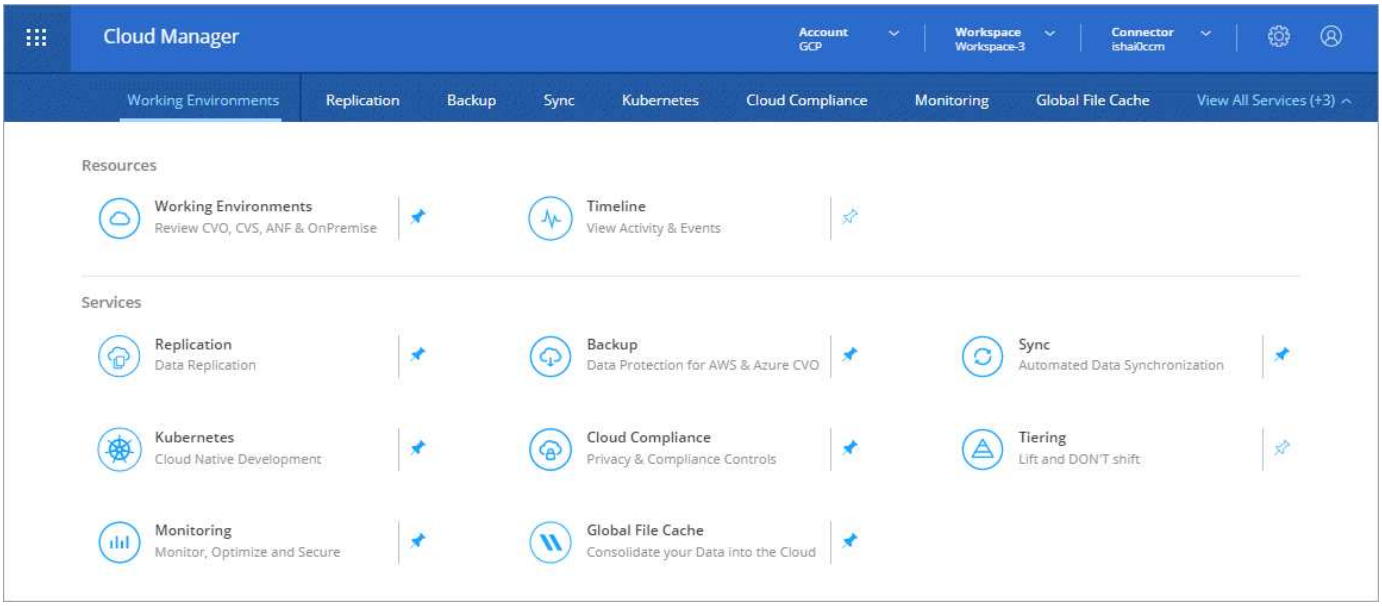
- Capacidade de verificar volumes de proteção de dados (DP)

  Os volumes DP são volumes de destino das operações do SnapMirror que costumam ser de clusters ONTAP on-premises. Agora você pode identificar facilmente os dados pessoais e confidenciais que residem nesses arquivos no local. "Veja como".

Navegação atualizada

Atualizamos o cabeçalho no Cloud Manager para facilitar a navegação entre os serviços de nuvem da NetApp.

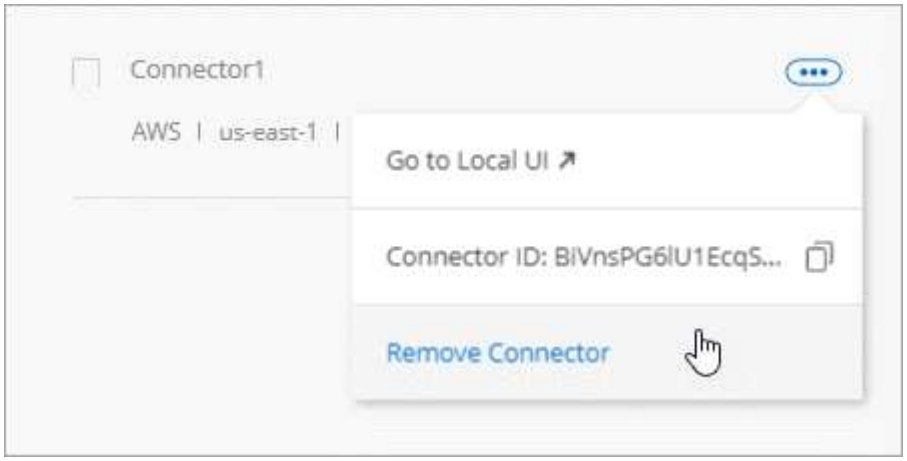
Clique em **Exibir todos os Serviços** e você pode fixar e desfixar os serviços que deseja ver na navegação.



Como você pode ver, também atualizamos os menus suspensos conta, Área de trabalho e conetor, para que seja mais fácil visualizar suas seleções atuais.

Melhorias na administração

- Agora você pode remover conetores inativos do Cloud Manager. "Saiba como".



- Agora você pode substituir a assinatura do Marketplace que está atualmente associada às credenciais do seu provedor de nuvem. Se você precisar alterar a forma como você é cobrado, essa alteração pode ajudá-lo a garantir que você está sendo cobrado por meio da assinatura certa do Marketplace.

  Saiba como "Na AWS", "No Azure" "No GCP"e .

Atualização das permissões necessárias do Azure (6 ago 2020)

Para evitar falhas de implantação do Azure, certifique-se de que sua política do Cloud Manager no Azure inclua a seguinte permissão:

```
"Microsoft.Resources/deployments/operationStatuses/read"
```

O Azure agora requer essa permissão para algumas implantações de máquinas virtuais (depende do hardware físico subjacente usado durante a implantação).

"Veja a política mais recente do Cloud Manager para Azure".

Cloud Manager 3.8.7 (3 de agosto de 2020)

- Nova experiência de software como serviço
- Melhorias no Cloud Volumes ONTAP
- Melhorias no Azure NetApp Files
- Aprimoramentos do Cloud Volumes Service para AWS
- Melhorias de conformidade com a nuvem
- Aprimoramentos do backup na nuvem
- Suporte para Global File Cache

Nova experiência de software como serviço

Introduzimos totalmente uma experiência de software como serviço no Cloud Manager. Essa nova experiência facilita o uso do Cloud Manager e nos permite fornecer recursos adicionais para gerenciar sua infraestrutura de nuvem híbrida.

O Cloud Manager inclui um "Interface baseada em SaaS" que é integrado ao NetApp Cloud Central e conetores que permitem ao Cloud Manager gerenciar recursos e processos em seu ambiente de nuvem pública. (Na verdade, o conetor é o mesmo que o software existente do Cloud Manager instalado.)

Na maioria dos casos, um conetor é necessário, mas não é necessário usar o Azure NetApp Files, o Cloud Volumes Service ou o Cloud Sync do Cloud Manager.

Como mencionado anteriormente nestas notas de versão, você precisará atualizar o tipo de máquina para seus conetores para acessar os novos recursos que estamos oferecendo. O Cloud Manager solicitará instruções para alterar o tipo de máquina. "Saiba mais".

Melhorias no Cloud Volumes ONTAP

Dois aprimoramentos estão disponíveis para o Cloud Volumes ONTAP.

- * Várias licenças BYOL para alocar capacidade adicional*

  Agora você pode comprar várias licenças para um sistema BYOL da Cloud Volumes ONTAP para alocar mais de 368 TB de capacidade. Por exemplo, você pode comprar duas licenças para alocar até 736 TB de capacidade para o Cloud Volumes ONTAP. Ou você pode comprar quatro licenças para obter até 1,4 PB.

  O número de licenças que você pode comprar para um único sistema de nó ou par de HA é ilimitado.

  Esteja ciente de que os limites de disco podem impedir que você alcance o limite de capacidade usando discos sozinhos. Você pode ir além do limite de disco pelo "disposição em camadas dos dados inativos no storage de objetos". Para obter informações sobre limites de disco, "Limites de armazenamento nas Notas de versão do Cloud Volumes ONTAP" consulte .

"Saiba como adicionar uma nova licença de sistema".

- **Encrypt discos gerenciados do Azure usando chaves externas**

  Agora você pode criptografar discos gerenciados do Azure em sistemas Cloud Volumes ONTAP de nó único usando chaves externas de outra conta. Esse recurso é compatível com APIs.

  Você só precisa adicionar o seguinte à solicitação de API ao criar o sistema de nó único:

```
"azureEncryptionParameters": {
      "key": <azure id of encryptionset>
  }
```

  Esse recurso requer novas permissões, como mostrado na última "Política do Cloud Manager para Azure".

```
"Microsoft.Compute/diskEncryptionSets/read"
```

Melhorias no Azure NetApp Files

Esta versão inclui várias melhorias no suporte do Azure NetApp Files.

- **Configuração do Azure NetApp Files**

  Agora você pode configurar e gerenciar o Azure NetApp Files diretamente do Cloud Manager. "Saiba como".

- * Novo suporte ao protocolo*

  Agora você pode criar volumes NFSv4,1 e volumes SMB.

- **Gerenciamento de snapshot de volume e pool de capacidade**

  O Cloud Manager permite criar, excluir e restaurar snapshots de volume. Você também pode criar novos pools de capacidade e especificar seus níveis de serviço.

- * Capacidade de editar volumes*

  Você pode editar um volume alterando seu tamanho e gerenciando tags.

Aprimoramentos do Cloud Volumes Service para AWS

Há muitas melhorias no Cloud Manager em suporte ao Cloud Volumes Service para AWS.

- * Novo suporte ao protocolo*

  Agora você pode criar volumes NFSv4,1, volumes SMB e volumes de protocolo duplo. Anteriormente, você só podia criar e descobrir volumes NFSv3 no Cloud Manager.

- **Suporte instantâneo**

  Você pode criar políticas de snapshot para automatizar a criação de snapshots de volume, criar um

snapshot sob demanda, restaurar um volume de um snapshot, criar um novo volume com base em um snapshot existente e muito mais. Consulte "Gerenciamento de snapshots do Cloud volumes" para obter mais informações.

- **Crie o volume inicial em uma região a partir do Cloud Manager**

  Antes desta versão, o primeiro volume em cada região tinha que ser criado na interface Cloud Volumes Service para AWS. Agora você pode se inscrever "Uma das ofertas do NetApp Cloud Volumes Service no AWS Marketplace"e criar o primeiro volume a partir do Cloud Manager.

Melhorias de conformidade com a nuvem

As melhorias a seguir estão agora disponíveis para o Cloud Compliance.

- **Processo de implantação revisado para sua instância de conformidade com a nuvem**

  A instância do Cloud Compliance é configurada e implantada usando um novo assistente no Cloud Manager. Após a conclusão da implementação, você ativa o serviço para cada ambiente de trabalho que deseja analisar.

- * Capacidade de selecionar os volumes a serem digitalizados dentro de um ambiente de trabalho*

  Agora você pode ativar e desativar a digitalização de volumes individuais em um ambiente de trabalho Cloud Volumes ONTAP ou Azure NetApp Files. Se você não precisar verificar certos volumes para conformidade, desative-os.

  "Saiba mais sobre como desativar a digitalização de volumes."

- * Abas de navegação para saltar rapidamente para a sua área de interesse*

  Novas guias para Dashboard, Investigation e Configuration permitem que você acesse essas seções com mais facilidade.

- **Relatório HIPAA**

  Um novo Relatório HIPAA (Health Insurance Portability and Accountability Act) já está disponível. Esse relatório foi elaborado para auxiliar a organização a obedecer às leis de privacidade de dados HIPAA.

  "Saiba mais sobre o relatório HIPAA."

- **Novo tipo de dados pessoais sensíveis**

  O Cloud Compliance agora pode encontrar códigos médicos ICD-9-CM em arquivos.

- **Novo tipo de dados pessoais**

  O Cloud Compliance agora pode encontrar dois novos identificadores nacionais em arquivos: Croatian ID (OIB) e Greek ID.

Aprimoramentos do backup na nuvem

Os aprimoramentos a seguir estão agora disponíveis para o Backup to Cloud.

- **Bring Your own License (BYOL) já está disponível**

O backup para a nuvem só estava disponível com uma licença Pay as You Go (PAYGO). Uma licença BYOL permite que você compre uma licença da NetApp para usar o backup na nuvem por um determinado período de tempo e por um espaço máximo de backup. Quando um dos limites for atingido, você precisará renovar a licença.

"Saiba mais sobre a nova licença BYOL do Backup to Cloud."

- **Suporte para volumes de proteção de dados (DP)**

  É possível fazer backup e restaurar volumes de proteção de dados agora.

Suporte para Global File Cache

Com o NetApp, você consolida silos de servidores de arquivos distribuídos em um espaço físico do storage global e coeso na nuvem pública. Isso cria um sistema de arquivos globalmente acessível na nuvem que todos os locais distribuídos podem usar como se fossem locais.

A partir desta versão, a instância Global File Cache Management e a instância Core podem ser implantadas e gerenciadas por meio do Cloud Manager. Isso economiza muitas horas durante o processo de implantação inicial e fornece um painel único por meio do Cloud Manager para este e outros sistemas implantados. As instâncias do Global File Cache Edge ainda são implantadas localmente em seus escritórios remotos.

Consulte "Visão geral do Global File Cache" para obter mais informações.

A configuração inicial que pode ser implantada usando o Cloud Manager deve atender aos seguintes requisitos. Outras configurações, como o Cloud Volumes Service, o Azure NetApp Files e o Cloud Volumes Service para AWS e o GCP, continuam sendo implantadas usando os procedimentos legados. "Saiba mais".

- A plataforma de storage de back-end usada como seu storage central deve ser um ambiente operacional no qual você implantou um par de HA do Cloud Volumes ONTAP no Azure.

  Outras plataformas de storage e outros provedores de nuvem não são compatíveis no momento usando o Cloud Manager, mas podem ser implantadas usando procedimentos de implantação legados.

- O GFC Core pode ser implantado apenas como uma instância autônoma.

  Se você precisar usar um design Load Distributed que inclua várias instâncias principais, você deve usar os procedimentos legados.

Esse recurso requer novas permissões, como mostrado na última "Política do Cloud Manager para Azure".

```
"Microsoft.Resources/deployments/operationStatuses/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/delete",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
```

Uma experiência melhorada requer um tipo de máquina mais forte (15 de julho de 2020)

À medida que melhoramos a experiência do Cloud Manager, você precisará atualizar seu tipo de máquina para acessar os novos recursos que oferecemos. As melhorias incluirão "Experiência de software como serviço para o Cloud Manager"integrações de serviços de nuvem novas e aprimoradas.

O Cloud Manager solicitará instruções para alterar o tipo de máquina.

Aqui estão alguns detalhes:

1. Para garantir que os recursos adequados estejam disponíveis para a funcionalidade adequada dos novos recursos no Cloud Manager, alteramos a instância padrão, a VM e o tipo de máquina da seguinte forma:
   - AWS: t3.xlarge
   - Azure: DS3 v2
   - GCP: N1-standard-4

   Esses tamanhos padrão são o mínimo "Com base nos requisitos de CPU e RAM"suportado .
2. Como parte dessa transição, o Cloud Manager requer acesso ao seguinte endpoint para que ele possa obter imagens de software de componentes de contentor para uma infraestrutura Docker:

   https://cloudmanagerinfraprod.azurecr.io

   Certifique-se de que o firewall permite o acesso a este endpoint a partir do Cloud Manager.

Cloud Manager 3.8.6 (6 de julho de 2020)

- Suporte para volumes iSCSI
- Suporte à política de disposição em categorias

Suporte para volumes iSCSI

Agora, o Cloud Manager permite criar volumes iSCSI para Cloud Volumes ONTAP e clusters ONTAP locais diretamente a partir da interface de usuário.

Quando você cria um volume iSCSI, o Cloud Manager cria automaticamente um LUN para você. Simplificamos a criação de apenas um LUN por volume, para que não haja gerenciamento envolvido. Depois de criar o volume, "Use o IQN para se conetar ao LUN a partir de seus hosts".

Você pode criar LUNs adicionais no System Manager ou na CLI.

Suporte à política de disposição em categorias

Agora, você pode escolher a política de disposição em categorias ao criar ou modificar um volume para o Cloud Volumes ONTAP. Quando você usa a política de disposição em categorias, os dados são imediatamente marcados como inativos e dispostos em camadas no storage de objetos o mais rápido possível. "Saiba mais sobre categorização de dados".

Transição do Cloud Manager para SaaS (22 de junho de 2020)

Apresentamos uma experiência de software como serviço para o Cloud Manager. Essa nova experiência facilita o uso do Cloud Manager e nos permite fornecer recursos adicionais para gerenciar sua infraestrutura de nuvem híbrida. "Saiba mais".

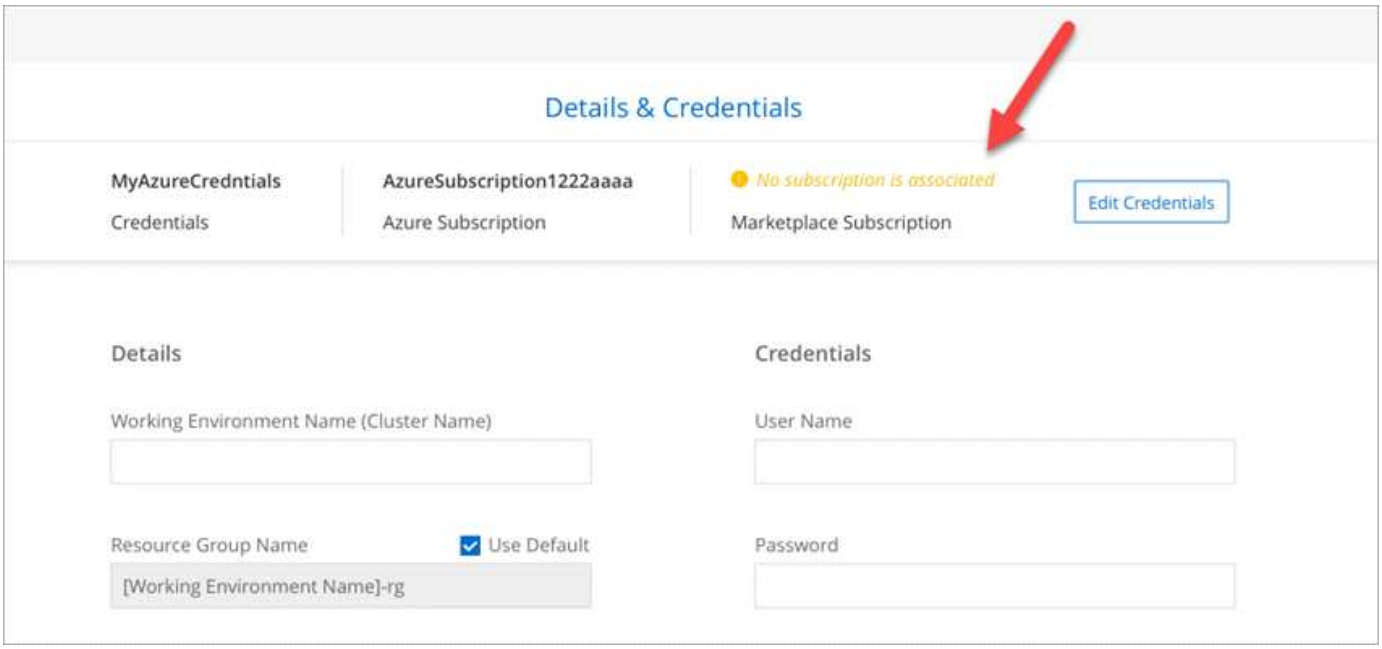
Cloud Manager 3.8.5 (31 de maio de 2020)

- É necessária uma nova subscrição no Azure Marketplace
- Aprimoramentos do backup na nuvem
- Melhorias de conformidade com a nuvem

É necessária uma nova subscrição no Azure Marketplace

Uma nova assinatura está disponível no Azure Marketplace. Essa assinatura única é necessária para implantar o Cloud Volumes ONTAP 9,7 PAYGO (exceto o sistema de avaliação gratuita de 30 dias). A assinatura também nos permite oferecer recursos adicionais para o Cloud Volumes ONTAP PAYGO e BYOL. Você será cobrado a partir desta assinatura por cada sistema Cloud Volumes ONTAP PAYGO que você criar e cada recurso de add-on que você ativar.

O Cloud Manager solicitará que você assine esta oferta quando você implantar um novo sistema Cloud Volumes ONTAP (9,7 P1 ou posterior).



Aprimoramentos do backup na nuvem

Os aprimoramentos a seguir estão agora disponíveis para o Backup to Cloud.

- No Azure, agora você pode criar um novo grupo de recursos ou selecionar um grupo de recursos existente em vez de ter o Cloud Manager criar um para você. O grupo de recursos não pode ser alterado depois de ativar o Backup to Cloud.
- Na AWS, agora você pode fazer backup de instâncias do Cloud Volumes ONTAP que residem em uma conta diferente da conta AWS do Cloud Manager.
- Opções adicionais estão agora disponíveis ao selecionar o agendamento de backup para volumes. Além das opções de backup diário, semanal e mensal, agora você pode selecionar uma das políticas definidas pelo sistema que oferecem políticas de combinação como 30 backups diários, 13 semanais e 12 mensais.
- Depois de excluir todos os backups de um volume, agora você pode começar a criar backups novamente para esse volume. Esta era uma limitação conhecida na versão anterior.

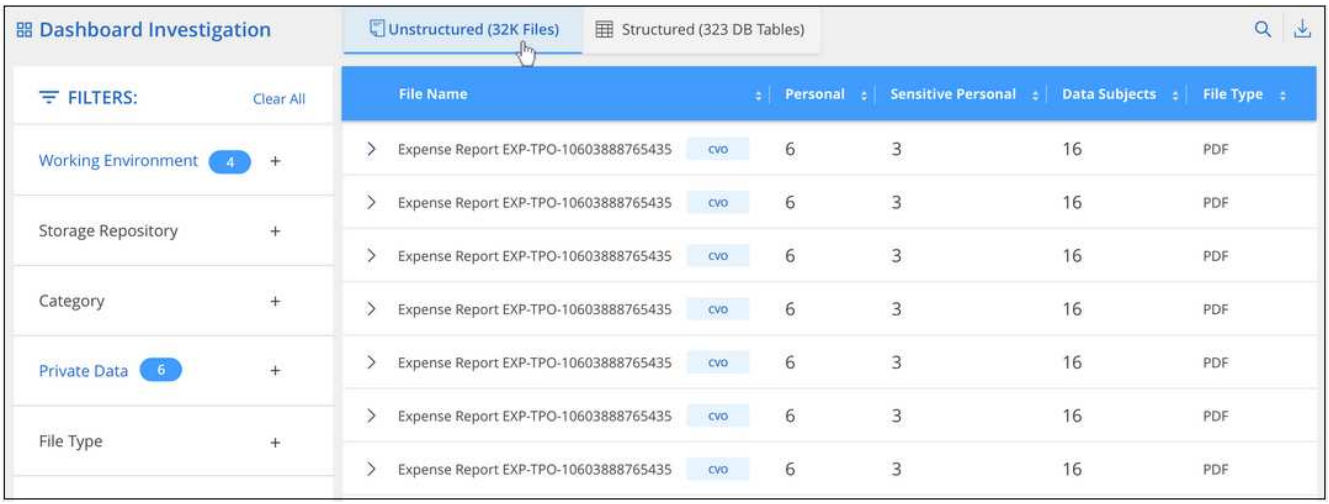
Melhorias de conformidade com a nuvem

Os aprimoramentos a seguir estão disponíveis para o Cloud Compliance.

- Agora você pode verificar buckets do S3 que estão em contas diferentes da AWS que a instância do Cloud Compliance. Você só precisa criar uma função nessa nova conta para que a instância existente do Cloud Compliance possa se conectar a esses buckets. "Saiba mais".

  Se você configurou o Cloud Compliance antes da versão 3,8.5, será necessário modificar o existente "Função do IAM para a instância de Cloud Compliance" para usar essa funcionalidade.

- Agora você pode filtrar o conteúdo da página de investigação para exibir apenas os resultados que deseja ver. Os filtros incluem ambiente de trabalho, categoria, dados privados, tipo de arquivo, data da última modificação e se as permissões do objeto S3 estão abertas ao acesso público.



- Agora você pode ativar e desativar o Cloud Compliance em um ambiente de trabalho diretamente na guia Cloud Compliance.

Atualização do Cloud Manager 3.8.4 (10 de maio de 2020)

Lançamos um aprimoramento para o Cloud Manager 3,8.4.

Integração com Cloud Insights

Ao utilizar o serviço Cloud Insights da NetApp, o Cloud Manager fornece insights sobre a integridade e a performance das instâncias do Cloud Volumes ONTAP e ajuda você a solucionar problemas e otimizar a performance do seu ambiente de storage de nuvem. "Saiba mais".

Cloud Manager 3.8.4 (3 de maio de 2020)

O Cloud Manager 3.8.4 inclui as seguintes melhorias.

Aprimoramentos do backup na nuvem

Os aprimoramentos a seguir estão agora disponíveis para o Backup to Cloud (anteriormente chamado de *Backup to S3* para AWS):

- **Fazer backup para armazenamento Azure Blob**

  O backup na nuvem agora está disponível para o Cloud Volumes ONTAP no Azure. O backup to Cloud

oferece recursos de backup e restauração para proteção e arquivamento de longo prazo de seus dados de nuvem. "Saiba mais".

- **Excluindo backups**

  Agora você pode excluir todos os backups de um volume específico diretamente da interface do Cloud Manager. "Saiba mais".

Cloud Manager 3.8.3 (5 de abril de 2020)

- Integração com o Cloud Tiering
- Migração de dados para o Azure NetApp Files
- Melhorias de conformidade com a nuvem
- Backup para aprimoramentos do S3
- Volumes iSCSI usando APIs

Integração com o Cloud Tiering

O serviço de disposição em camadas de nuvem do NetApp agora está disponível no Cloud Manager. Com o Cloud Tiering, você pode categorizar dados de um cluster ONTAP no local para storage de objetos de baixo custo na nuvem. Isso libera espaço de storage de alta performance no cluster para mais workloads.

"Saiba mais".

Migração de dados para o Azure NetApp Files

Agora é possível migrar dados NFS ou SMB para o Azure NetApp Files diretamente do Cloud Manager. As sincronizações de dados são alimentadas pelo serviço Cloud Sync da NetApp.

"Saiba como migrar dados para o Azure NetApp Files".

Melhorias de conformidade com a nuvem

As melhorias a seguir estão agora disponíveis para o Cloud Compliance.

- **Avaliação gratuita de 30 dias para o Amazon S3**

  Uma avaliação gratuita de 30 dias agora está disponível para verificar dados do Amazon S3 com o Cloud Compliance. Se você ativou o Cloud Compliance anteriormente no Amazon S3, sua avaliação gratuita de 30 dias estará ativa a partir de hoje (5 de abril de 2020).

  Uma assinatura do AWS Marketplace é necessária para continuar a digitalizar o Amazon S3 após o término da avaliação gratuita. "Saiba como se inscrever".

  "Saiba mais sobre a definição de preço para verificar o Amazon S3".

- **Novo tipo de dados pessoais**

  O Cloud Compliance agora pode encontrar um novo identificador nacional nos arquivos: Brazilian ID (CPF).

  "Saiba mais sobre os tipos de dados pessoais".

- **Suporte para categorias adicionais de metadados**

  Agora, o Cloud Compliance pode categorizar seus dados em nove categorias adicionais de metadados. "Consulte a lista completa das categorias de metadados compatíveis".

Backup para aprimoramentos do S3

As melhorias a seguir estão agora disponíveis para o serviço Backup to S3.

- **S3 política de ciclo de vida para backups**

  Os backups começam na classe de armazenamento *Standard* e passam para a classe de armazenamento *Standard-unusual Access* após 30 dias.

- **Excluindo backups**

  Agora você pode excluir backups usando uma API do Cloud Manager. "Saiba mais".

- **Bloquear acesso público**

  Agora, o Cloud Manager ativa o "Recurso de acesso público do Amazon S3 Block" bucket do S3 onde os backups são armazenados.

Volumes iSCSI usando APIs

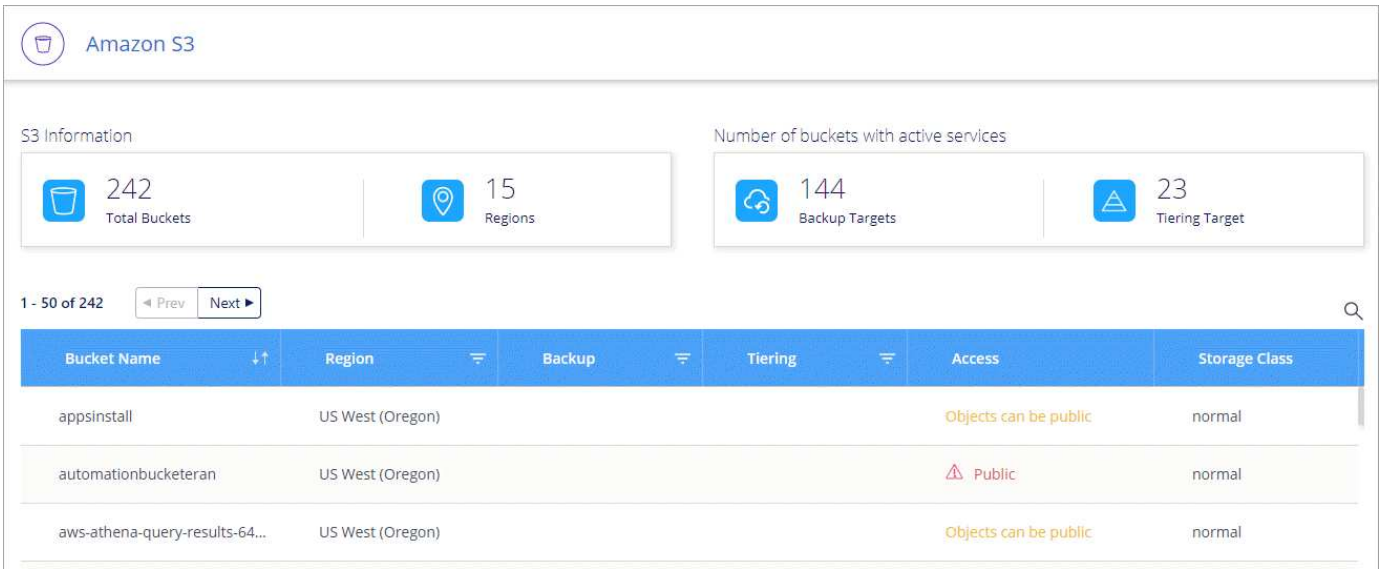
As APIs do Cloud Manager agora permitem que você crie volumes iSCSI. "Veja um exemplo aqui".

Cloud Manager 3.8.2 (1 de março de 2020)

- Ambientes de trabalho do Amazon S3
- Melhorias de conformidade com a nuvem
- Versão de NFS para volumes
- Suporte para regiões Azure US Gov

Ambientes de trabalho do Amazon S3

O Cloud Manager agora descobre automaticamente informações sobre os buckets do Amazon S3 que residem na conta da AWS onde são instalados. Isso permite que você veja facilmente detalhes sobre os buckets do S3, incluindo a região, nível de acesso, classe de storage e se o bucket é usado com o Cloud Volumes ONTAP para backups ou categorização de dados. E você pode verificar os buckets do S3 com o Cloud Compliance, conforme descrito abaixo.



Melhorias de conformidade com a nuvem

As melhorias a seguir estão agora disponíveis para o Cloud Compliance.

- **Suporte para Amazon S3**

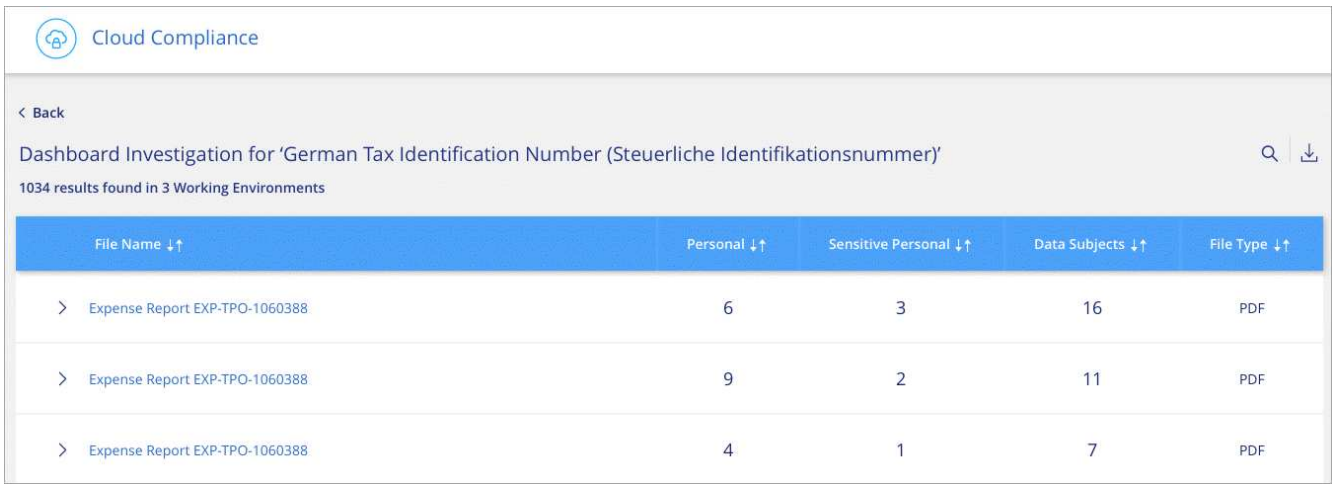
  O Cloud Compliance agora pode verificar seus buckets do Amazon S3 para identificar os dados pessoais e confidenciais que residem no storage de objetos do S3. O Cloud Compliance pode verificar qualquer bucket da conta, independentemente de ter sido criado para uma solução da NetApp.

  "Saiba como começar".

- **Página de investigação**

  Uma nova página de investigação agora está disponível para cada tipo de arquivo pessoal, arquivo pessoal sensível, categoria e tipo de arquivo. A página mostra detalhes sobre os arquivos afetados e permite classificar pelos arquivos que incluem a maioria dos dados pessoais, dados pessoais confidenciais e nomes dos titulares dos dados. Esta página substitui o relatório CSV que estava disponível anteriormente.

  Aqui está uma amostra:



  "Saiba mais sobre a página de investigação".

- **Relatório PCI DSS**

  Um novo Relatório PCI DSS (Payment Card Industry Data Security Standard) já está disponível. Este relatório pode ajudá-lo a identificar a distribuição de informações de cartão de crédito em seus arquivos. Você pode ver quantos arquivos contêm informações de cartão de crédito, quer os ambientes de trabalho sejam protegidos por criptografia ou proteção contra ransomware, detalhes de retenção e muito mais.

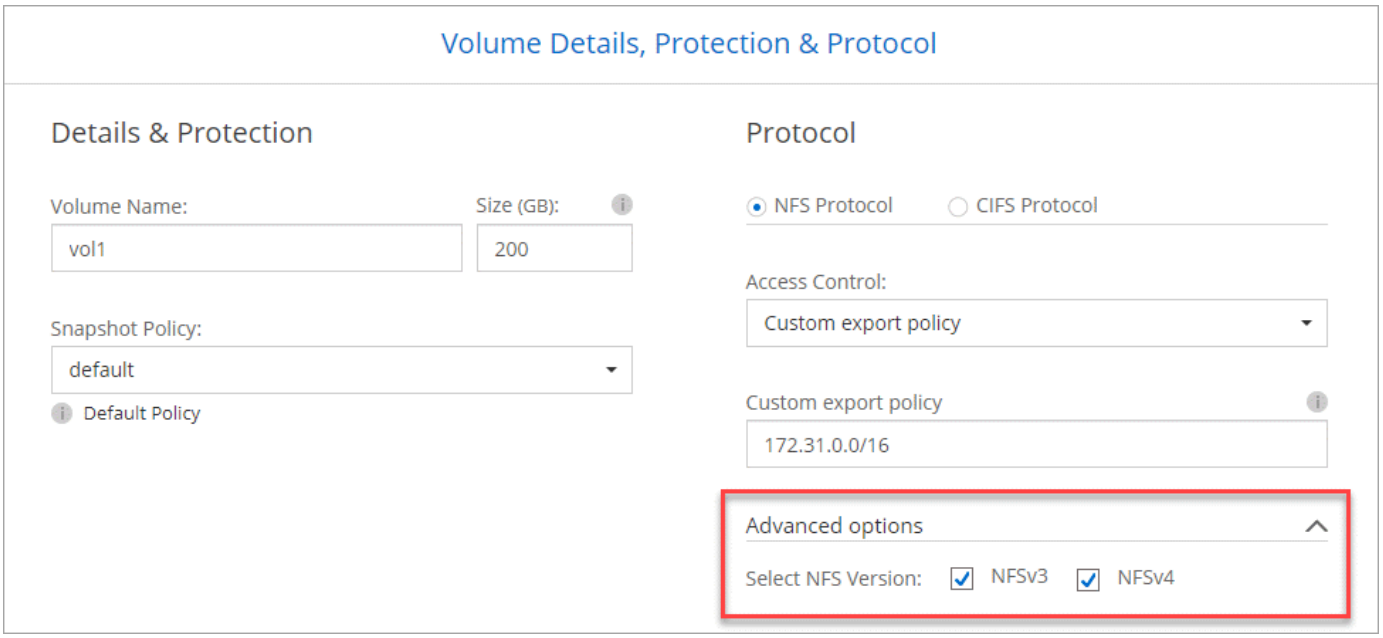
  "Saiba mais sobre o relatório PCI DSS".

- **Novo tipo de dados pessoais sensíveis**

  O Cloud Compliance agora pode encontrar códigos médicos ICD-10-CM, que são usados na indústria médica e de saúde.

Versão de NFS para volumes

Agora você pode selecionar a versão NFS para ativar em um volume quando criar ou editar um volume para o Cloud Volumes ONTAP.



Suporte para regiões Azure US Gov

Os pares de HA do Cloud Volumes ONTAP agora são compatíveis com regiões Azure US Gov.

"Consulte a lista de regiões do Azure suportadas".

Atualização do Cloud Manager 3.8.1 (16 de fevereiro de 2020)

Lançamos algumas melhorias no Cloud Manager 3,8.1.

Backup para aprimoramentos do S3

- As cópias de backup agora são armazenadas em um bucket do S3 criado pelo Cloud Manager na sua conta da AWS, com um bucket por ambiente de trabalho do Cloud Volumes ONTAP.
- O backup para S3 agora é compatível com todas as regiões da AWS "Onde o Cloud Volumes ONTAP é suportado" .

- Você pode definir o agendamento de backup para diário, semanal ou mensal.
- O Cloud Manager não precisa mais configurar *links privados* para o serviço Backup to S3.

Permissões adicionais do S3 são necessárias para esses aprimoramentos. A função do IAM que fornece permissões ao Cloud Manager deve incluir permissões do último "Política do Cloud Manager".

"Saiba mais sobre o Backup para S3".

Atualizações da AWS

Introduzimos o suporte para novas instâncias do EC2 e uma alteração no número de discos de dados suportados para o Cloud Volumes ONTAP 9,6 e 9,7. Confira as alterações nas Notas de versão do Cloud Volumes ONTAP.

- "Notas de versão do Cloud Volumes ONTAP 9,7"
- "Notas de versão do Cloud Volumes ONTAP 9,6"

Cloud Manager 3.8.1 (2 de fevereiro de 2020)

- Melhorias de conformidade com a nuvem
- Melhorias nas contas e assinaturas
- Melhorias na linha do tempo

Melhorias de conformidade com a nuvem

As melhorias a seguir estão agora disponíveis para o Cloud Compliance.

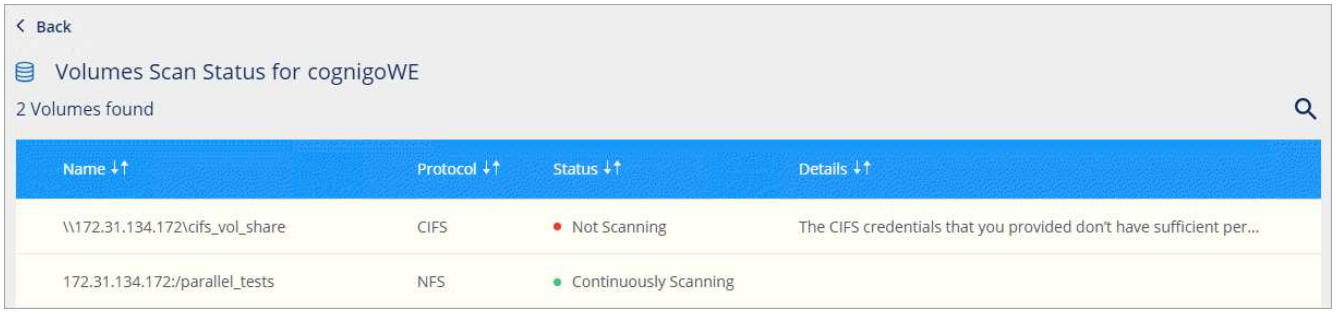
- **Suporte para Azure NetApp Files**

  Temos o prazer de anunciar que o Cloud Compliance agora pode verificar o Azure NetApp Files para identificar dados pessoais e confidenciais que residem nos volumes.

  "Saiba como começar".

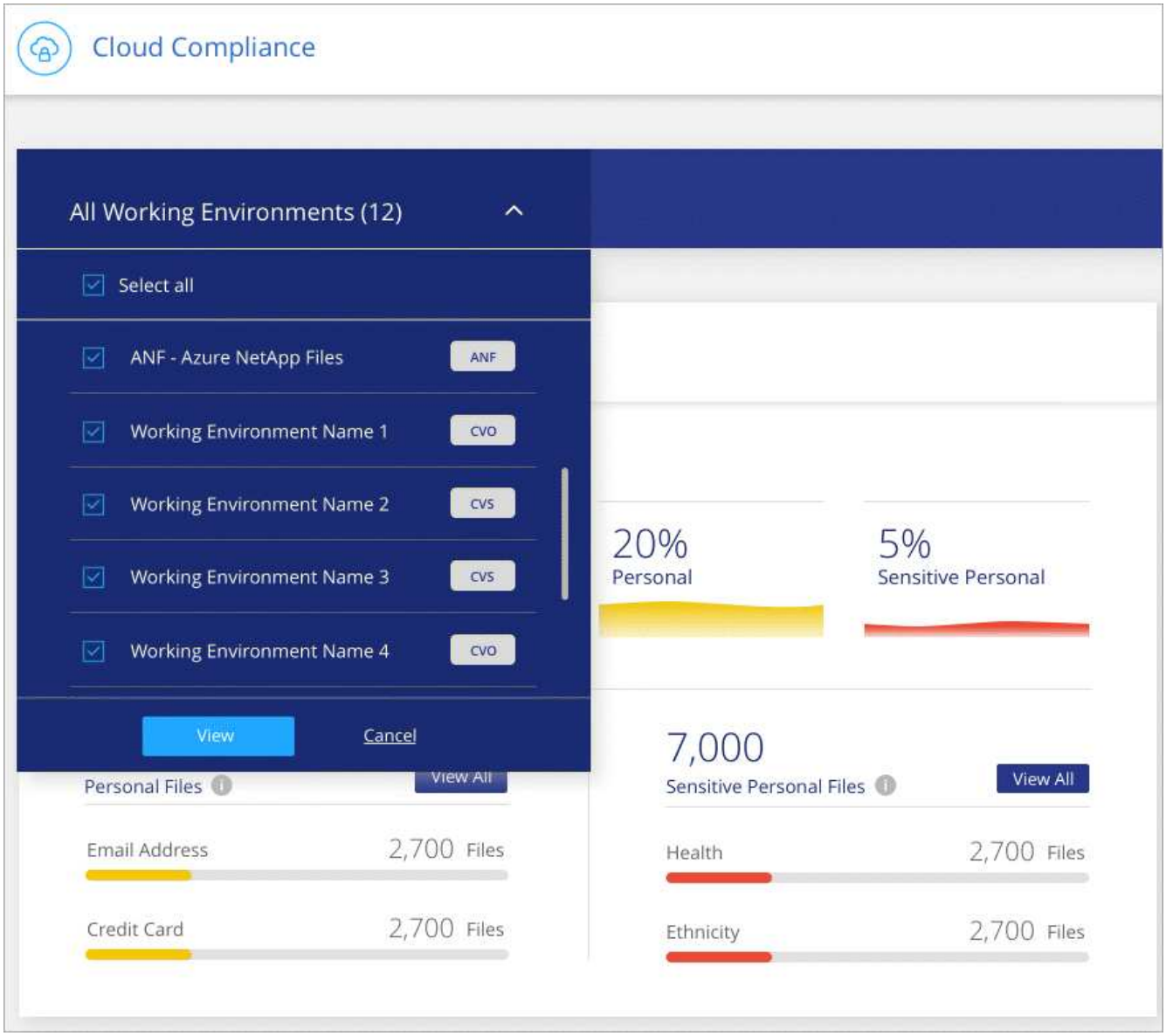
- **Estado de digitalização**

  O Cloud Compliance agora mostra um status de verificação para cada volume CIFS e NFS, incluindo mensagens de erro que podem ser usadas para corrigir quaisquer problemas.



- * Filtro de painel por ambiente de trabalho *

  Agora você pode filtrar o conteúdo do painel do Cloud Compliance para ver os dados de conformidade para ambientes de trabalho específicos.



- **Novo tipo de dados pessoais**

  O Cloud Compliance agora pode identificar uma Licença de motorista da Califórnia ao digitalizar dados.

- **Suporte para categorias adicionais**

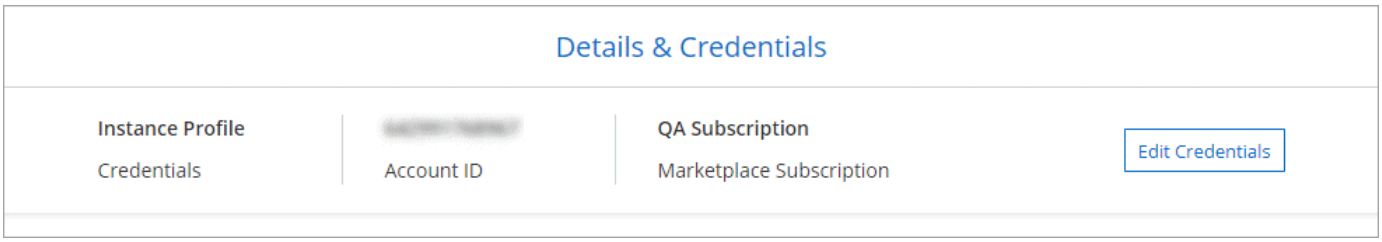
  São suportadas três categorias adicionais: Dados de aplicações, registos e ficheiros de base de dados e índice.

  "Saiba mais sobre categorias".

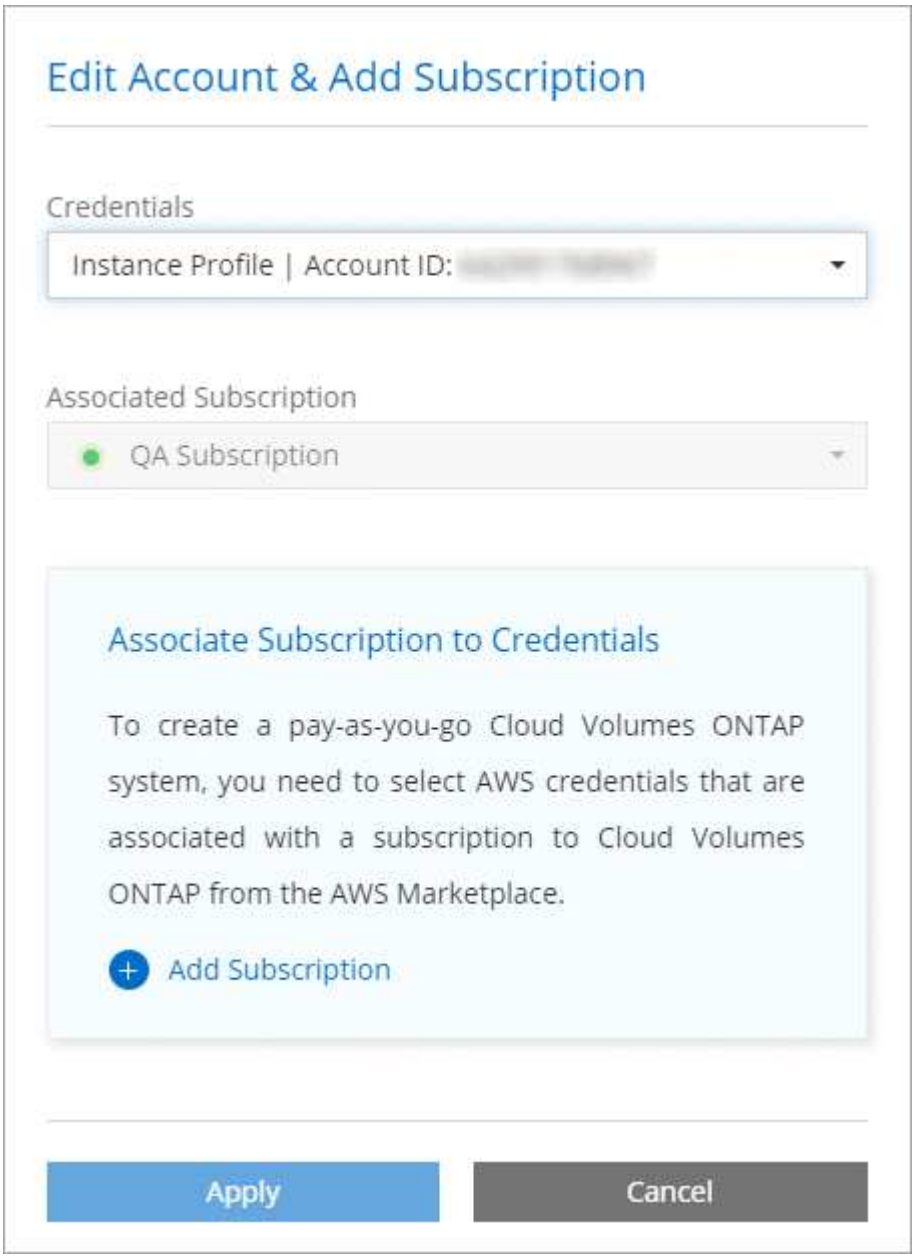
Melhorias nas contas e assinaturas

Facilitamos a seleção de uma conta da AWS ou de um projeto do GCP e de uma assinatura associada ao mercado para um sistema Cloud Volumes ONTAP de pagamento conforme o uso. Essas melhorias ajudam a garantir que você está pagando a partir da conta ou projeto certo.

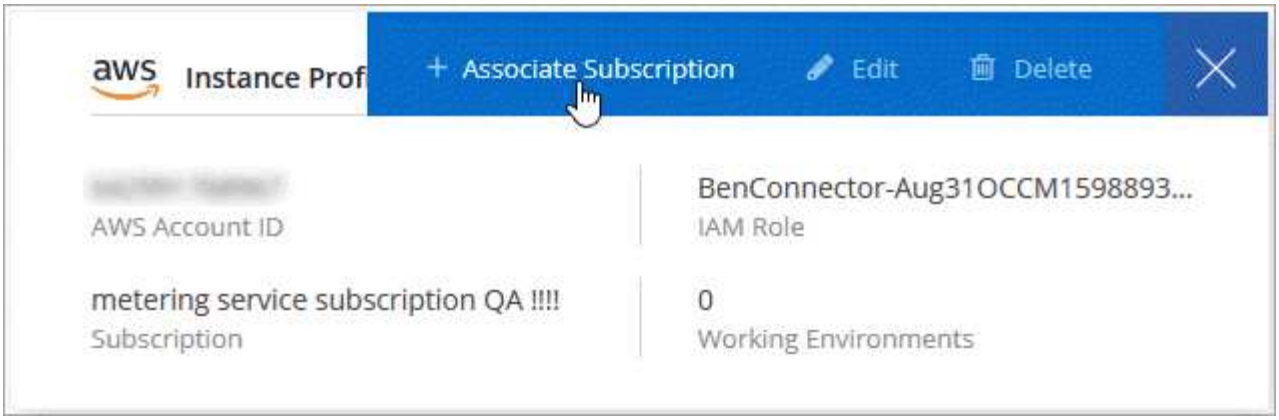
Por exemplo, quando você cria um sistema na AWS, clique em **Editar credenciais** se não quiser usar a conta e a assinatura padrão:



A partir daí, você pode escolher as credenciais da conta que deseja usar e a assinatura associada do AWS Marketplace. Você pode até mesmo adicionar uma assinatura de mercado, se necessário.



E se você gerenciar várias assinaturas da AWS, poderá atribuir cada uma delas a diferentes credenciais da AWS na página credenciais nas configurações:

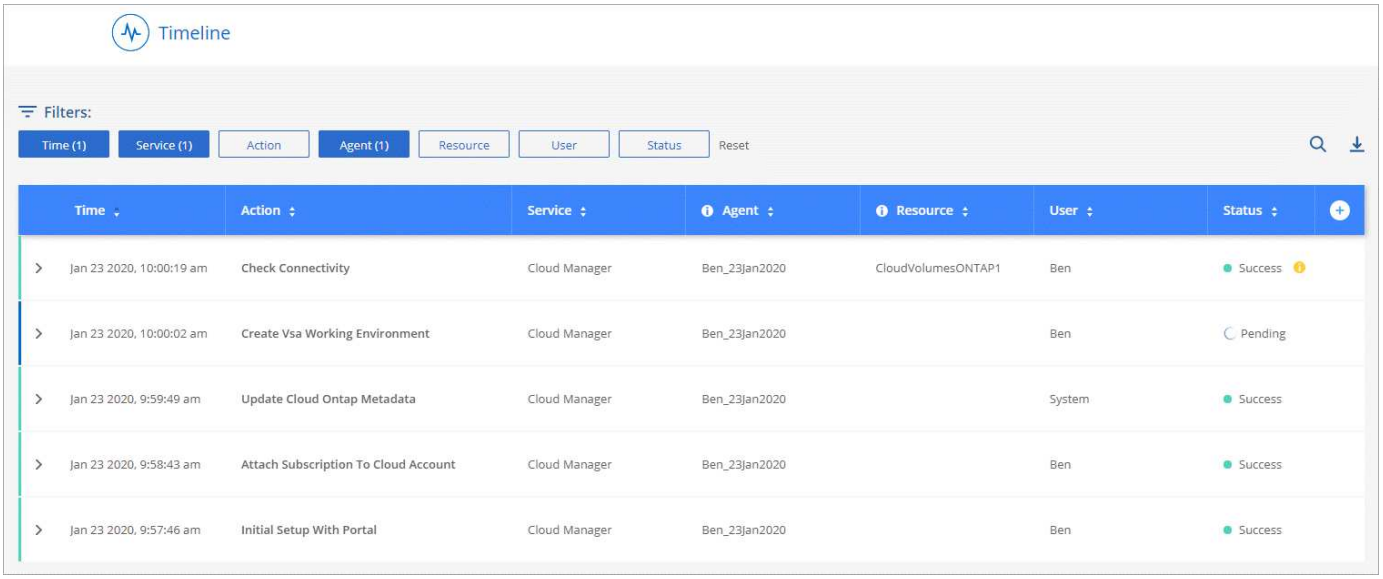


"Saiba como gerenciar credenciais da AWS no Cloud Manager".

Melhorias na linha do tempo

A linha do tempo foi aprimorada para fornecer mais informações sobre os serviços de nuvem da NetApp que você usa.

- A linha de tempo agora mostra ações para todos os sistemas do Cloud Manager dentro da mesma conta do Cloud Central
- Agora você pode encontrar informações mais facilmente filtrando, pesquisando e adicionando e removendo colunas
- Agora você pode baixar os dados da linha do tempo em formato CSV
- No futuro, a linha do tempo mostrará ações para cada serviço de nuvem do NetApp que você usar (mas você pode filtrar as informações para um único serviço)



Cloud Manager 3,8 (8 de janeiro de 2020)

- Aprimoramentos DE HA no Azure
- Melhorias na disposição de dados em categorias no GCP

Aprimoramentos DE HA no Azure

As melhorias a seguir estão agora disponíveis para pares de HA do Cloud Volumes ONTAP no Azure.

- **Substituir bloqueios CIFS para o Cloud Volumes ONTAP HA no Azure**

  Agora você pode habilitar uma configuração no Cloud Manager que impede problemas com o failover de storage do Cloud Volumes ONTAP durante eventos de manutenção do Azure. Quando você ativa essa configuração, o Cloud Volumes ONTAP veta o CIFS bloqueia e redefine as sessões ativas do CIFS. "Saiba mais".

- **Ligação HTTPS do Cloud Volumes ONTAP para contas de armazenamento**

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

- **Suporte para contas de armazenamento v2 de uso geral do Azure**

  As contas de storage criadas pelo Cloud Manager para pares de HA do Cloud Volumes ONTAP 9,7 agora são contas de storage do v2 de uso geral.

Melhorias na disposição de dados em categorias no GCP

Os aprimoramentos a seguir estão disponíveis para disposição de dados em categorias do Cloud Volumes ONTAP no GCP.

- * Classes de armazenamento do Google Cloud para categorização de dados*

  Agora, você pode escolher uma classe de storage para os dados que o Cloud Volumes ONTAP dispõe para o Google Cloud Storage:

  - Armazenamento padrão (padrão)
  - Armazenamento Nearline
  - Storage Coldline

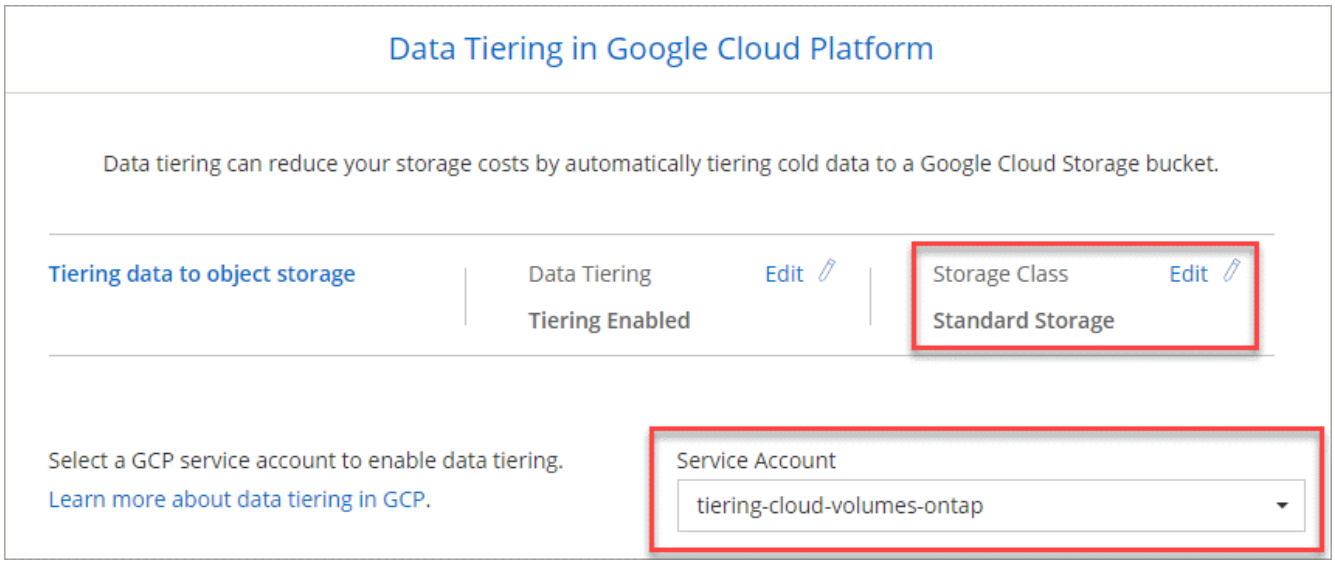
    "Saiba mais sobre as classes de armazenamento do Google Cloud".

  "Saiba como alterar a classe de armazenamento para Cloud Volumes ONTAP".

- **Disposição em camadas de dados usando uma conta de serviço**

  A partir da versão 9,7, o Cloud Manager agora define uma conta de serviço na instância do Cloud Volumes ONTAP. Essa conta de serviço fornece permissões para categorização de dados em um bucket do Google Cloud Storage. Esta alteração fornece mais segurança e requer menos configuração. Para obter instruções passo a passo ao implantar um novo sistema"consulte o passo 4 nesta página", .

  A imagem a seguir mostra o assistente ambiente de trabalho onde você pode selecionar uma classe de armazenamento e uma conta de serviço:



O Cloud Manager requer as seguintes permissões do GCP para esses aprimoramentos, como mostrado na última "Política do Cloud Manager para GCP".

```
- storage.buckets.update
- compute.instances.setServiceAccount
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
```

Transição do Cloud Manager para SaaS

Introduzimos uma experiência de software como serviço para o Cloud Manager. Essa nova experiência facilita o uso do Cloud Manager e nos permite fornecer recursos adicionais para gerenciar sua infraestrutura de nuvem híbrida.

A experiência anterior do Cloud Manager

O software Cloud Manager anteriormente era composto por uma interface de usuário e uma camada de gerenciamento que enviava solicitações para provedores de nuvem. Para começar, você implantaria o Cloud Manager em sua rede na nuvem ou na rede local e, em seguida, acessaria a interface de usuário executada nessa instância.

Essa experiência mudou.

A nova experiência SaaS

A interface do Cloud Manager agora está acessível por meio de uma interface de usuário baseada em SaaS à qual você faz login a partir do NetApp. Você não precisa mais acessar uma interface de usuário a partir de um software executado em sua rede.

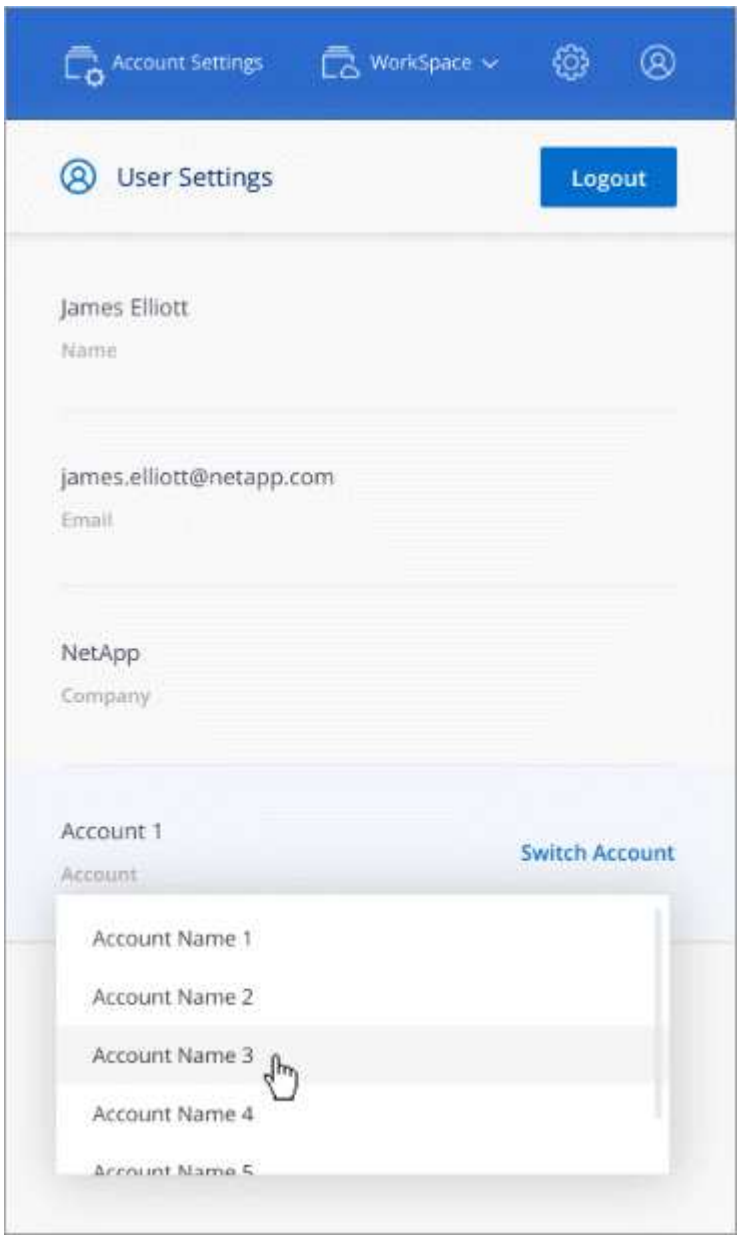
Na maioria dos casos, você precisa implantar um *Connector* em sua nuvem ou rede local. O conetor é um software necessário para gerenciar o Cloud Volumes ONTAP e outros serviços de dados em nuvem. (Na verdade, o conetor é o mesmo que o software existente do Cloud Manager instalado.)

Benefícios

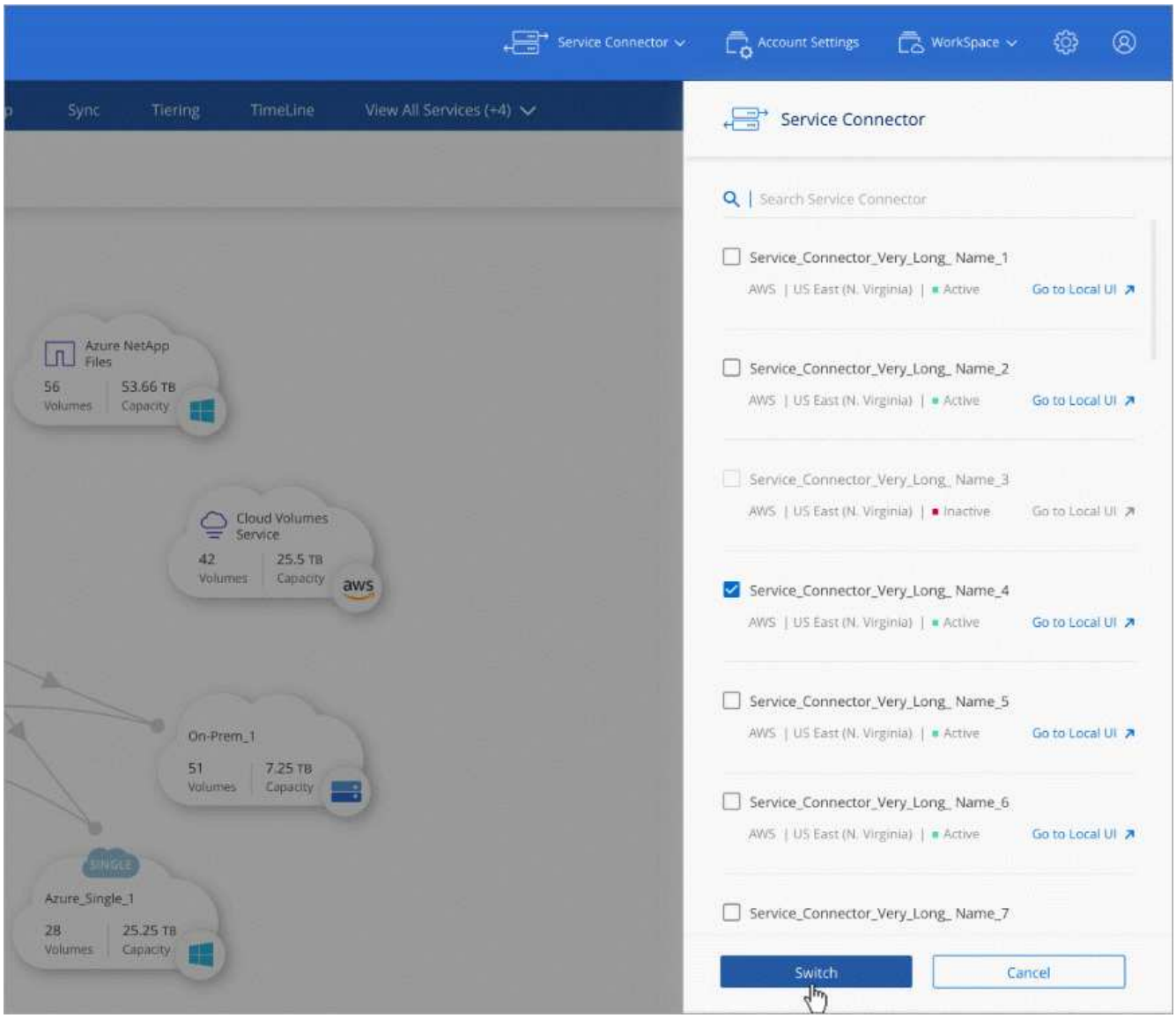
Essa abordagem baseada em SaaS oferece vários benefícios:

- Com ele, oferecemos recursos de gerenciamento adicionais para Azure NetApp Files e Cloud Volumes Service sem a necessidade de implantar software no seu ambiente.
- Você pode alternar facilmente entre suas contas do Cloud Central.

  Se um usuário estiver associado a várias contas do Cloud Central, ele poderá mudar para uma conta diferente a qualquer momento no menu Configurações do usuário. Em seguida, eles podem ver os conetores e os ambientes de trabalho associados a essa conta.



- Você pode alternar facilmente entre conetores (o que você sabe hoje como o software Cloud Manager) que são instalados em diferentes redes ou diferentes provedores de nuvem.

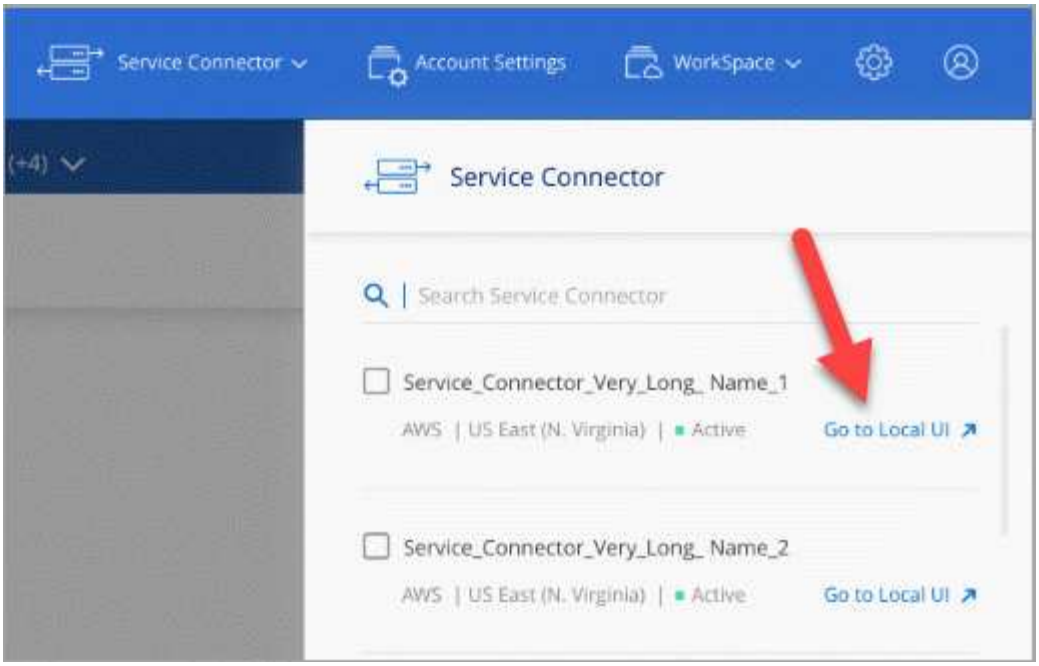


A interface do utilizador local

Embora você deva executar quase todas as tarefas a partir da interface de usuário SaaS, uma interface de usuário local ainda está disponível no conetor. Esta interface é necessária para algumas tarefas que precisam ser executadas a partir do próprio conetor:

- Configurando um servidor proxy
- Instalando um patch
- A transferir mensagens AutoSupport

Você pode acessar a interface de usuário local diretamente da interface de usuário SaaS:



Alterações de instância, VM e tipo de máquina

Para garantir que os recursos adequados estejam disponíveis para novos e futuros recursos no Cloud Manager, alteramos o mínimo necessário de instância, VM e tipo de máquina da seguinte forma:

- AWS: t3.xlarge
- Azure: DS3 v2
- GCP: N1-standard-4

Ao atualizar o tipo de máquina, você terá acesso a recursos como uma nova experiência do Kubernetes, Global File Cache, Monitoramento e muito mais.

Esses tamanhos padrão são o mínimo "Com base nos requisitos de CPU e RAM"suportado .

O Cloud Manager solicitará instruções para alterar o tipo de máquina do conetor.

Problemas conhecidos

Problemas conhecidos identificam problemas que podem impedi-lo de usar esta versão do produto com sucesso.

Não há problemas conhecidos nesta versão do Cloud Manager.

Você pode encontrar problemas conhecidos para o Cloud Volumes ONTAP no "Notas de versão do Cloud Volumes ONTAP" e para o software ONTAP em geral no "Notas de versão do ONTAP".

Limitações conhecidas

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

Os conetores devem permanecer em funcionamento

Um conetor deve permanecer sempre em funcionamento. É importante para a saúde e operação contínuas dos serviços que você habilitar.

Por exemplo, um conetor é um componente chave na integridade e operação dos sistemas Cloud Volumes ONTAP PAYGO. Se um conetor for desligado, os sistemas Cloud Volumes ONTAP PAYGO desligarão após perder a comunicação com um conetor por mais de 14 dias.

A plataforma SaaS está desativada para regiões do governo

Se você implantar um conetor em uma região do AWS GovCloud, uma região do Azure Gov ou uma região do Azure DoD, o acesso ao Cloud Manager estará disponível somente por meio do endereço IP do host de um conetor. O acesso à plataforma SaaS está desativado para toda a conta.

Isso significa que somente usuários privilegiados que podem acessar a VPC/VNet interna do usuário final podem usar a IU ou API do Cloud Manager.

Isso também significa que os seguintes serviços não estão disponíveis no Cloud Manager:

- Conformidade com a nuvem
- Kubernetes
- Disposição em camadas na nuvem
- Cache de arquivos global
- Monitoramento (Cloud Insights)

A plataforma SaaS é necessária para usar esses serviços.

Hosts Linux compartilhados não são suportados

O conetor não é suportado em um host que é compartilhado com outros aplicativos. O host deve ser um host dedicado.

O Cloud Manager não é compatível com o FlexGroup volumes

Embora o Cloud Volumes ONTAP ofereça suporte ao FlexGroup volumes, o Cloud Manager não oferece. Se você criar um volume do FlexGroup a partir do Gerenciador do sistema ou da CLI, defina o modo de gerenciamento de capacidade do Cloud Manager como Manual. O modo automático pode não funcionar corretamente com volumes FlexGroup.

Mudanças importantes no Cloud Manager

Esta página destaca mudanças importantes no Cloud Manager que podem ajudá-lo a usar o serviço à medida que introduzimos novos aprimoramentos. Você deve continuar lendo "O que há de novo"a página para saber mais sobre todos os novos recursos e aprimoramentos.

Alterações de SaaS

Introduzimos uma experiência de software como serviço no Cloud Manager. Essa nova experiência facilita o uso do Cloud Manager e nos permite fornecer recursos adicionais para gerenciar sua infraestrutura de nuvem híbrida.

- "Transição do Cloud Manager para SaaS"
- "Saiba como o Cloud Manager funciona"

Alterações do tipo de máquina

Para garantir que os recursos adequados estejam disponíveis para novos e futuros recursos no Cloud Manager, alteramos o mínimo necessário de instância, VM e tipo de máquina da seguinte forma:

- AWS: t3.xlarge
- Azure: DS3 v2
- GCP: N1-standard-4

Ao atualizar o tipo de máquina, você terá acesso a recursos como uma nova experiência do Kubernetes, Global File Cache, Monitoramento e muito mais.

Esses tamanhos padrão são o mínimo "Com base nos requisitos de CPU e RAM"suportado .

O Cloud Manager solicitará instruções para alterar o tipo de máquina do conetor.

Definições de conta

Introduzimos as contas do Cloud Central para fornecer alocação a vários clientes, para ajudá-lo a organizar usuários e recursos em espaços de trabalho isolados e gerenciar o acesso a conetores e assinaturas.

- "Saiba mais sobre as contas do Cloud Central: Usuários, workspaces, conetores e assinaturas"
- "Saiba como começar a usar sua conta"
- "Saiba como gerenciar sua conta depois de configurá-la"

Novas permissões

O Cloud Manager ocasionalmente requer permissões adicionais de provedores de nuvem à medida que introduzimos novos recursos e melhorias. Esta seção identifica novas permissões que agora são necessárias.

Pode encontrar a lista mais recente de permissões no "Página de políticas do Cloud Manager".

AWS

A partir da versão 3.8.1, as permissões a seguir são necessárias para usar o backup na nuvem com o Cloud Volumes ONTAP. "Saiba mais".

```
{
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
            ]
        },
```

Azure

- Para evitar falhas de implantação do Azure, certifique-se de que sua política do Cloud Manager no Azure inclua a seguinte permissão:

```
"Microsoft.Resources/deployments/operationStatuses/read"
```

- A partir da versão 3.8.7, a seguinte permissão é necessária para criptografar discos gerenciados do Azure em sistemas Cloud Volumes ONTAP de nó único usando chaves externas de outra conta. "Saiba mais".

```
"Microsoft.Compute/diskEncryptionSets/read"
```

- As permissões a seguir são necessárias para habilitar o cache de arquivos global no Cloud Volumes ONTAP. "Saiba mais".

```
"Microsoft.Resources/deployments/operationStatuses/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/delete",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
```

GCP

Novas permissões para gerenciamento do Kubernetes

A partir da versão 3.8.8, a conta de serviço de um conetor requer as seguintes permissões para descobrir e gerenciar clusters do Kubernetes executados no Google Kubernetes Engine (GKE):

```
- container.*
```

Novas permissões para categorização de dados

A partir da versão 3,8, as permissões a seguir são necessárias para usar uma conta de serviço para categorização de dados. "Saiba mais".

```
- storage.buckets.update
- compute.instances.setServiceAccount
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
```

Novos endpoints

O conetor requer acesso de saída à Internet para gerenciar recursos e processos em seu ambiente de nuvem pública. Esta seção identifica novos endpoints que agora são necessários.

Pode encontrar o "lista completa de endpoints acessados a partir do seu navegador da web aqui" e o "Lista completa de endpoints acessados pelo conetor aqui".

- Os usuários precisam acessar o Cloud Manager a partir de um navegador da Web entrando em Contato com o seguinte endpoint:

  https://cloudmanager.NetApp.com

- Os conetores exigem acesso ao seguinte ponto final para obter imagens de software de componentes de contentor para uma infra-estrutura Docker:

  https://cloudmanagerinfraprod.azurecr.io

Certifique-se de que o firewall permite o acesso a este ponto final a partir do conetor.

Comece a usar o Cloud Manager

Saiba mais sobre o Cloud Manager

O Cloud Manager permite que especialistas DE TI e arquitetos de nuvem gerenciem centralmente sua infraestrutura multicloud híbrida usando as soluções de nuvem da NetApp.

Caraterísticas

O Cloud Manager é uma plataforma de gerenciamento de classe empresarial baseada em SaaS que mantém você no controle dos seus dados, onde quer que eles estejam.

- Configure e use "Cloud Volumes ONTAP" para um gerenciamento de dados eficiente em vários protocolos nas nuvens.
- Configurar e utilizar serviços de armazenamento de ficheiros: "Azure NetApp Files", , "Cloud Volumes Service para AWS" E "Cloud Volumes Service para Google Cloud".
- Descubra e gerencie clusters do ONTAP locais criando volumes, fazendo backup na nuvem, replicando dados na nuvem híbrida e dispondo dados pouco acessados em categorias na nuvem.
- Habilite serviços de nuvem e software integrados, como "Conformidade com a nuvem", "Cloud Insights", "Cloud Backup Service", "Trident"e muito mais.

"Saiba mais sobre o Cloud Manager".

Fornecedores de storage de objetos compatíveis

O Cloud Manager permite gerenciar o storage de nuvem e usar serviços de nuvem na Amazon Web Services, Microsoft Azure e Google Cloud.

Custo

O software Cloud Manager é gratuito da NetApp.

Para a maioria das tarefas, o Cloud Manager solicita que você implante um conetor em sua rede de nuvem, o que resulta em cobranças do seu provedor de nuvem para a instância de computação e o armazenamento associado. Você tem a opção de executar o software Connector em suas instalações.

Como o Cloud Manager funciona

O Cloud Manager inclui uma interface baseada em SaaS integrada ao NetApp Cloud Central e conetores que gerenciam o Cloud Volumes ONTAP e outros serviços de nuvem.

Software como serviço

O Cloud Manager pode ser acessado por meio das APIs a "Interface de usuário baseada em SaaS" e. Essa experiência SaaS permite que você acesse automaticamente os recursos mais recentes à medida que são lançados e alterne facilmente entre suas contas e conetores do Cloud Central.

Centro de nuvem da NetApp

"Centro de nuvem da NetApp" fornece um local centralizado para acessar e "Serviços de nuvem da NetApp" gerenciar o . Com a autenticação de usuário centralizada, você pode usar o mesmo conjunto de credenciais

para acessar o Cloud Manager e outros serviços de nuvem, como o Cloud Insights.

Ao fazer login no Cloud Manager pela primeira vez, você será solicitado a criar uma conta *Cloud Central*. Essa conta fornece alocação a vários clientes e permite organizar usuários e recursos em *workspaces* isolados.

Conetores

Na maioria dos casos, um administrador de conta precisará implantar um *Connector* na sua nuvem ou na rede local. O conetor permite que o Cloud Manager gerencie recursos e processos em seu ambiente de nuvem pública.

Um conetor deve permanecer sempre em funcionamento. É importante para a saúde e operação contínuas dos serviços que você habilitar.

Por exemplo, um conetor é um componente chave na integridade e operação dos sistemas Cloud Volumes ONTAP PAYGO. Se um conetor for desligado, os sistemas Cloud Volumes ONTAP PAYGO desligarão após perder a comunicação com um conetor por mais de 14 dias.

"Saiba mais sobre quando os conetores são necessários e como funcionam".

Visão geral da rede

Antes que os usuários façam login no Cloud Manager, você precisará garantir que seus navegadores da Web possam acessar endpoints específicos. Depois disso, você precisa verificar os requisitos de rede para o tipo específico de ambiente de trabalho e serviços que serão usados.

Endpoints acessados a partir do seu navegador da Web

Os usuários devem acessar o Cloud Manager a partir de um navegador da Web. A máquina que executa o navegador da Web deve ter conexões com os seguintes endpoints:

Endpoints	Finalidade
https://cloudmanager.cloud.NetApp.com	Para conectá-lo à interface SaaS do Cloud Manager.
https://api.services.cloud.NetApp.com	Para entrar em Contato com as APIs do Cloud Central.
https://auth0.com https://cdn.auth0.com://NetApp-cloud-account.auth0.com https://services.cloud.NetApp.com	Seu navegador da Web se coneta a esses endpoints para autenticação de usuário centralizada por meio do NetApp Cloud Central.
https://widget.intercom.io	Para um bate-papo no produto que permite conversar com especialistas em nuvem da NetApp.

Índice de requisitos de rede

- "Conetores"
- "Cloud Volumes ONTAP para AWS"
- "Cloud Volumes ONTAP para Azure"
- "Cloud Volumes ONTAP para GCP"

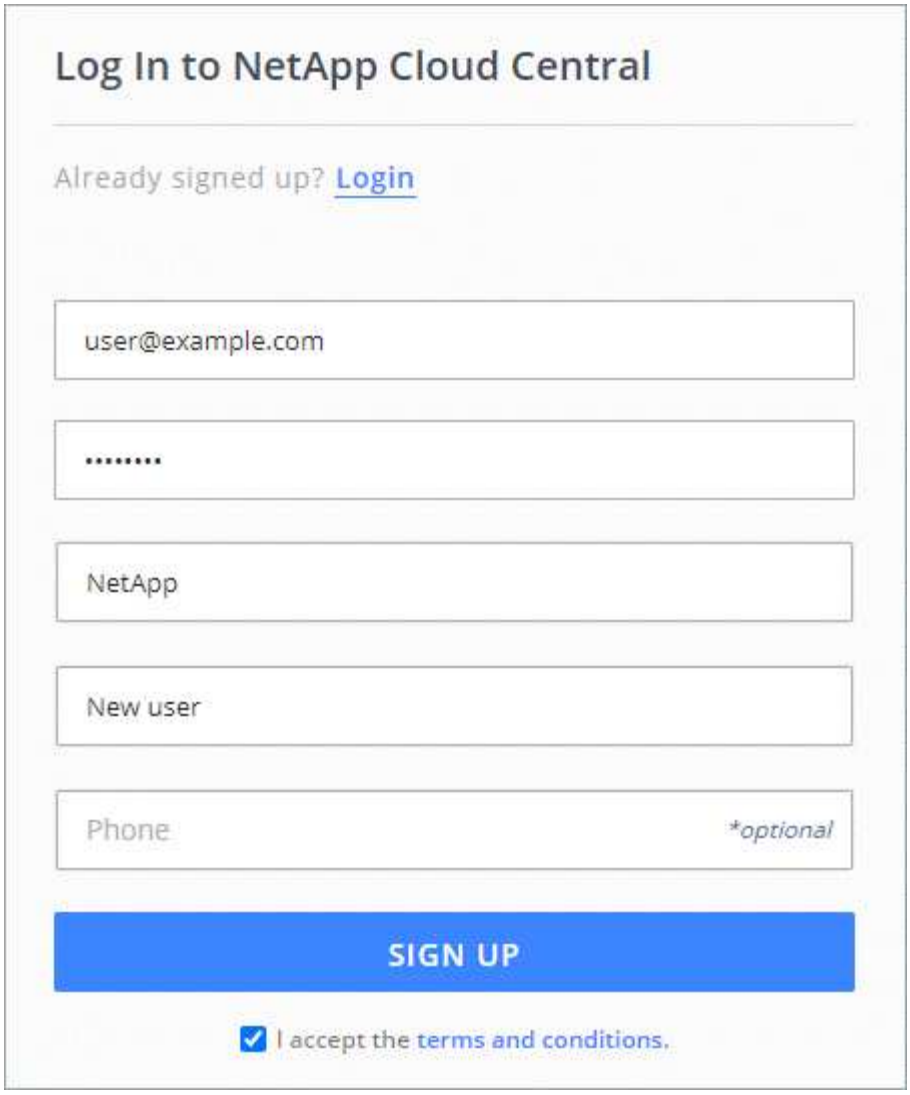
- "Replicação de dados entre sistemas ONTAP"
- "Cloud Compliance para Cloud Volumes ONTAP ou Azure NetApp Files"
- "Conformidade com a nuvem para Amazon S3"
- "Clusters ONTAP no local"
  - "Disposição de dados em camadas dos clusters do ONTAP para o Amazon S3"
  - "Disposição de dados em camadas dos clusters do ONTAP para o storage Azure Blob"
  - "Disposição de dados em camadas dos clusters do ONTAP para o Google Cloud Storage"
  - "Disposição de dados em camadas dos clusters do ONTAP para o StorageGRID"

Inscreva-se no NetApp Cloud Central

Inscreva-se no NetApp Cloud Central para que você possa acessar os serviços de nuvem da NetApp.

Passos

1. Abra um navegador da Web e vá para "Centro de nuvem da NetApp".
2. Clique em **Inscrever-se**.
3. Preencha o formulário e clique em **Inscrever-se**.



4. Aguarde um e-mail do NetApp Cloud Central.
5. Clique no link no e-mail para verificar seu endereço de e-mail.

Resultado

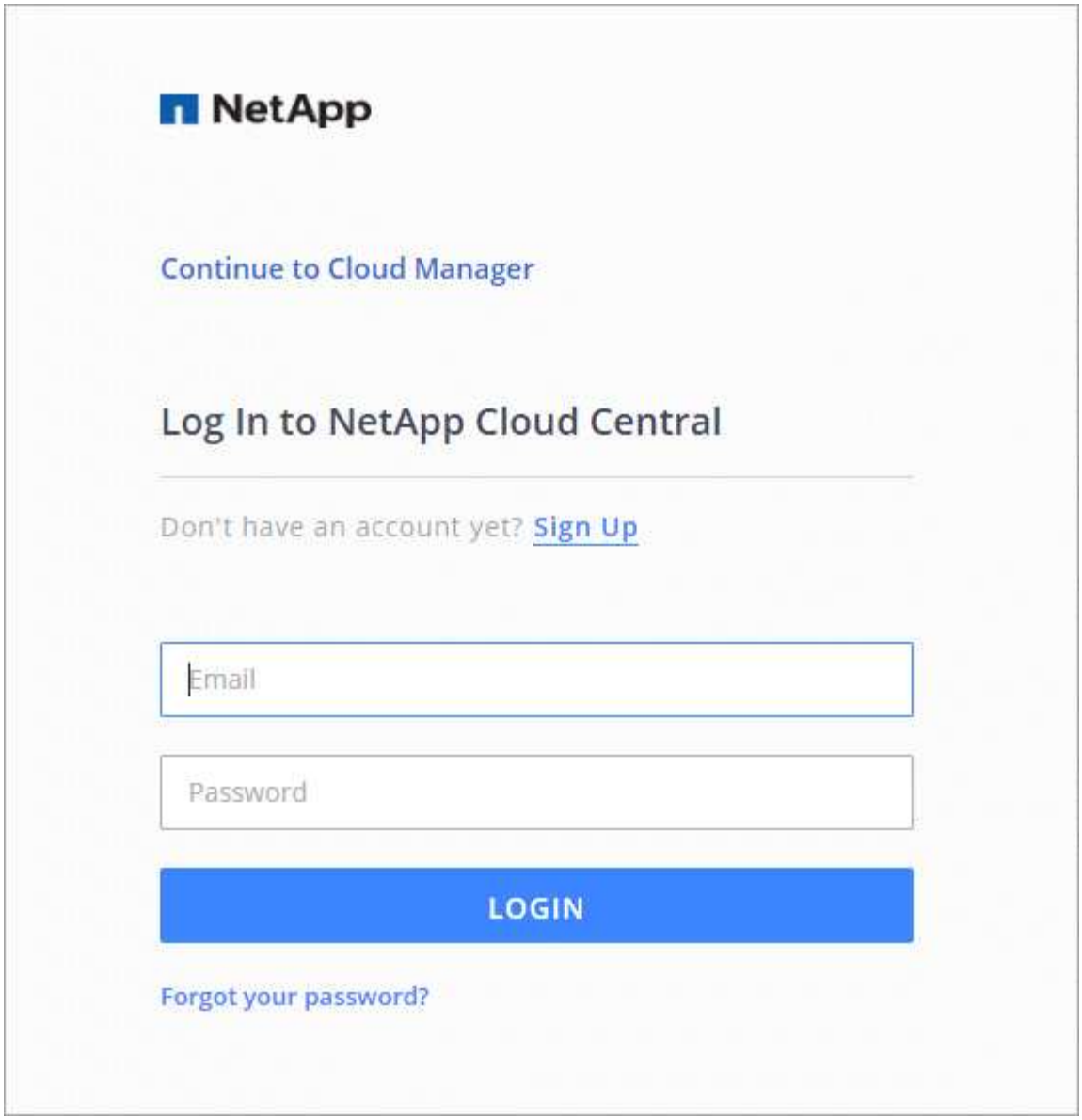
Agora você tem um login de usuário ativo do Cloud Central.

Iniciar sessão no Cloud Manager

A interface do Cloud Manager pode ser acessada por meio de uma interface de usuário baseada em SaaS acessando https://cloudmanager.netapp.com .

Passos

1. Abra um navegador da Web e vá para https://cloudmanager.netapp.com.
2. Faça login usando suas credenciais do NetApp Cloud Central.



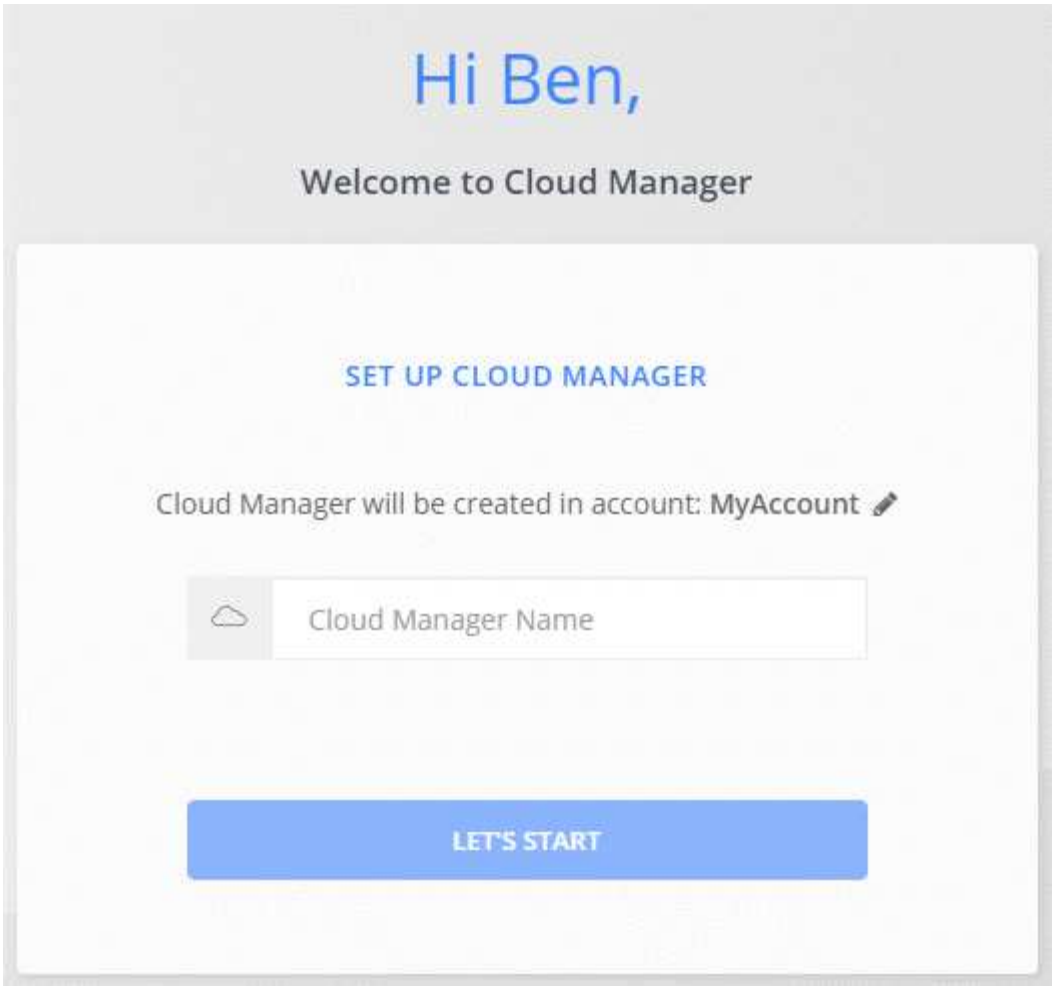
Configure uma conta do Cloud Central

Configurações de conta: Usuários, workspaces, conetores e assinaturas

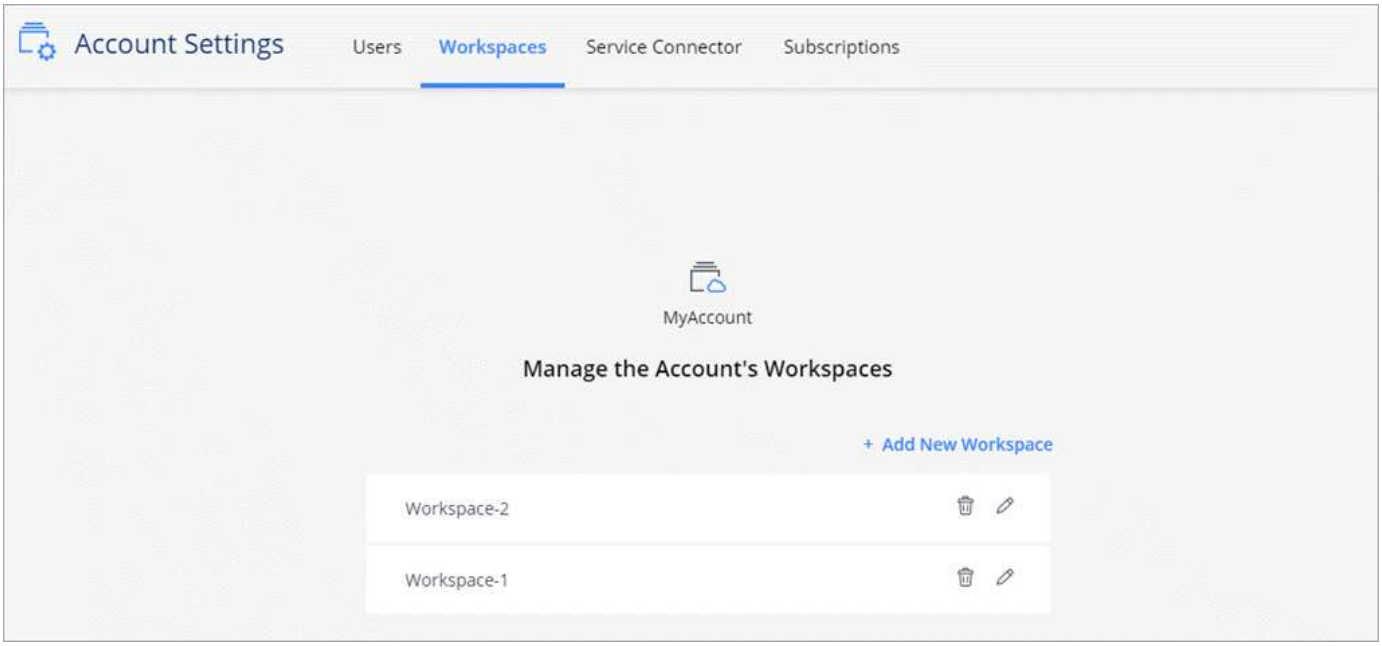
Uma conta *Cloud Central* fornece alocação a vários clientes e permite organizar usuários e recursos em espaços de trabalho isolados a partir do Cloud Manager.

Por exemplo, vários usuários podem implantar e gerenciar sistemas Cloud Volumes ONTAP em ambientes isolados chamados *workspaces*. Esses espaços de trabalho são invisíveis para outros usuários, a menos que sejam compartilhados.

Quando você acessa o Cloud Manager pela primeira vez, será solicitado a selecionar ou criar uma conta do Cloud Central:



Os administradores de conta podem modificar as configurações dessa conta gerenciando usuários, espaços de trabalho, conetores e assinaturas:



Para obter instruções passo a passo, "Configurando a conta do Cloud Central"consulte .

Definições de conta

O widget Configurações de conta no Cloud Manager permite que os administradores de conta gerenciem uma conta do Cloud Central. Se você acabou de criar sua conta, então você vai começar do zero. Mas se você já configurou uma conta, verá *todos* os usuários, espaços de trabalho, conetores e assinaturas associados à conta.

Usuários

Os usuários exibidos nas Configurações da conta são usuários do NetApp que você associa à sua conta do Cloud Central. Associar um usuário a uma conta e um ou mais espaços de trabalho nessa conta permite que esses usuários criem e gerenciem ambientes de trabalho no Cloud Manager.

Quando você associa um usuário, você atribui a ele uma função:

- *Account Admin*: Pode executar qualquer ação no Cloud Manager.
- *Workspace Admin*: Pode criar e gerenciar recursos na área de trabalho atribuída.
- *Visualizador de conformidade na nuvem*: Só pode visualizar informações de conformidade e gerar relatórios para sistemas que eles têm permissão para acessar.

Espaços de trabalho

No Cloud Manager, uma área de trabalho isola qualquer número de *ambientes de trabalho* de outros ambientes de trabalho. Os administradores do workspace não podem acessar os ambientes de trabalho em um workspace, a menos que o administrador da conta associe o administrador a esse workspace.

Um ambiente de trabalho representa um sistema de storage:

- Um sistema Cloud Volumes ONTAP de nó único ou um par de HA
- Um cluster ONTAP no local na sua rede
- Um cluster do ONTAP em uma configuração de storage privado do NetApp

Conetores

Um conetor permite que o Cloud Manager gerencie recursos e processos em seu ambiente de nuvem pública. O conetor é executado em uma instância de máquina virtual que você implanta em seu fornecedor de nuvem ou em um host local configurado.

Você pode usar um conector com mais de um serviço de dados de nuvem da NetApp. Por exemplo, se você já tiver um conetor para o Cloud Manager, poderá selecioná-lo quando configurar o serviço Cloud Tiering.

Subscrições

O widget Configurações de conta mostra as assinaturas do NetApp associadas à conta selecionada.

Quando você se inscreve no Cloud Manager no mercado de um provedor de nuvem, você é redirecionado para o Cloud Central, onde você precisa salvar sua assinatura e associá-la a contas específicas.

Depois de se inscrever, cada assinatura estará disponível no widget Configurações da conta. Você só verá as assinaturas associadas à conta que você está visualizando no momento.

Você tem a opção de renomear uma assinatura e desassociar a assinatura de uma ou mais contas.

Por exemplo, digamos que você tem duas contas e cada uma é cobrada através de assinaturas separadas. Você pode desassociar uma assinatura de uma das contas para que os usuários dessa conta não escolham acidentalmente a assinatura errada ao criar um ambiente de trabalho do Cloud volume ONTAP.

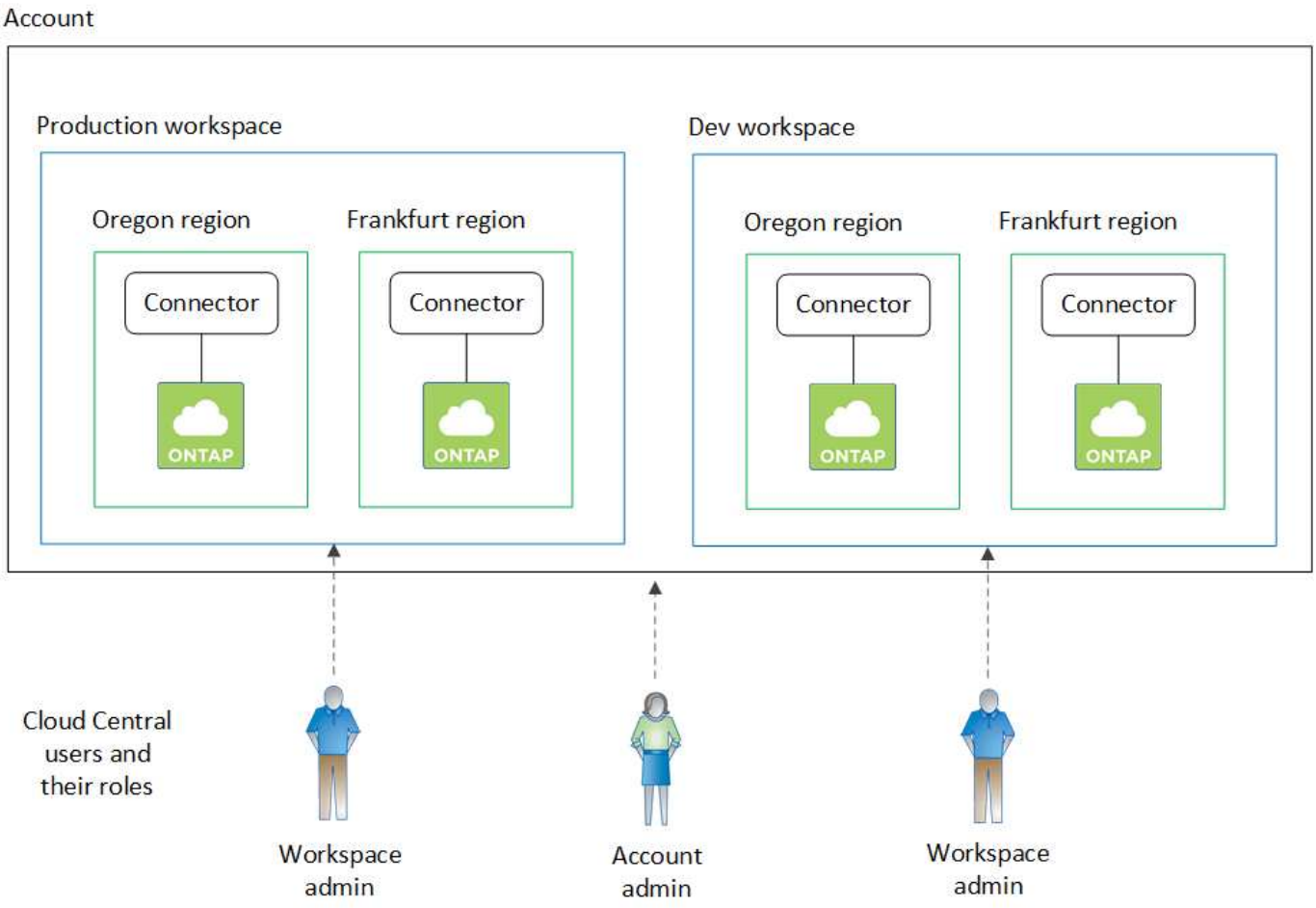
Exemplos

Os exemplos a seguir descrevem como você pode configurar suas contas.

> Em ambos os exemplos de imagens que se seguem, o conetor e os sistemas Cloud Volumes ONTAP não residem *in* a conta NetApp Central - eles estão sendo executados em um provedor de nuvem. Esta é uma representação conceitual da relação entre cada componente.

Exemplo 1

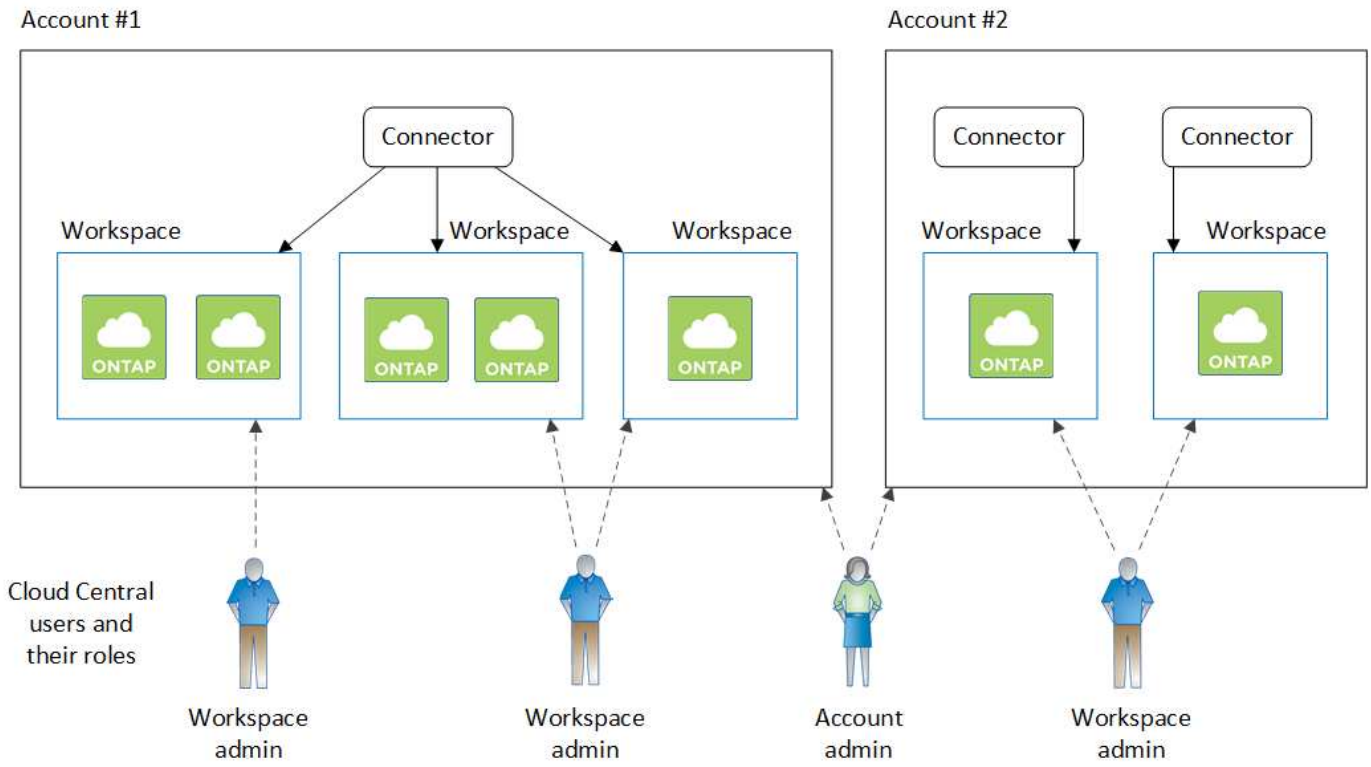
O exemplo a seguir mostra uma conta que usa dois espaços de trabalho para criar ambientes isolados. O primeiro espaço de trabalho é para um ambiente de produção e o segundo é para um ambiente de desenvolvimento.



Exemplo 2

Aqui está outro exemplo que mostra o mais alto nível de alocação a vários clientes usando duas contas separadas do Cloud Central. Por exemplo, um provedor de serviços pode usar o Cloud Manager em uma conta para fornecer serviços para seus clientes, enquanto usa outra conta para fornecer recuperação de desastres para uma de suas unidades de negócios.

Observe que a conta 2 inclui dois conetores separados. Isso pode acontecer se você tiver sistemas em regiões separadas ou em provedores de nuvem separados.



Configurando espaços de trabalho e usuários na conta do Cloud Central

Quando você faz login no Cloud Manager pela primeira vez, será solicitado que você crie uma conta *NetApp Cloud Central*. Essa conta fornece alocação a vários clientes e permite organizar usuários e recursos em *workspaces* isolados.

"Saiba mais sobre como as contas do Cloud Central funcionam".

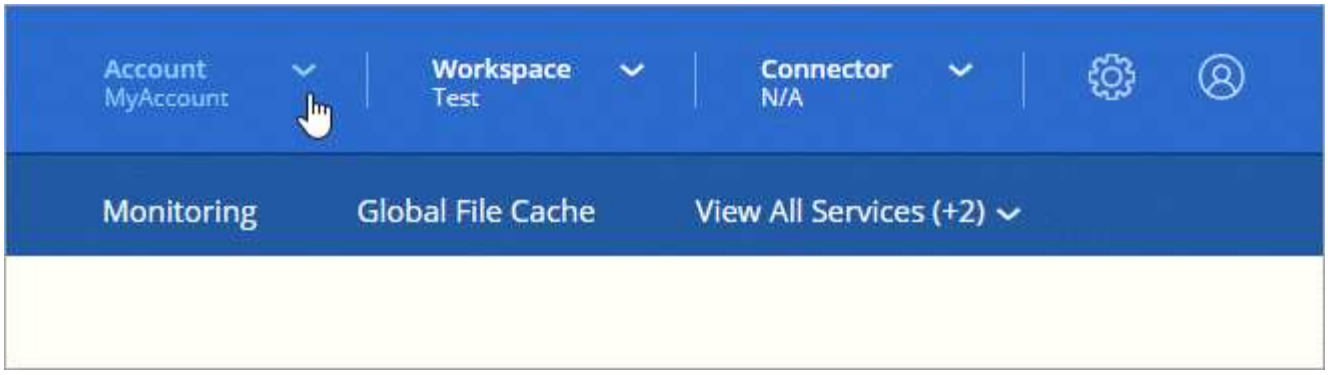
Configure sua conta do Cloud Central para que os usuários possam acessar o Cloud Manager e acessar os ambientes de trabalho em um workspace. Basta adicionar um único usuário ou adicionar vários usuários e workspaces.

Adicionar espaços de trabalho

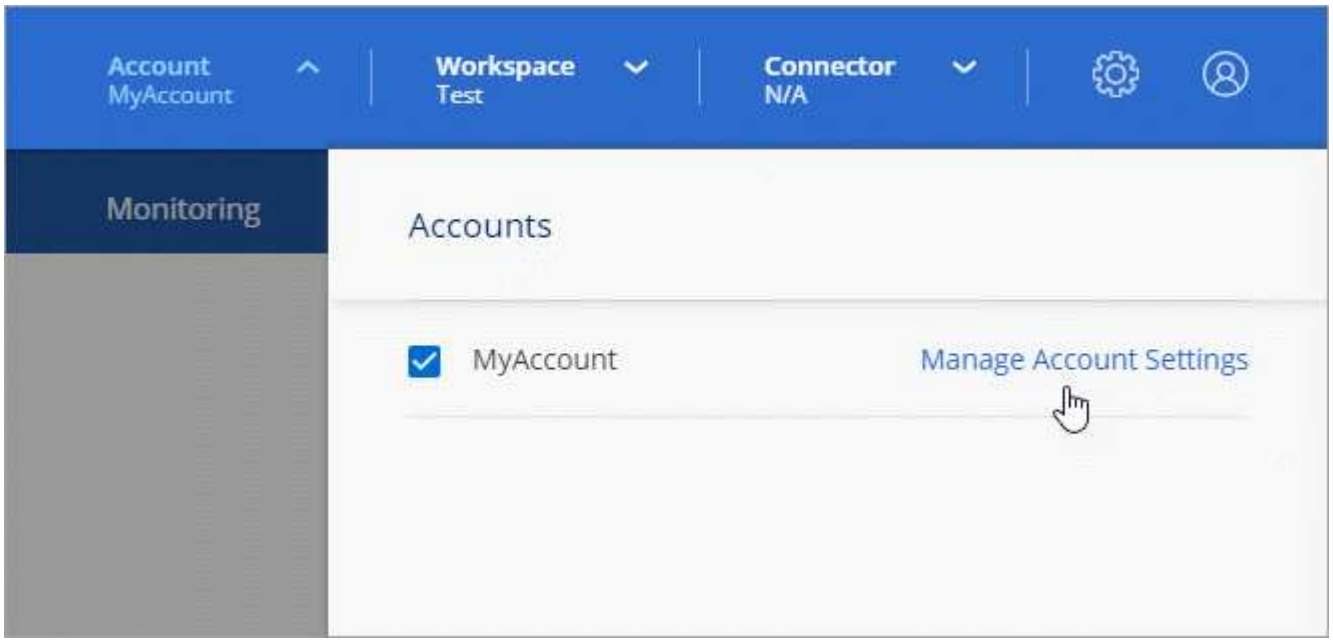
No Cloud Manager, os espaços de trabalho permitem isolar um conjunto de ambientes de trabalho de outros ambientes de trabalho e de outros usuários. Por exemplo, você pode criar dois espaços de trabalho e associar usuários separados a cada área de trabalho.

Passos

1. Na parte superior do Cloud Manager, clique no menu suspenso **Account**.



2. Clique em **Gerenciar conta** ao lado da conta selecionada no momento.



3. Clique em **Workspaces**.
4. Clique em **Adicionar novo espaço de trabalho**.
5. Insira um nome para o workspace e clique em **Add**.

Depois de terminar

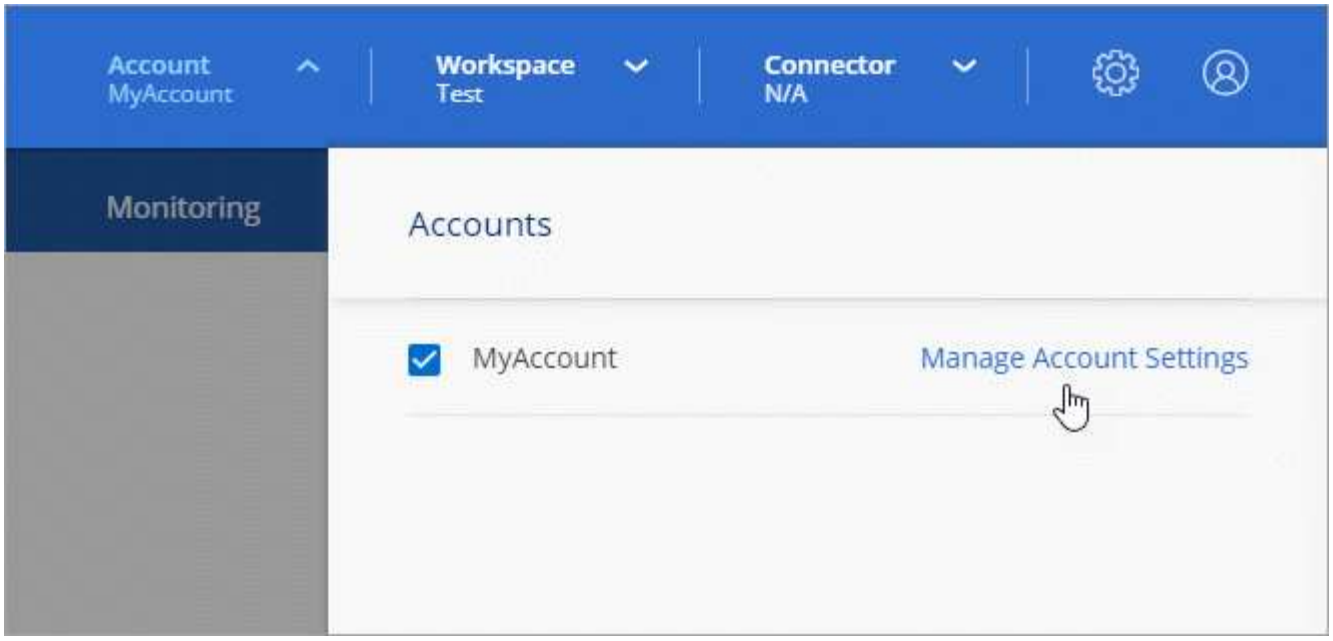
Se um administrador do espaço de trabalho precisar de acesso a essa área de trabalho, você precisará associar o usuário. Você também precisará associar conetores ao espaço de trabalho para que os administradores do Workspace possam usar esses conetores.

Adicionando usuários

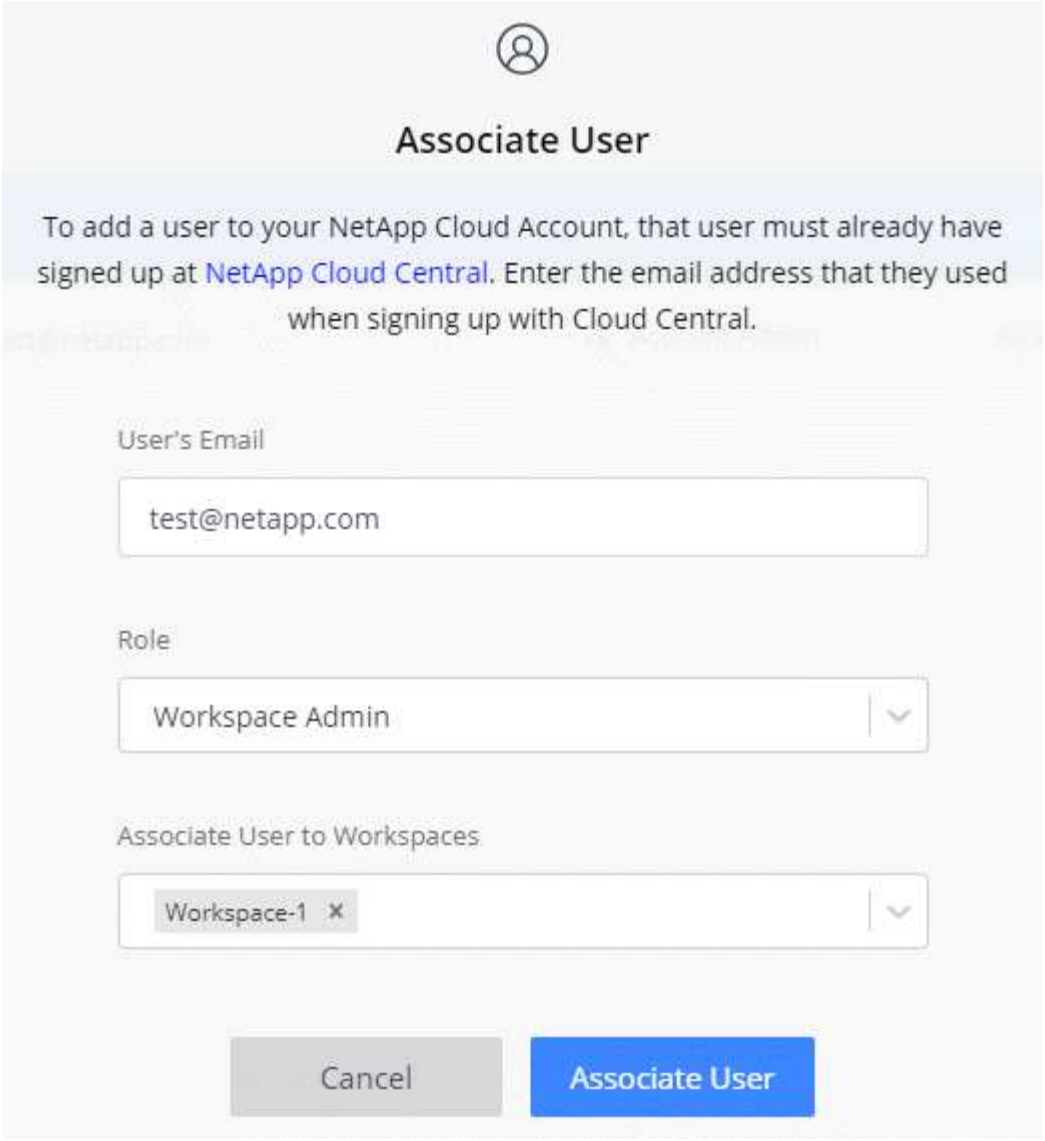
Associe usuários do Cloud Central à conta do Cloud Central para que esses usuários possam criar e gerenciar ambientes de trabalho no Cloud Manager.

Passos

1. Se o usuário ainda não tiver feito isso, peça ao usuário para ir "Centro de nuvem da NetApp" e se inscrever.
2. Na parte superior do Cloud Manager, clique no menu suspenso **Account** e clique em **Manage Account**.



3. Na guia usuários, clique em **Usuário associado**.
4. Insira o endereço de e-mail do usuário e selecione uma função para o usuário:
   - **Admin da conta**: Pode executar qualquer ação no Cloud Manager.
   - **Workspace Admin**: Pode criar e gerenciar recursos em workspaces atribuídos.
   - **Visualizador de conformidade**: Só pode visualizar informações de conformidade e gerar relatórios para espaços de trabalho que eles têm permissão para acessar.
5. Se você selecionou Workspace Admin ou Compliance Viewer, selecione um ou mais workspaces para associar a esse usuário.



6. Clique em **Usuário associado**.

Resultado

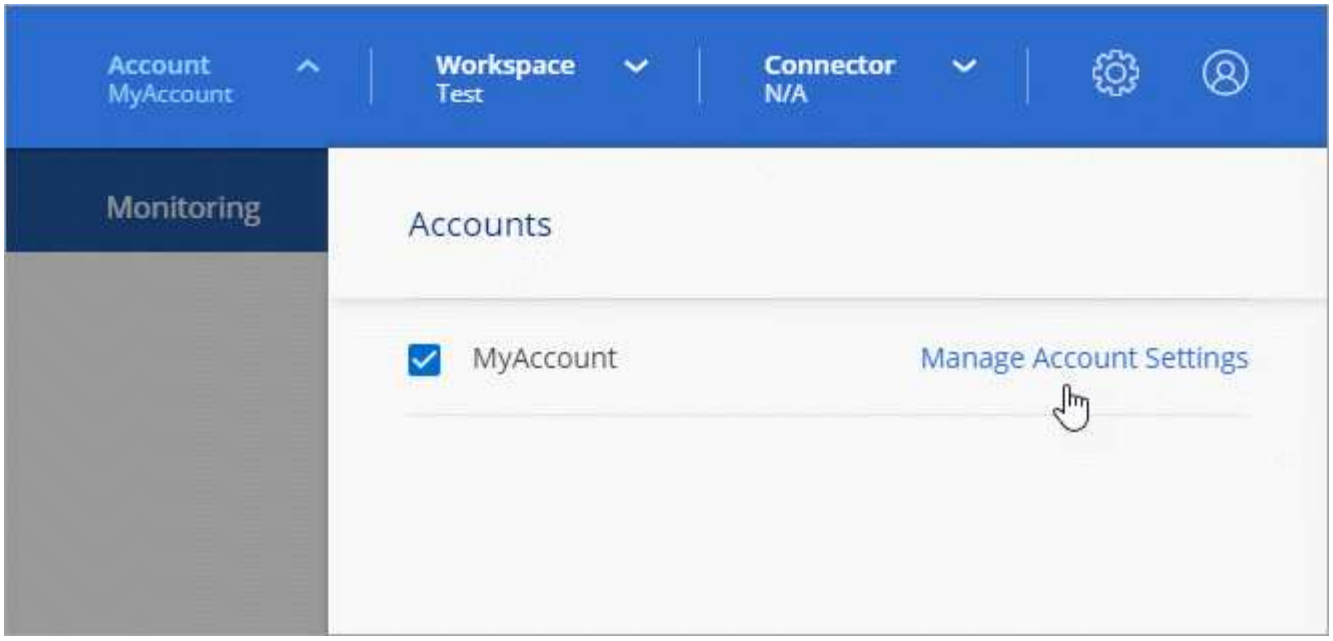
O usuário deve receber um e-mail do NetApp Cloud Central intitulado "Associação de Contas". O e-mail inclui as informações necessárias para acessar o Cloud Manager.

Associar administradores de workspace a workspaces

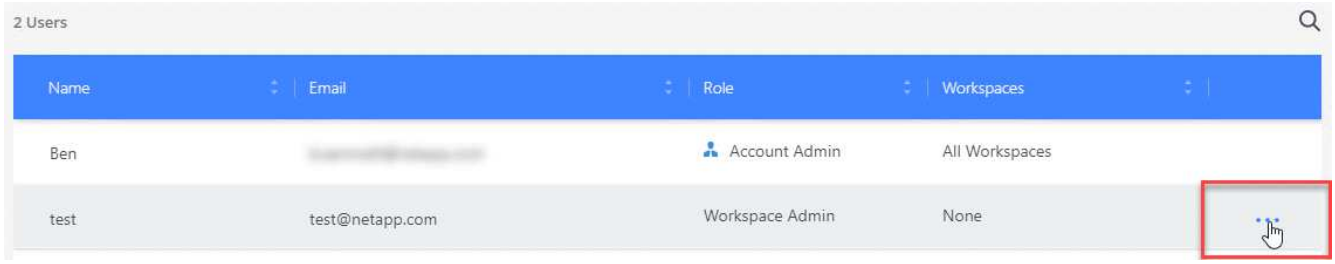
Você pode associar administradores do Workspace a espaços de trabalho adicionais a qualquer momento. Associar o usuário permite que ele crie e visualize os ambientes de trabalho nesse espaço de trabalho.

Passos

1. Na parte superior do Cloud Manager, clique no menu suspenso **Account** e clique em **Manage Account**.



2. Na guia usuários, clique no menu de ação na linha que corresponde ao usuário.



3. Clique em **Gerenciar espaços de trabalho**.
4. Selecione um ou mais espaços de trabalho e clique em **Apply**.

Resultado

O usuário agora pode acessar esses workspaces a partir do Cloud Manager, desde que o conetor também esteja associado aos workspaces.

Associar conetores a espaços de trabalho

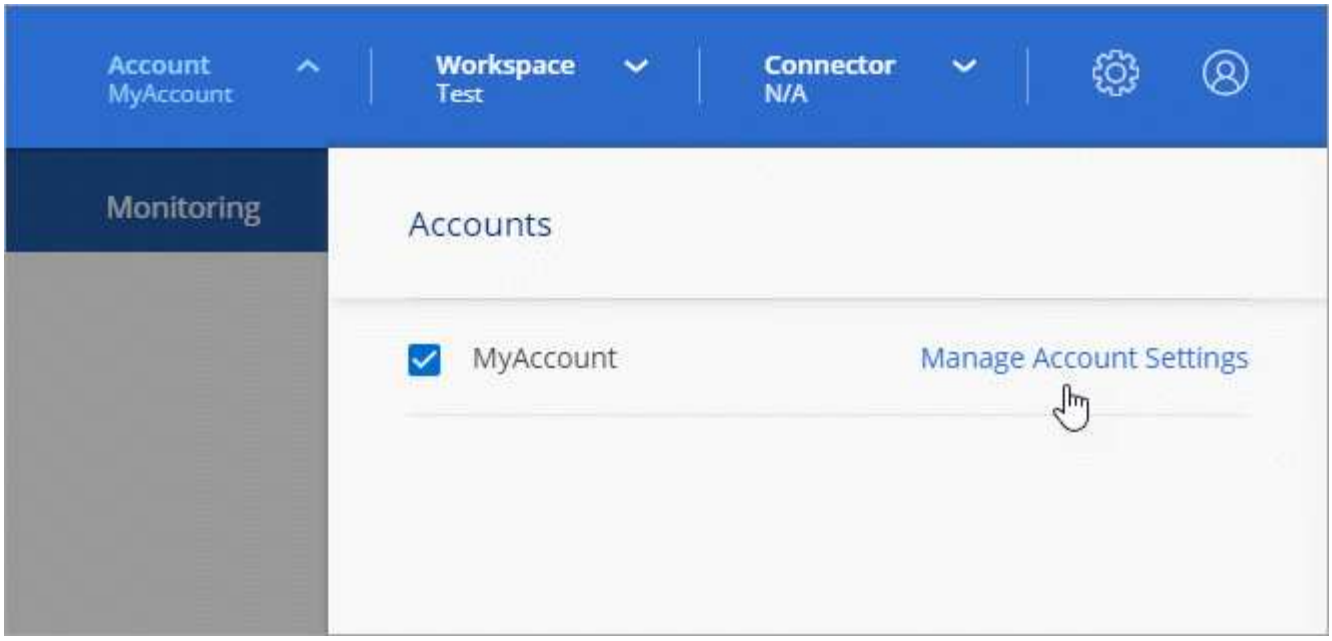
Você precisa associar um conetor aos workspaces para que os administradores do workspace possam usar esses conetores para criar sistemas Cloud Volumes ONTAP.

Se você tiver apenas administradores de conta, associar o conetor com workspaces não será necessário. Administradores de conta têm a capacidade de acessar todos os espaços de trabalho no Cloud Manager por padrão.

"Saiba mais sobre usuários, workspaces e conetores".

Passos

1. Na parte superior do Cloud Manager, clique no menu suspenso **Account** e clique em **Manage Account**.



2. Clique em **Connector**.
3. Clique em **Manage Workspaces** (gerir espaços de trabalho) para o conetor que pretende associar.
4. Selecione um ou mais espaços de trabalho e clique em **Apply**.

Resultado

Administradores de workspace agora podem usar esses conetores para criar sistemas Cloud Volumes ONTAP.

O que se segue?

Agora que você configurou sua conta, você pode gerenciá-la a qualquer momento removendo usuários, gerenciando espaços de trabalho, conetores e assinaturas. "Saiba mais".

Configure um conetor

Saiba mais sobre conetores

Na maioria dos casos, um administrador de conta precisará implantar um *Connector* na sua nuvem ou na rede local. O conetor permite que o Cloud Manager gerencie recursos e processos em seu ambiente de nuvem pública.

Quando é necessário um conetor

Um conetor é necessário para usar qualquer um dos seguintes recursos no Cloud Manager:

- Cloud Volumes ONTAP
- Clusters ONTAP on-premises
- Conformidade com a nuvem
- Kubernetes
- Backup na nuvem

- Monitorização
- Disposição em camadas no local
- Cache de arquivos global
- Descoberta de bucket do Amazon S3

Um conetor é ***not*** necessário para Azure NetApp Files, Cloud Volumes Service ou Cloud Sync.

Embora um conetor não seja necessário para configurar e gerenciar o Azure NetApp Files, um conetor é necessário se você quiser usar o Cloud Compliance para verificar os dados do Azure NetApp Files.

Locais suportados

Um conetor é suportado nos seguintes locais:

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- No local

Se você quiser criar um sistema Cloud Volumes ONTAP no Google Cloud, também precisa ter um conetor em execução no Google Cloud. Não é possível usar um conetor que esteja sendo executado em outro local.

Os conetores devem permanecer em funcionamento

Um conetor deve permanecer sempre em funcionamento. É importante para a saúde e operação contínuas dos serviços que você habilitar.

Por exemplo, um conetor é um componente chave na integridade e operação dos sistemas Cloud Volumes ONTAP PAYGO. Se um conetor for desligado, os sistemas Cloud Volumes ONTAP PAYGO desligarão após perder a comunicação com um conetor por mais de 14 dias.

Como criar um conetor

Um administrador de conta precisa criar um conetor antes que um administrador do espaço de trabalho possa criar um ambiente de trabalho do Cloud Volumes ONTAP e usar qualquer um dos outros recursos listados acima.

Um administrador de conta pode criar um conetor de várias maneiras:

- Diretamente do Cloud Manager (recomendado)
  - "Crie na AWS"
  - "Criar no Azure"
  - "Crie no GCP"
- "No AWS Marketplace"
- "A partir do Azure Marketplace"
- "Baixando e instalando o software em um host Linux existente"

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

Permissões

Permissões específicas são necessárias para criar o conetor e outro conjunto de permissões é necessário para a própria instância do conetor.

Permissões para criar um conetor

O usuário que cria um conetor do Cloud Manager precisa de permissões específicas para implantar a instância em seu provedor de nuvem de sua escolha. O Cloud Manager irá lembrá-lo dos requisitos de permissões quando você criar um conetor.

"Veja as políticas de cada provedor de nuvem".

Permissões para a instância do conetor

O conetor precisa de permissões específicas do provedor de nuvem para executar operações em seu nome. Por exemplo, para implantar e gerenciar o Cloud Volumes ONTAP.

Quando você cria um conetor diretamente do Cloud Manager, o Cloud Manager cria o conetor com as permissões de que ele precisa. Não há nada que você precise fazer.

Se você criar o conetor a partir do AWS Marketplace, do Azure Marketplace ou instalando manualmente o software, precisará garantir que as permissões certas estejam em vigor.

"Veja as políticas de cada provedor de nuvem".

Quando utilizar vários conetores

Em alguns casos, você pode precisar apenas de um conetor, mas você pode encontrar-se precisando de dois ou mais conetores.

Aqui estão alguns exemplos:

- Você está usando um ambiente multicloud (AWS e Azure), então você tem um conetor na AWS e outro no Azure. Cada um gerencia os sistemas Cloud Volumes ONTAP executados nesses ambientes.
- Um provedor de serviços pode usar uma conta do Cloud Central para fornecer serviços para seus clientes, enquanto usa outra conta para fornecer recuperação de desastres para uma de suas unidades de negócios. Cada conta teria conetores separados.

Quando alternar entre conetores

Quando você cria seu primeiro conetor, o Cloud Manager usa esse conetor automaticamente para cada ambiente de trabalho adicional criado. Depois de criar um conetor adicional, você precisará alternar entre eles para ver os ambientes de trabalho específicos de cada conetor.

"Saiba como alternar entre conetores".

A interface do utilizador local

Embora você deva executar quase todas as tarefas do "Interface de usuário SaaS", uma interface de usuário local ainda está disponível no conetor. Esta interface é necessária para algumas tarefas que precisam ser executadas a partir do próprio conetor:

- "Configurando um servidor proxy"
- Instalando um patch (você normalmente trabalhará com o pessoal do NetApp para instalar um patch)
- Download de mensagens do AutoSupport (geralmente direcionadas pelo pessoal do NetApp quando você tiver problemas)

"Saiba como acessar a IU local".

Atualizações do conetor

O conetor atualiza automaticamente o software para a versão mais recente, desde que seja "acesso de saída à internet" necessário obter a atualização de software.

Requisitos de rede para o conetor

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

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

Conexão com redes de destino

Um conetor requer uma conexão de rede com o tipo de ambiente de trabalho que você está criando e os serviços que você está planejando habilitar.

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

Acesso de saída à Internet

O conetor requer acesso de saída à Internet para gerenciar recursos e processos em seu ambiente de nuvem pública. O acesso de saída à Internet também é necessário se você quiser instalar manualmente o conetor em um host Linux ou acessar a IU local em execução no conetor.

As seções a seguir identificam os endpoints específicos.

Endpoints para gerenciar recursos na AWS

Um conetor entra em Contato com os seguintes endpoints ao gerenciar recursos na AWS:

Endpoints	Finalidade
Serviços da AWS (amazonaws.com): • CloudFormation • Nuvem de computação elástica (EC2) • Key Management Service (KMS) • Serviço de token de segurança (STS) • Serviço de armazenamento simples (S3) O endpoint exato depende da região em que você implementa o Cloud Volumes ONTAP. "Consulte a documentação da AWS para obter detalhes."	Permite que o conetor implante e gerencie o Cloud Volumes ONTAP na AWS.
https://api.services.cloud.NetApp.com:443	Solicitações de API para o NetApp Cloud Central.
https://cloud.support.NetApp.com.s3.us-west-1.amazonaws.com	Fornece acesso a imagens de software, manifestos e modelos.
https://repo.cloud.support.NetApp.com	Usado para baixar dependências do Cloud Manager.
http://repo.mysql.com/	Usado para baixar MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-NetApp-com-accelerated.s3.amazonaws.com	Permite que o conetor acesse e baixe manifestos, modelos e imagens de atualização do Cloud Volumes ONTAP.
https://cloudmanagerinfraprod.azurecr.io	Acesso a imagens de software de componentes de contentor para uma infraestrutura que esteja executando o Docker e fornece uma solução para integrações de serviços com o Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permite que o NetApp transmita dados de Registros de auditoria.
https://cloudmanager.cloud.NetApp.com	Comunicação com o serviço Cloud Manager, que inclui contas do Cloud Central.
https://NetApp-cloud-account.auth0.com	Comunicação com o NetApp Cloud Central para autenticação centralizada de usuários.
https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist	Usado para adicionar seu ID de conta da AWS à lista de usuários permitidos para Backup em S3.
https://support.NetApp.com/aods/asupmessage https://support.NetApp.com/asupprod/post/1,0/postAsup	Comunicação com NetApp AutoSupport.

Endpoints	Finalidade
https://support.NetApp.com/svcgw - https://support.NetApp.com/ServiceGW/Entitlement - https://eval.lic.NetApp.com.s3.us-west-1.amazonaws.com - https://cloud-support-NetApp-com.s3.us-west-1.amazonaws.com	Comunicação com o NetApp para licenciamento de sistema e Registro de suporte.
https://client.infra.support.NetApp.com.s3.us-west-1.amazonaws.com - https://cloud-support-NetApp-com-accelerated.s3.us-west-1.amazonaws.com - https://trigger.asup.NetApp.com.s3.us-west-1.amazonaws.com	Permite que o NetApp colete informações necessárias para solucionar problemas de suporte.
https://ipa-signer.cloudmanager.NetApp.com	Permite que o Cloud Manager gere licenças (por exemplo, uma licença FlexCache para Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/Trident/Releases/download/	Necessário para conectar sistemas Cloud Volumes ONTAP a um cluster Kubernetes. Os endpoints permitem a instalação do NetApp Trident.
Vários locais de terceiros, por exemplo: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com Locais de terceiros estão sujeitos a alterações.	Durante as atualizações, o Cloud Manager baixa os pacotes mais recentes para dependências de terceiros.

Endpoints para gerenciar recursos no Azure

Um conetor entra em Contato com os seguintes endpoints ao gerenciar recursos no Azure:

Endpoints	Finalidade
https://management.azure.com https://login.microsoftonline.com	Permite que o Cloud Manager implante e gerencie o Cloud Volumes ONTAP na maioria das regiões do Azure.
https://management.microsoftazure.de https://login.microsoftonline.de	Permite que o Cloud Manager implante e gerencie o Cloud Volumes ONTAP nas regiões Azure Alemanha.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Permite que o Cloud Manager implante e gerencie o Cloud Volumes ONTAP nas regiões Azure US Gov.
https://api.services.cloud.NetApp.com:443	Solicitações de API para o NetApp Cloud Central.
https://cloud.support.NetApp.com.s3.us-west-1.amazonaws.com	Fornece acesso a imagens de software, manifestos e modelos.
https://repo.cloud.support.NetApp.com	Usado para baixar dependências do Cloud Manager.
http://repo.mysql.com/	Usado para baixar MySQL.

Endpoints	Finalidade
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-NetApp-com-accelerated.s3.amazonaws.com	Permite que o conetor acesse e baixe manifestos, modelos e imagens de atualização do Cloud Volumes ONTAP.
https://cloudmanagerinfraprod.azurecr.io	Acesso a imagens de software de componentes de contentor para uma infraestrutura que esteja executando o Docker e fornece uma solução para integrações de serviços com o Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permite que o NetApp transmita dados de Registros de auditoria.
https://cloudmanager.cloud.NetApp.com	Comunicação com o serviço Cloud Manager, que inclui contas do Cloud Central.
https://NetApp-cloud-account.auth0.com	Comunicação com o NetApp Cloud Central para autenticação centralizada de usuários.
https://mysupport.NetApp.com	Comunicação com NetApp AutoSupport.
https://support.NetApp.com/svcgw - https://support.NetApp.com/ServiceGW/Entitlement - https://eval.lic.NetApp.com.s3.us-west-1.amazonaws.com - https://cloud-support-NetApp-com.s3.us-west-1.amazonaws.com	Comunicação com o NetApp para licenciamento de sistema e Registro de suporte.
https://client.infra.support.NetApp.com.s3.us-west-1.amazonaws.com - https://cloud-support-NetApp-com-accelerated.s3.us-west-1.amazonaws.com - https://trigger.asup.NetApp.com.s3.us-west-1.amazonaws.com	Permite que o NetApp colete informações necessárias para solucionar problemas de suporte.
https://ipa-signer.cloudmanager.NetApp.com	Permite que o Cloud Manager gere licenças (por exemplo, uma licença FlexCache para Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/Trident/Releases/download/	Necessário para conectar sistemas Cloud Volumes ONTAP a um cluster Kubernetes. Os endpoints permitem a instalação do NetApp Trident.
*.blob.core.windows.net	Necessário para pares de HA ao usar um proxy.

Endpoints	Finalidade
Vários locais de terceiros, por exemplo: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com Locais de terceiros estão sujeitos a alterações.	Durante as atualizações, o Cloud Manager baixa os pacotes mais recentes para dependências de terceiros.

Endpoints para gerenciar recursos no GCP

Um conetor entra em Contato com os seguintes endpoints ao gerenciar recursos no GCP:

Endpoints	Finalidade
https://www.googleapis.com	Permite que o conetor entre em Contato com as APIs do Google para implantar e gerenciar o Cloud Volumes ONTAP no GCP.
https://api.services.cloud.NetApp.com:443	Solicitações de API para o NetApp Cloud Central.
https://cloud.support.NetApp.com.s3.us-west-1.amazonaws.com	Fornece acesso a imagens de software, manifestos e modelos.
https://repo.cloud.support.NetApp.com	Usado para baixar dependências do Cloud Manager.
http://repo.mysql.com/	Usado para baixar MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-NetApp-com-accelerated.s3.amazonaws.com	Permite que o conetor acesse e baixe manifestos, modelos e imagens de atualização do Cloud Volumes ONTAP.
https://cloudmanagerinfraprod.azurecr.io	Acesso a imagens de software de componentes de contentor para uma infraestrutura que esteja executando o Docker e fornece uma solução para integrações de serviços com o Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permite que o NetApp transmita dados de Registros de auditoria.
https://cloudmanager.cloud.NetApp.com	Comunicação com o serviço Cloud Manager, que inclui contas do Cloud Central.
https://NetApp-cloud-account.auth0.com	Comunicação com o NetApp Cloud Central para autenticação centralizada de usuários.
https://mysupport.NetApp.com	Comunicação com NetApp AutoSupport.

Endpoints	Finalidade
https://support.NetApp.com/svcgw - https://support.NetApp.com/ServiceGW/Entitlement - https://eval.lic.NetApp.com.s3.us-west-1.amazonaws.com - https://cloud-support-NetApp-com.s3.us-west-1.amazonaws.com	Comunicação com o NetApp para licenciamento de sistema e Registro de suporte.
https://client.infra.support.NetApp.com.s3.us-west-1.amazonaws.com - https://cloud-support-NetApp-com-accelerated.s3.us-west-1.amazonaws.com - https://trigger.asup.NetApp.com.s3.us-west-1.amazonaws.com	Permite que o NetApp colete informações necessárias para solucionar problemas de suporte.
https://ipa-signer.cloudmanager.NetApp.com	Permite que o Cloud Manager gere licenças (por exemplo, uma licença FlexCache para Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/Trident/Releases/download/	Necessário para conectar sistemas Cloud Volumes ONTAP a um cluster Kubernetes. Os endpoints permitem a instalação do NetApp Trident.
Vários locais de terceiros, por exemplo: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com Locais de terceiros estão sujeitos a alterações.	Durante as atualizações, o Cloud Manager baixa os pacotes mais recentes para dependências de terceiros.

Endpoints para instalar o conetor em um host Linux

Você tem a opção de instalar manualmente o software Connector em seu próprio host Linux. Se o fizer, o instalador do conetor deve acessar os seguintes URLs durante o processo de instalação:

- http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm
- https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
- https://s3.amazonaws.com/aws-cli/awscli-bundle.zip

O host pode tentar atualizar os pacotes do sistema operacional durante a instalação. O host pode entrar em Contato com diferentes sites de espelhamento para esses pacotes do sistema operacional.

Endpoints acessados a partir do navegador da Web ao usar a IU local

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

Endpoints	Finalidade
O host do conetor	Você deve inserir o endereço IP do host de um navegador da Web para carregar o console do Cloud Manager. Dependendo da sua conetividade com o seu provedor de nuvem, você pode usar o IP privado ou um IP público atribuído ao host: • Um IP privado funciona se você tiver uma VPN e acesso direto à sua rede virtual • Um IP público funciona em qualquer cenário de rede Em qualquer caso, você deve proteger o acesso à rede, garantindo que as regras do grupo de segurança permitam o acesso somente de IPs ou sub-redes autorizados.
https://auth0.com https://cdn.auth0.com://NetApp-cloud-account.auth0.com https://services.cloud.NetApp.com	Seu navegador da Web se coneta a esses endpoints para autenticação de usuário centralizada por meio do NetApp Cloud Central.
https://widget.intercom.io	Para um bate-papo no produto que permite conversar com especialistas em nuvem da NetApp.

Portas e grupos de segurança

Não há tráfego de entrada para o conetor, a menos que você o inicie. HTTP e HTTPS fornecem acesso ao "IU local", que você usará em circunstâncias raras. O SSH só é necessário se você precisar se conetar ao host para solução de problemas.

Regras para o conetor na AWS

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

Regras de entrada

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

Protocolo	Porta	Finalidade
SSH	22	Fornece acesso SSH ao host do conetor
HTTP	80	Fornece acesso HTTP a partir de navegadores da Web cliente para a interface de usuário local e conexões a partir do Cloud Compliance
HTTPS	443	Fornece acesso HTTPS a partir de navegadores da Web cliente para a interface de usuário local
TCP	3128	Fornece à instância de conformidade com a nuvem acesso à Internet, se sua rede AWS não usar um NAT ou proxy

Regras de saída

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

Regras básicas de saída

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

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

Regras de saída avançadas

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

O endereço IP de origem é o host do conetor.

Serviço	Protocolo	Porta	Destino	Finalidade
Ative Directory	TCP	88	Floresta do ative Directory	Autenticação Kerberos V.
	TCP	139	Floresta do ative Directory	Sessão de serviço NetBIOS
	TCP	389	Floresta do ative Directory	LDAP
	TCP	445	Floresta do ative Directory	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
	TCP	464	Floresta do ative Directory	Kerberos V alterar e definir senha (SET_CHANGE)
	TCP	749	Floresta do ative Directory	Palavra-passe de alteração e definição Kerberos V do ative Directory (RPCSEC_GSS)
	UDP	137	Floresta do ative Directory	Serviço de nomes NetBIOS
	UDP	138	Floresta do ative Directory	Serviço de datagrama NetBIOS
	UDP	464	Floresta do ative Directory	Administração de chaves Kerberos

Serviço	Protocolo	Porta	Destino	Finalidade
Chamadas de API e AutoSupport	HTTPS	443	LIF de gerenciamento de cluster de ONTAP e Internet de saída	Chamadas de API para AWS e ONTAP e envio de mensagens AutoSupport para o NetApp
Chamadas de API	TCP	3000	LIF de gerenciamento de clusters ONTAP	Chamadas de API para ONTAP
	TCP	8088	Cópia de segurança para S3	Chamadas de API para Backup para S3
DNS	UDP	53	DNS	Usado para resolução de DNS pelo Cloud Manager
Conformidade com a nuvem	HTTP	80	Instância de Cloud Compliance	Cloud Compliance para Cloud Volumes ONTAP

Regras para o conetor no Azure

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

Regras de entrada

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

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

Regras de saída

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

Regras básicas de saída

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

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

Regras de saída avançadas

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

O endereço IP de origem é o host do conetor.

Serviço	Porta	Protocolo	Destino	Finalidade
Ative Directory	88	TCP	Floresta do ative Directory	Autenticação Kerberos V.
	139	TCP	Floresta do ative Directory	Sessão de serviço NetBIOS
	389	TCP	Floresta do ative Directory	LDAP
	445	TCP	Floresta do ative Directory	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
	464	TCP	Floresta do ative Directory	Kerberos V alterar e definir senha (SET_CHANGE)
	749	TCP	Floresta do ative Directory	Palavra-passe de alteração e definição Kerberos V do ative Directory (RPCSEC_GSS)
	137	UDP	Floresta do ative Directory	Serviço de nomes NetBIOS
	138	UDP	Floresta do ative Directory	Serviço de datagrama NetBIOS
	464	UDP	Floresta do ative Directory	Administração de chaves Kerberos
Chamadas de API e AutoSupport	443	HTTPS	LIF de gerenciamento de cluster de ONTAP e Internet de saída	Chamadas de API para AWS e ONTAP e envio de mensagens AutoSupport para o NetApp
Chamadas de API	3000	TCP	LIF de gerenciamento de clusters ONTAP	Chamadas de API para ONTAP

Serviço	Porta	Protocolo	Destino	Finalidade
DNS	53	UDP	DNS	Usado para resolução de DNS pelo Cloud Manager

Regras para o conetor na GCP

As regras de firewall para o conetor exigem regras de entrada e saída.

Regras de entrada

A origem das regras de entrada nas regras de firewall predefinidas é 0,0.0,0/0.

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

Regras de saída

As regras de firewall predefinidas para o conetor abrem todo o tráfego de saída. Se isso for aceitável, siga as regras básicas de saída. Se você precisar de regras mais rígidas, use as regras de saída avançadas.

Regras básicas de saída

As regras de firewall predefinidas para o conetor incluem as seguintes regras de saída.

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

Regras de saída avançadas

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

O endereço IP de origem é o host do conetor.

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

Criando um conetor na AWS a partir do Cloud Manager

Um administrador de conta precisa implantar um *Connector* antes de poder usar a maioria dos recursos do Cloud Manager. "Aprenda quando um conetor é necessário". O conetor permite que o Cloud Manager gerencie recursos e processos em seu ambiente de nuvem pública.

Esta página descreve como criar um conetor na AWS diretamente do Cloud Manager. Também tem a opção

de "Crie o conetor no AWS Marketplace", ou para "baixe o software e instale-o em seu próprio host".

Essas etapas devem ser concluídas por um usuário que tenha a função Administrador da conta. Um administrador do espaço de trabalho não pode criar um conetor.

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

Configurando permissões da AWS para criar um conetor

Antes de implantar um conetor do Cloud Manager, você precisa garantir que sua conta da AWS tenha as permissões corretas.

Passos

1. Transfira a política do IAM do conetor a partir da seguinte localização:

   "Gerenciador de nuvem do NetApp: Políticas da AWS, Azure e GCP"

2. No console do AWS IAM, crie sua própria política copiando e colando o texto da política do Connector IAM.
3. Anexe a política criada na etapa anterior ao usuário do IAM que criará o conetor do Cloud Manager.

Resultado

O usuário da AWS agora tem as permissões necessárias para criar o conetor do Cloud Manager. Você precisará especificar as chaves de acesso da AWS para esse usuário quando for solicitado pelo Cloud Manager.

Criando um conetor na AWS

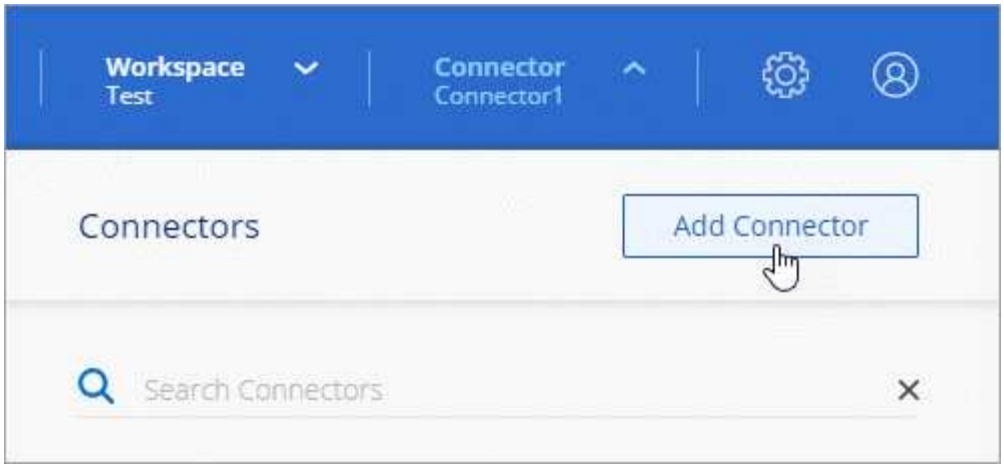
O Cloud Manager permite que você crie um conetor na AWS diretamente a partir de sua interface de usuário.

O que você vai precisar

- Uma chave de acesso da AWS e uma chave secreta para um usuário do IAM que tenha o "permissões necessárias".
- Uma VPC, sub-rede e um par de chaves na sua região da AWS escolhida.

Passos

1. Se você estiver criando seu primeiro ambiente de trabalho, clique em **Adicionar ambiente de trabalho** e siga as instruções. Caso contrário, clique no menu suspenso **Connector** e selecione **Add Connector**.



2. Clique em **Let's Start**.
3. Escolha **Amazon Web Services** como seu provedor de nuvem.

   Lembre-se de que o conetor deve ter uma conexão de rede com o tipo de ambiente de trabalho que você está criando e os serviços que você está planejando habilitar.

   "Saiba mais sobre os requisitos de rede para o conetor".

4. Revise o que você precisará e clique em **continuar**.
5. Forneça as informações necessárias:
   - **Credenciais da AWS**: Insira um nome para a instância e especifique a chave de acesso e a chave secreta da AWS que atendem aos requisitos de permissões.
   - **Localização**: Especifique uma região, VPC e sub-rede da AWS para a instância.
   - **Rede**: Selecione o par de chaves a utilizar com a instância, se pretende ativar um endereço IP público e, opcionalmente, especificar uma configuração de proxy.
   - **Grupo de segurança**: Escolha se deseja criar um novo grupo de segurança ou se deseja selecionar um grupo de segurança existente que permita o acesso HTTP, HTTPS e SSH de entrada.

     Não há tráfego de entrada para o conetor, a menos que você o inicie. HTTP e HTTPS fornecem acesso ao "IU local", que você usará em circunstâncias raras. O SSH só é necessário se você precisar se conetar ao host para solução de problemas.

6. Clique em **criar**.

   A instância deve estar pronta em cerca de 7 minutos. Você deve permanecer na página até que o processo esteja concluído.

Depois de terminar

Você precisa associar um conetor aos workspaces para que os administradores do workspace possam usar esses conetores para criar sistemas Cloud Volumes ONTAP. Se você tiver apenas administradores de conta, associar o conetor aos workspaces não será necessário. Administradores de conta têm a capacidade de acessar todos os espaços de trabalho no Cloud Manager por padrão. "Saiba mais".

Criando um conetor no Azure a partir do Cloud Manager

Um administrador de conta precisa implantar um *Connector* antes de poder usar a

maioria dos recursos do Cloud Manager. "Aprenda quando um conetor é necessário". O conetor permite que o Cloud Manager gerencie recursos e processos em seu ambiente de nuvem pública.

Esta página descreve como criar um conetor no Azure diretamente do Cloud Manager. Também tem a opção de "Crie o conetor no Azure Marketplace", ou para "baixe o software e instale-o em seu próprio host".

Essas etapas devem ser concluídas por um usuário que tenha a função Administrador da conta. Um administrador do espaço de trabalho não pode criar um conetor.

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

Configurando permissões do Azure para criar um conetor

Antes de implantar um conetor do Cloud Manager, você precisa garantir que sua conta do Azure tenha as permissões corretas.

Passos

1. Crie uma função personalizada usando a política do Azure para o conetor:

   a. Faça download do "Política do Azure para o conetor".

      Clique com o botão direito no link e clique em **Salvar link como...** para baixar o arquivo.

   b. Modifique o arquivo JSON adicionando sua ID de assinatura do Azure ao escopo atribuível.

      Exemplo

      ```
      "AssignableScopes": [
      "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
      ],
      ```

   c. Use o arquivo JSON para criar uma função personalizada no Azure.

      O exemplo a seguir mostra como criar uma função personalizada usando a CLI do Azure 2,0:

      ```
      az role definition create --role-definition
      C:\Policy_for_Setup_As_Service_Azure.json
      ```

   Agora você deve ter uma função personalizada chamada *Azure SetupAsService*.

2. Atribua a função ao usuário que implantará o conetor do Cloud Manager:

   a. Abra o serviço **Subscrições** e selecione a assinatura do usuário.

   b. Clique em **Access Control (IAM)**.

   c. Clique em **Adicionar** > **Adicionar atribuição de função** e, em seguida, adicione as permissões:

      - Selecione a função **Azure SetupAsService**.

Azure SetupAsService é o nome padrão fornecido no "Política de implantação do Connector para Azure". Se você escolher um nome diferente para a função, selecione esse nome em vez disso.

- Atribua acesso a um **usuário, grupo ou aplicativo do Azure AD**.
- Selecione a conta de utilizador.
- Clique em **Salvar**.

Resultado

O usuário do Azure agora tem as permissões necessárias para implantar o conetor do Cloud Manager.

Criando um conetor no Azure

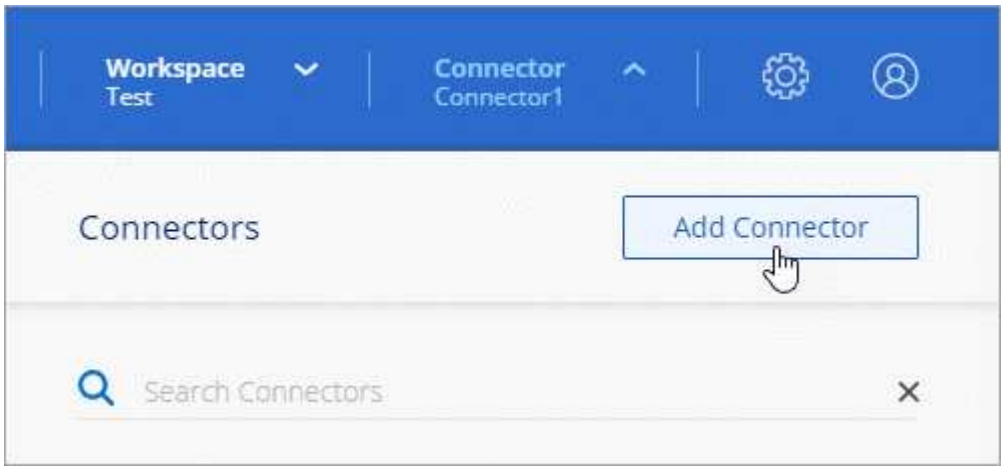
O Cloud Manager permite que você crie um conetor no Azure diretamente a partir de sua interface de usuário.

O que você vai precisar

- A "permissões necessárias" para a sua conta Azure.
- Uma subscrição do Azure.
- Uma VNet e uma sub-rede na sua região do Azure escolhida.

Passos

1. Se você estiver criando seu primeiro ambiente de trabalho, clique em **Adicionar ambiente de trabalho** e siga as instruções. Caso contrário, clique no menu suspenso **Connector** e selecione **Add Connector**.



2. Clique em **Let's Start**.
3. Escolha **Microsoft Azure** como seu provedor de nuvem.

   Lembre-se de que o conetor deve ter uma conexão de rede com o tipo de ambiente de trabalho que você está criando e os serviços que você está planejando habilitar.

   "Saiba mais sobre os requisitos de rede para o conetor".

4. Revise o que você precisará e clique em **continuar**.
5. Se você for solicitado, faça login na sua conta Microsoft, que deve ter as permissões necessárias para criar a máquina virtual.

O formulário é de propriedade e hospedado pela Microsoft. Suas credenciais não são fornecidas ao NetApp.

Se você já estiver conetado a uma conta do Azure, o Cloud Manager usará essa conta automaticamente. Se você tiver várias contas, talvez seja necessário fazer logout primeiro para garantir que esteja usando a conta certa.

6. Forneça as informações necessárias:
   - **Autenticação da VM**: Insira um nome para a máquina virtual e um nome de usuário e senha ou chave pública.
   - **Configurações básicas**: Escolha uma assinatura do Azure, uma região do Azure e se deseja criar um novo grupo de recursos ou usar um grupo de recursos existente.
   - **Rede**: Escolha uma VNet e uma sub-rede, se deseja ativar um endereço IP público e, opcionalmente, especifique uma configuração de proxy.
   - **Grupo de segurança**: Escolha se deseja criar um novo grupo de segurança ou se deseja selecionar um grupo de segurança existente que permita o acesso HTTP, HTTPS e SSH de entrada.

     Não há tráfego de entrada para o conetor, a menos que você o inicie. HTTP e HTTPS fornecem acesso ao "IU local", que você usará em circunstâncias raras. O SSH só é necessário se você precisar se conetar ao host para solução de problemas.

7. Clique em **criar**.

   A máquina virtual deve estar pronta em cerca de 7 minutos. Você deve permanecer na página até que o processo esteja concluído.

Depois de terminar

Você precisa associar um conetor aos workspaces para que os administradores do workspace possam usar esses conetores para criar sistemas Cloud Volumes ONTAP. Se você tiver apenas administradores de conta, associar o conetor aos workspaces não será necessário. Administradores de conta têm a capacidade de acessar todos os espaços de trabalho no Cloud Manager por padrão. "Saiba mais".

Criando um conetor no GCP a partir do Cloud Manager

Um administrador de conta precisa implantar um *Connector* antes de poder usar a maioria dos recursos do Cloud Manager. "Aprenda quando um conetor é necessário". O conetor permite que o Cloud Manager gerencie recursos e processos em seu ambiente de nuvem pública.

Esta página descreve como criar um conetor no GCP diretamente do Cloud Manager. Você também tem a opção de "baixe o software e instale-o em seu próprio host".

Essas etapas devem ser concluídas por um usuário que tenha a função Administrador da conta. Um administrador do espaço de trabalho não pode criar um conetor.

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

Configurando permissões do GCP para criar um conetor

Antes de implantar um conetor do Cloud Manager, você precisa garantir que sua conta do GCP tenha as permissões corretas e que uma conta de serviço esteja configurada para a VM Connector.

Passos

1. Certifique-se de que o usuário do GCP que implanta o Gerenciador de nuvem do NetApp Central tenha as permissões no "Política de implantação do Connector para GCP".

   "Você pode criar uma função personalizada usando o arquivo YAML" e, em seguida, anexá-lo ao usuário. Você precisará usar a linha de comando gcloud para criar a função.

2. Configure uma conta de serviço que tenha as permissões necessárias para criar e gerenciar sistemas Cloud Volumes ONTAP em projetos.

   Você associará essa conta de serviço à VM Connector ao criá-la a partir do Cloud Manager.

   a. "Crie uma função no GCP" isso inclui as permissões definidas no "Política do Cloud Manager para GCP". Novamente, você precisará usar a linha de comando gcloud.

      As permissões contidas neste arquivo YAML são diferentes das permissões na etapa 2a.

   b. "Crie uma conta de serviço do GCP e aplique a função personalizada que você acabou de criar".

   c. Se você quiser implantar o Cloud Volumes ONTAP em outros projetos "Conceda acesso adicionando a conta de serviço com a função Cloud Manager a esse projeto", . Você precisará repetir esta etapa para cada projeto.

Resultado

O usuário do GCP agora tem as permissões necessárias para criar o conetor do Cloud Manager e a conta de serviço para a VM do conetor está configurada.

Ativação das APIs do Google Cloud

Várias APIs são necessárias para implantar o conetor e o Cloud Volumes ONTAP.

Passo

1. "Ative as seguintes APIs do Google Cloud em seu projeto".
   - API do Cloud Deployment Manager V2
   - API Cloud Logging
   - API do Cloud Resource Manager
   - API do mecanismo de computação
   - API de gerenciamento de identidade e acesso (IAM)

Criando um conetor no GCP

O Cloud Manager permite criar um conetor no GCP diretamente a partir da interface de usuário.

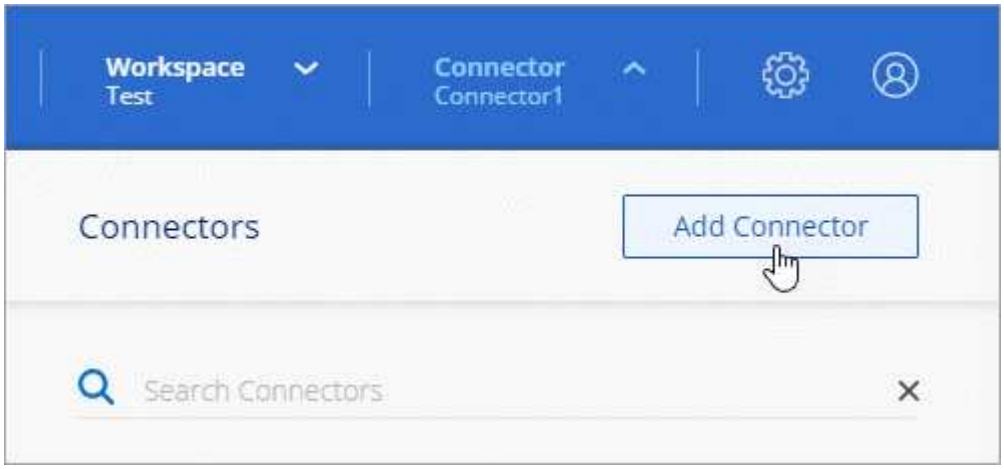
O que você vai precisar

- A "permissões necessárias" para a sua conta do Google Cloud.
- Um projeto do Google Cloud.

- Uma conta de serviço que tem as permissões necessárias para criar e gerenciar o Cloud Volumes ONTAP.
- Uma VPC e uma sub-rede na região escolhida pelo Google Cloud.

Passos

1. Se você estiver criando seu primeiro ambiente de trabalho, clique em **Adicionar ambiente de trabalho** e siga as instruções. Caso contrário, clique no menu suspenso **Connector** e selecione **Add Connector**.



2. Clique em **Let's Start**.
3. Escolha **Google Cloud Platform** como seu provedor de nuvem.

   Lembre-se de que o conetor deve ter uma conexão de rede com o tipo de ambiente de trabalho que você está criando e os serviços que você está planejando habilitar.

   "Saiba mais sobre os requisitos de rede para o conetor".

4. Revise o que você precisará e clique em **continuar**.
5. Se você for solicitado, faça login na sua conta do Google, que deve ter as permissões necessárias para criar a instância da máquina virtual.

   O formulário é de propriedade e hospedado pelo Google. Suas credenciais não são fornecidas ao NetApp.

6. Forneça as informações necessárias:
   - **Configurações básicas**: Insira um nome para a instância da máquina virtual e especifique uma conta de projeto e serviço que tenha as permissões necessárias.
   - **Localização**: Especifique uma região, zona, VPC e sub-rede para a instância.
   - **Rede**: Escolha se deseja ativar um endereço IP público e, opcionalmente, especificar uma configuração de proxy.
   - **Política de firewall**: Escolha se deseja criar uma nova política de firewall ou se deseja selecionar uma política de firewall existente que permita o acesso HTTP, HTTPS e SSH de entrada.

     Não há tráfego de entrada para o conetor, a menos que você o inicie. HTTP e HTTPS fornecem acesso ao "IU local", que você usará em circunstâncias raras. O SSH só é necessário se você precisar se conetar ao host para solução de problemas.

7. Clique em **criar**.

A instância deve estar pronta em cerca de 7 minutos. Você deve permanecer na página até que o processo esteja concluído.

Depois de terminar

Você precisa associar um conetor aos workspaces para que os administradores do workspace possam usar esses conetores para criar sistemas Cloud Volumes ONTAP. Se você tiver apenas administradores de conta, associar o conetor aos workspaces não será necessário. Administradores de conta têm a capacidade de acessar todos os espaços de trabalho no Cloud Manager por padrão. "Saiba mais".

Onde ir a seguir

Agora que você fez login e configurou o Cloud Manager, os usuários podem começar a criar e descobrir ambientes de trabalho.

- "Comece a usar o Cloud Volumes ONTAP para AWS"
- "Comece a usar o Cloud Volumes ONTAP para Azure"
- "Comece a usar o Cloud Volumes ONTAP para Google Cloud"
- "Configure o Azure NetApp Files"
- "Configure o Cloud Volumes Service para AWS"
- "Descubra um cluster ONTAP no local"
- "Descubra seus buckets do Amazon S3"

Se você for um administrador, poderá gerenciar as configurações do Cloud Manager depois de criar seu primeiro conetor.

- "Saiba mais sobre conetores"
- "Gerencie um certificado HTTPS para acesso seguro"
- "Configure as definições de proxy"

Gerenciar o Cloud Volumes ONTAP

Aprenda

Saiba mais sobre o Cloud Volumes ONTAP

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

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

- Eficiência de storage

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

- Alta disponibilidade

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

- Proteção de dados

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

  O Cloud Volumes ONTAP também se integra ao Cloud Backup Service para fornecer recursos de backup e restauração para proteção e arquivamento a longo prazo de seus dados de nuvem.

- Categorização de dados

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

- Consistência de aplicativos

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

- Segurança dos dados

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

- Controles de conformidade de privacidade

  A integração com o Cloud Compliance ajuda você a entender o contexto dos dados e identificar dados confidenciais.

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

"Veja as configurações do Cloud Volumes ONTAP compatíveis"

"Saiba mais sobre o Cloud Volumes ONTAP"

Armazenamento

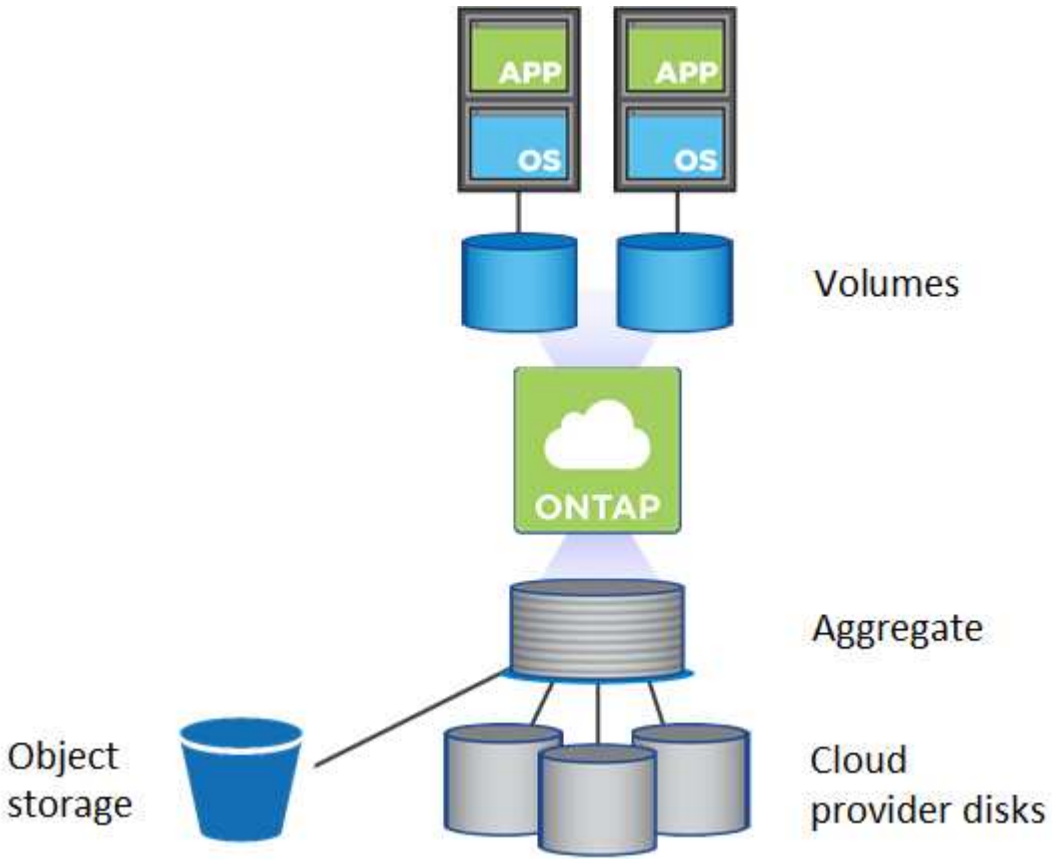
Discos e agregados

Entender como o Cloud Volumes ONTAP usa o storage de nuvem pode ajudar você a entender seus custos de storage.

Todos os discos e agregados devem ser criados e excluídos diretamente do Cloud Manager. Você não deve executar essas ações de outra ferramenta de gerenciamento. Isso pode afetar a estabilidade do sistema, dificultar a capacidade de adicionar discos no futuro e, potencialmente, gerar taxas redundantes de provedores de nuvem.

Visão geral

A Cloud Volumes ONTAP usa o storage de fornecedor de nuvem como discos e os agrupa em uma ou mais agregados. Agregados fornecem storage para um ou mais volumes.



Vários tipos de discos de nuvem são suportados. Você escolhe o tipo de disco ao criar um volume e o tamanho de disco padrão ao implantar o Cloud Volumes ONTAP.

A quantidade total de storage comprada de um fornecedor de nuvem é a *capacidade bruta*. A *capacidade utilizável* é menor porque aproximadamente 12 a 14% é sobrecarga reservada para uso Cloud Volumes ONTAP. Por exemplo, se o Cloud Manager criar um agregado de 500 GB, a capacidade utilizável será de 442,94 GB.

Storage da AWS

Na AWS, o Cloud Volumes ONTAP usa o armazenamento EBS para dados de usuário e armazenamento NVMe local como Flash Cache em alguns tipos de instâncias do EC2.

Armazenamento EBS

Na AWS, um agregado pode conter até 6 discos com o mesmo tamanho. O tamanho máximo do disco é de 16 TB.

O tipo de disco EBS subjacente pode ser SSD de uso geral, SSD IOPS provisionado, HDD otimizado para taxa de transferência ou HDD frio. Você pode emparelhar um disco EBS com o Amazon S3 para "categorize os dados inativos em storage de objetos de baixo custo".

A um nível elevado, as diferenças entre os tipos de discos EBS são as seguintes:

- *Discos SSD* de uso geral equilibram custo e desempenho para uma ampla variedade de cargas de trabalho. A performance é definida em termos de IOPS.
- Os discos SSD _IOPS provisionados são para aplicativos críticos que exigem o mais alto desempenho a um custo mais alto.
- *Discos HDD* otimizados para taxa de transferência são para cargas de trabalho acessadas com frequência que exigem taxa de transferência rápida e consistente a um preço menor.
- *Cold HDD* discos são destinados a backups, ou dados acessados com pouca frequência, porque o desempenho é muito baixo. Assim como os discos HDD otimizados para taxa de transferência, o desempenho é definido em termos de taxa de transferência.

Discos rígidos inativos não são compatíveis com configurações de HA e com categorização de dados.

Storage NVMe local

Alguns tipos de instâncias do EC2 incluem storage NVMe local, que o Cloud Volumes ONTAP usa como "Flash Cache".

- Ligações relacionadas*
- "Documentação da AWS: Tipos de volume do EBS"
- "Saiba como escolher tipos de disco e tamanhos de disco para seus sistemas na AWS"
- "Analisar os limites de armazenamento do Cloud Volumes ONTAP na AWS"
- "Revise as configurações compatíveis do Cloud Volumes ONTAP na AWS"

Storage Azure

No Azure, um agregado pode conter até 12 discos com o mesmo tamanho. O tipo de disco e o tamanho máximo do disco dependem se você usa um sistema de nó único ou um par de HA:

Sistemas de nó único

Sistemas de nó único podem usar três tipos de discos gerenciados do Azure:

- *Discos gerenciados SSD premium* fornecem alto desempenho para cargas de trabalho com uso intenso de e/S a um custo mais alto.
- *Discos gerenciados SSD padrão* fornecem desempenho consistente para cargas de trabalho que exigem IOPS baixo.
- *Discos gerenciados HDD padrão* são uma boa escolha se você não precisa de IOPS alto e quer reduzir seus custos.

  Cada tipo de disco gerenciado tem um tamanho máximo de disco de 32 TB.

  É possível emparelhar um disco gerenciado com o storage Azure Blob ao "categorize os dados inativos em storage de objetos de baixo custo".

Pares HA

Os pares HA usam blobs de página Premium, que têm um tamanho máximo de disco de 8 TB.

- Ligações relacionadas*
- "Documentação do Microsoft Azure: Introdução ao Microsoft Azure Storage"
- "Saiba como escolher tipos de disco e tamanhos de disco para seus sistemas no Azure"
- "Analisar os limites de armazenamento do Cloud Volumes ONTAP no Azure"

Armazenamento do GCP

Na GCP, um agregado pode conter até 6 discos com o mesmo tamanho. O tamanho máximo do disco é de 16 TB.

O tipo de disco pode ser *Zonal SSD Persistent Disks* ou *Zonal Standard Persistent Disks*. É possível emparelhar discos persistentes com um bucket do Google Storage ao "categorize os dados inativos em storage de objetos de baixo custo".

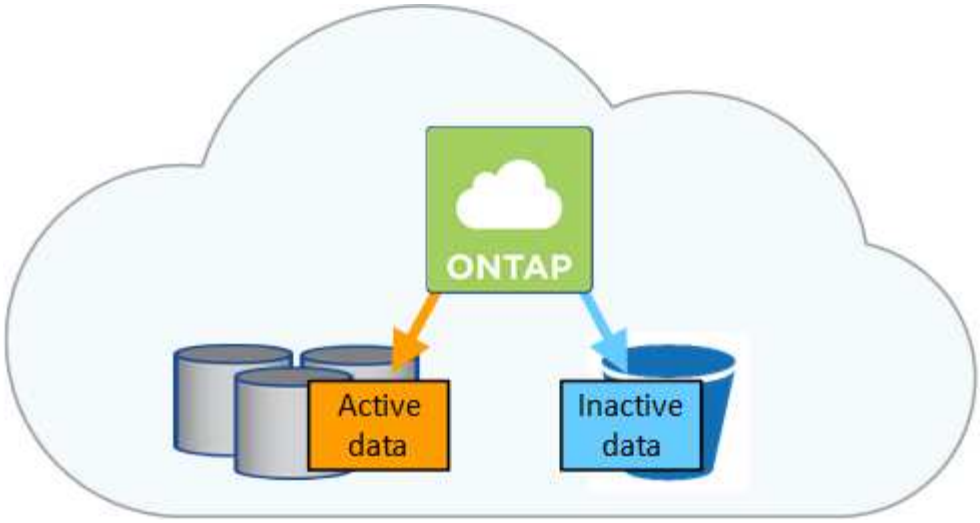
- Ligações relacionadas*
- "Documentação do Google Cloud Platform: Opções de armazenamento"
- "Analisar os limites de armazenamento do Cloud Volumes ONTAP na GCP"

Tipo de RAID

O tipo RAID para cada agregado Cloud Volumes ONTAP é RAID0 (striping). Nenhum outro tipo de RAID é suportado. A Cloud Volumes ONTAP conta com o fornecedor de nuvem para disponibilidade e durabilidade de disco.

Visão geral de categorização de dados

Reduza seus custos de storage habilitando a disposição automatizada de dados inativos em storage de objetos de baixo custo. Os dados ativos permanecem em SSDs ou HDDs de alta performance, enquanto os dados inativos são dispostos em camadas em storage de objetos de baixo custo. Isso permite recuperar espaço no storage primário e reduzir o storage secundário.



O Cloud Volumes ONTAP é compatível com categorização de dados na AWS, Azure e Google Cloud Platform. A disposição de dados em categorias é baseada na tecnologia FabricPool.

Não é necessário instalar uma licença de recurso para habilitar a disposição de dados em camadas (FabricPool).

Categorização de dados no AWS

Ao habilitar a disposição de dados em categorias na AWS, o Cloud Volumes ONTAP usa o EBS como uma camada de desempenho para dados ativos e o AWS S3 como uma camada de capacidade para dados inativos.

Camada de performance

A categoria de performance pode ser SSDs de uso geral, SSDs IOPS provisionados ou HDDs otimizados para taxa de transferência.

Camada de capacidade

Um sistema Cloud Volumes ONTAP classifica dados inativos em um único bucket do S3 usando a classe de armazenamento *Standard*. O padrão é ideal para dados acessados com frequência armazenados em várias zonas de disponibilidade.

O Cloud Manager cria um único bucket do S3 para cada ambiente de trabalho e o nomeia Fabric-pool-*cluster unique identifier*. Não é criado um bucket S3 diferente para cada volume.

Classes de armazenamento

A classe de armazenamento padrão para dados em camadas na AWS é *Standard*. Se você não planeja acessar os dados inativos, você pode reduzir seus custos de armazenamento alterando a classe de armazenamento para um dos seguintes: *Intelligent Tiering*, *One-Zone unless Access*, ou *Standard-Unfrequent Access*. Quando você altera a classe de armazenamento, os dados inativos começam na classe de armazenamento padrão e passam para a classe de armazenamento selecionada, se os dados não forem acessados após 30 dias.

Os custos de acesso são maiores se você acessar os dados, então leve isso em consideração antes de alterar a classe de storage. "Saiba mais sobre as classes de armazenamento do Amazon S3".

Você pode selecionar uma classe de armazenamento ao criar o ambiente de trabalho e pode alterá-la a qualquer momento. Para obter detalhes sobre como alterar a classe de armazenamento, "Disposição em

camadas dos dados inativos em storage de objetos de baixo custo"consulte .

A classe de storage para disposição de dados em categorias é de todo o sistema, não é por volume.

Categorização de dados no Azure

Ao habilitar a categorização de dados no Azure, o Cloud Volumes ONTAP usa discos gerenciados do Azure como uma categoria de performance para dados ativos e o storage Blob do Azure como uma categoria de capacidade para dados inativos.

Camada de performance

A camada de performance pode ser SSDs ou HDDs.

Camada de capacidade

Um sistema Cloud Volumes ONTAP categoriza dados inativos em um único contêiner de Blob usando a camada de storage *hot* do Azure. O hot Tier é ideal para dados acessados com frequência.

O Cloud Manager cria uma nova conta de storage com um único contêiner para cada ambiente de trabalho do Cloud Volumes ONTAP. O nome da conta de armazenamento é aleatório. Não é criado um recipiente diferente para cada volume.

Camadas de acesso ao storage

A camada de acesso de storage padrão para dados em camadas no Azure é o nível *hot*. Se você não planeja acessar os dados inativos, pode reduzir seus custos de storage mudando para a camada de storage *COOL*. Quando você altera a camada de storage, os dados inativos começam na camada de storage quente e passam para a camada de storage frio, se os dados não forem acessados após 30 dias.

Os custos de acesso são maiores se você acessar os dados, então leve isso em consideração antes de alterar a camada de storage. "Saiba mais sobre as camadas de acesso ao armazenamento Azure Blob".

Você pode selecionar uma camada de storage ao criar o ambiente de trabalho e alterá-la a qualquer momento. Para obter detalhes sobre como alterar a camada de storage, "Disposição em camadas dos dados inativos em storage de objetos de baixo custo"consulte .

A camada de acesso a storage para categorização de dados é de todo o sistema, não é por volume.

Categorização de dados no GCP

Ao habilitar a categorização de dados no GCP, o Cloud Volumes ONTAP usa discos persistentes como uma categoria de performance para dados ativos e um bucket do Google Cloud Storage como uma categoria de capacidade para dados inativos.

Camada de performance

A camada de performance pode ser SSDs ou HDDs (discos padrão).

Camada de capacidade

Um sistema Cloud Volumes ONTAP classifica os dados inativos em um único bucket do Google Cloud Storage usando a classe de storage *Regional*.

O Cloud Manager cria um único bucket para cada ambiente de trabalho e o nomeia Fabric-pool-*cluster unique identifier*. Não é criado um intervalo diferente para cada volume.

Classes de armazenamento

A classe de armazenamento padrão para dados em camadas é a classe *Standard Storage*. Se os dados forem acessados com pouca frequência, você poderá reduzir seus custos de armazenamento alterando para *Nearline Storage* ou *Coldline Storage*. Quando você altera a classe de armazenamento, os dados inativos começam na classe armazenamento padrão e passam para a classe de armazenamento selecionada, se os dados não forem acessados após 30 dias.

Os custos de acesso são maiores se você acessar os dados, então leve isso em consideração antes de alterar a classe de storage. "Saiba mais sobre as classes de armazenamento para o Google Cloud Storage".

Você pode selecionar uma camada de storage ao criar o ambiente de trabalho e alterá-la a qualquer momento. Para obter detalhes sobre como alterar a classe de armazenamento, "Disposição em camadas dos dados inativos em storage de objetos de baixo custo"consulte .

A classe de storage para disposição de dados em categorias é de todo o sistema, não é por volume.

Disposição de dados em categorias e limites de capacidade

Se você habilitar a disposição de dados em categorias, o limite de capacidade de um sistema permanecerá o mesmo. O limite se estende pela camada de performance e pela camada de capacidade.

Políticas de disposição em camadas de volume

Para habilitar a disposição de dados em categorias, você deve selecionar uma política de disposição em categorias de volume ao criar, modificar ou replicar um volume. Pode selecionar uma política diferente para cada volume.

Algumas políticas de disposição em categorias têm um período de resfriamento mínimo associado, que define o tempo em que os dados do usuário em um volume precisam permanecer inativos para que os dados sejam considerados "frios" e movidos para o nível de capacidade.

O Cloud Manager permite que você escolha uma das seguintes políticas de disposição em categorias de volume ao criar ou modificar um volume:

Apenas Snapshot

Depois que um agregado atinge a capacidade de 50%, o Cloud Volumes ONTAP classifica os dados inativos dos usuários das cópias Snapshot que não estão associados ao sistema de arquivos ativo à categoria de capacidade. O período de resfriamento é de aproximadamente 2 dias.

Se forem lidos, os blocos de dados inativos na camada de capacidade aquecem e são movidos para a categoria de performance.

Tudo

Todos os dados (não incluindo metadados) são imediatamente marcados como frios e dispostos em camadas no storage de objetos o mais rápido possível. Não há necessidade de esperar 48 horas para que novos blocos em um volume fiquem frios. Observe que os blocos localizados no volume antes da política tudo ser definida exigem 48 horas para ficarem frios.

Se lidos, os blocos de dados inativos na categoria de nuvem não são gravados de volta na categoria de performance. Esta política está disponível a partir do ONTAP 9.6.

Auto

Depois que um agregado atinge a capacidade de 50%, o Cloud Volumes ONTAP dispõe de blocos de

dados inativos em um volume para uma categoria de capacidade. Os dados inativos incluem não apenas cópias Snapshot, mas também dados de usuários inativos do sistema de arquivos ativo. O período de resfriamento é de aproximadamente 31 dias.

Esta política é suportada a partir do Cloud Volumes ONTAP 9,4.

Se forem lidos por leituras aleatórias, os blocos de dados inativos na camada de capacidade aquecem e migram para a camada de performance. Se forem lidos por leituras sequenciais, como as associadas a verificações de índice e antivírus, os blocos de dados inativos permanecem inativos e não se movem para o nível de desempenho.

Nenhum

Mantém os dados de um volume na categoria de performance, impedindo que ele seja migrado para a categoria de capacidade.

Ao replicar um volume, você pode escolher se deseja categorizar os dados em storage de objetos. Se o fizer, o Cloud Manager aplica a política **Backup** ao volume de proteção de dados. A partir do Cloud Volumes ONTAP 9,6, a política de disposição em camadas **All** substitui a política de backup.

A desativação do Cloud Volumes ONTAP afeta o período de resfriamento

Os blocos de dados são resfriados por exames de resfriamento. Durante este processo, os blocos que não foram usados têm a temperatura do bloco movida (resfriada) para o próximo valor mais baixo. O tempo de resfriamento padrão depende da política de disposição em categorias de volume:

- Auto: 31 dias
- Somente snapshot: 2 dias

O Cloud Volumes ONTAP deve estar em execução para que o exame de arrefecimento funcione. Se o Cloud Volumes ONTAP estiver desligado, o resfriamento também parará. Como resultado, você pode experimentar tempos de resfriamento mais longos.

Configuração de categorização de dados

Para obter instruções e uma lista de configurações suportadas, "Disposição em camadas dos dados inativos em storage de objetos de baixo custo"consulte .

Gerenciamento de storage

O Cloud Manager oferece gerenciamento simplificado e avançado do storage Cloud Volumes ONTAP.

> Todos os discos e agregados devem ser criados e excluídos diretamente do Cloud Manager. Você não deve executar essas ações de outra ferramenta de gerenciamento. Isso pode afetar a estabilidade do sistema, dificultar a capacidade de adicionar discos no futuro e, potencialmente, gerar taxas redundantes de provedores de nuvem.

Provisionamento de storage

O Cloud Manager facilita o provisionamento de storage para Cloud Volumes ONTAP comprando discos e gerenciando agregados para você. Você simplesmente precisa criar volumes. Você pode usar uma opção avançada de alocação para provisionar agregados, se desejar.

Provisionamento simplificado

Agregados fornecem storage de nuvem para volumes. O Cloud Manager cria agregados para você ao iniciar uma instância e ao provisionar volumes adicionais.

Quando você cria um volume, o Cloud Manager faz uma de três coisas:

- Ele coloca o volume em um agregado existente que tem espaço livre suficiente.
- Ele coloca o volume em um agregado existente comprando mais discos para esse agregado.
- Ele compra discos para um novo agregado e coloca o volume nesse agregado.

O Cloud Manager determina onde colocar um novo volume analisando vários fatores: O tamanho máximo de um agregado, se o thin Provisioning está habilitado e os limites de espaço livre para agregados.

O administrador da conta pode modificar limites de espaço livre a partir da página **Configurações**.

Seleção de tamanho de disco para agregados na AWS

Quando o Cloud Manager cria novos agregados para o Cloud Volumes ONTAP na AWS, ele aumenta gradualmente o tamanho do disco em um agregado, à medida que o número de agregados no sistema aumenta. O Cloud Manager faz isso para garantir que você possa utilizar a capacidade máxima do sistema antes de atingir o número máximo de discos de dados permitidos pela AWS.

Por exemplo, o Cloud Manager pode escolher os seguintes tamanhos de disco para agregados em um sistema Cloud Volumes ONTAP Premium ou BYOL:

Número agregado	Tamanho do disco	Capacidade de agregado máxima
1	500 MB	3 TB
4	1 TB	6 TB
6	2 TB	12 TB

Você pode escolher o tamanho do disco usando a opção de alocação avançada.

Alocação avançada

Em vez de permitir que o Cloud Manager gerencie agregados para você, você pode fazê-lo sozinho. "Na página **Alocação avançada**", você pode criar novos agregados que incluem um número específico de discos, adicionar discos a um agregado existente e criar volumes em agregados específicos.

Gerenciamento de capacidade

O administrador da conta pode escolher se o Cloud Manager notifica você sobre decisões de capacidade de storage ou se o Cloud Manager gerencia automaticamente os requisitos de capacidade para você. Pode ajudar você a entender como esses modos funcionam.

Gerenciamento automático de capacidade

Por padrão, o modo de gerenciamento de capacidade é definido como automático. Nesse modo, o Cloud Manager compra automaticamente novos discos para instâncias do Cloud Volumes ONTAP quando é necessária mais capacidade, exclui coleções não usadas de discos (agregados), move volumes entre

agregados quando necessário e tenta desfazer discos.

Os exemplos a seguir ilustram como esse modo funciona:

- Se um agregado com 5 ou menos discos EBS atingir o limite de capacidade, o Cloud Manager comprará automaticamente novos discos para esse agregado para que os volumes possam continuar a crescer.
- Se um agregado com 12 discos Azure atingir o limite de capacidade, o Cloud Manager moverá automaticamente um volume desse agregado para um agregado com capacidade disponível ou para um novo agregado.

  Se o Cloud Manager criar um novo agregado para o volume, ele escolherá um tamanho de disco que acomoda o tamanho desse volume.

  Note que o espaço livre está agora disponível no agregado original. Volumes existentes ou novos volumes podem usar esse espaço. O espaço não pode ser retornado à AWS, ao Azure ou ao GCP nesse cenário.

- Se um agregado não contiver volumes por mais de 12 horas, o Cloud Manager o excluirá.

Gerenciamento de LUNs com gerenciamento automático de capacidade

O gerenciamento automático de capacidade do Cloud Manager não se aplica a LUNs. Quando o Cloud Manager cria um LUN, ele desativa o recurso de crescimento automático.

Gestão de inodes com gestão automática de capacidade

O Cloud Manager monitora o uso de inode em um volume. Quando 85% dos inodes são usados, o Cloud Manager aumenta o tamanho do volume para aumentar o número de inodes disponíveis. O número de arquivos que um volume pode conter é determinado por quantos inodes ele tem.

Gerenciamento manual de capacidade

Se o administrador da conta definir o modo de gerenciamento de capacidade como manual, o Cloud Manager exibirá as mensagens Ação necessárias quando as decisões de capacidade devem ser tomadas. Os mesmos exemplos descritos no modo automático aplicam-se ao modo manual, mas cabe a você aceitar as ações.

Flash Cache

Algumas configurações do Cloud Volumes ONTAP na AWS e no Azure incluem o storage NVMe local, que o Cloud Volumes ONTAP usa como *Flash Cache* para melhorar a performance.

O que é Flash Cache?

O Flash Cache acelera o acesso aos dados por meio do armazenamento em cache inteligente em tempo real dos dados do usuário lidos recentemente e dos metadados do NetApp. Ele é eficaz para cargas de trabalho com uso intenso de leitura aleatória, incluindo bancos de dados, e-mail e serviços de arquivos.

Instâncias compatíveis na AWS

Selecione um dos seguintes tipos de instância do EC2 com um sistema Cloud Volumes ONTAP Premium ou BYOL novo ou existente:

- c5d.4xlarge

- c5d.9xlarge
- c5d.18xlarge
- m5d.8xlarge
- m5d.12xlarge
- r5d.2xlarge

Tipo de VM compatível no Azure

Selecione o tipo de VM Standard_L8s_v2 com um único sistema Cloud Volumes ONTAP BYOL no Azure.

Limitações

- A compactação deve ser desativada em todos os volumes para aproveitar as melhorias de desempenho do Flash Cache.

  Não escolha eficiência de storage ao criar um volume no Cloud Manager ou criar um volume e, em seguida "Desative a compressão de dados usando a CLI", .

- O reaquecimento do cache após uma reinicialização não é suportado com o Cloud Volumes ONTAP.

STORAGE WORM

Você pode ativar o storage WORM (uma gravação, muitas leituras) em um sistema Cloud Volumes ONTAP para reter arquivos de forma não modificada por um período de retenção especificado. O STORAGE WORM é baseado na tecnologia SnapLock no modo empresarial, o que significa que os arquivos WORM são protegidos no nível do arquivo.

Depois que um arquivo foi comprometido com o storage WORM, ele não poderá ser modificado, mesmo depois que o período de retenção expirou. Um relógio à prova de violação determina quando o período de retenção para um arquivo WORM expirou.

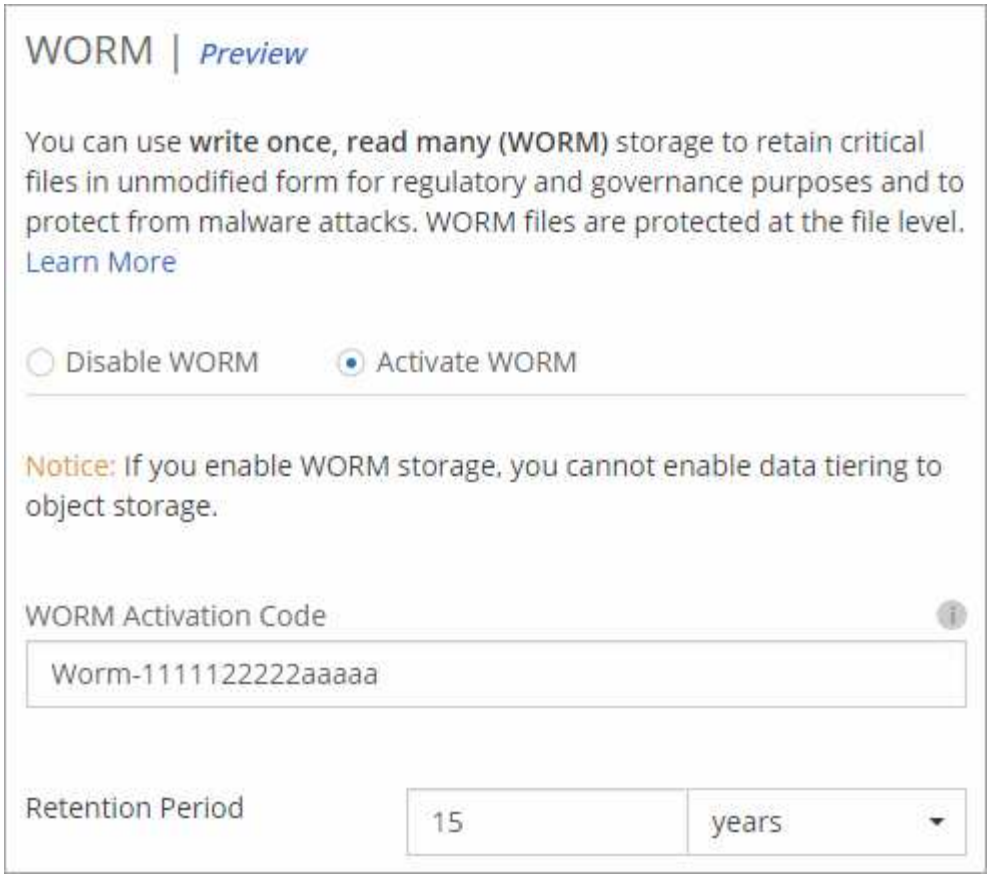
Após o período de retenção ter terminado, você é responsável por excluir quaisquer arquivos que você não precisa mais.

Ativar o storage WORM

Você pode ativar o storage WORM em um sistema Cloud Volumes ONTAP ao criar um novo ambiente de trabalho. Isso inclui especificar um código de ativação e definir o período de retenção padrão para arquivos. Você pode obter um código de ativação usando o ícone de bate-papo no canto inferior direito da interface do Cloud Manager.

Não é possível ativar o storage WORM em volumes individuais—WORM deve ser ativado no nível do sistema.

A imagem a seguir mostra como ativar o storage WORM ao criar um ambiente de trabalho:



Armazenando arquivos no WORM

Você pode usar uma aplicação para vincular arquivos ao WORM em NFS ou CIFS, ou usar a CLI da ONTAP para vincular automaticamente arquivos ao WORM. Você também pode usar um arquivo anexado WORM para reter dados gravados de forma incremental, como informações de log.

Depois de ativar o storage WORM em um sistema Cloud Volumes ONTAP, você precisa usar a CLI da ONTAP para todo o gerenciamento de storage WORM. Para obter instruções, "Documentação do ONTAP" consulte .

O suporte do Cloud Volumes ONTAP para storage WORM é equivalente ao modo SnapLock Enterprise.

Limitações

- Se você excluir ou mover um disco diretamente da AWS ou do Azure, um volume poderá ser excluído antes da data de expiração.
- Quando o storage WORM é ativado, a disposição de dados em categorias para storage de objetos não pode ser habilitada.
- O backup na nuvem deve ser desativado para habilitar o storage WORM.

Pares de alta disponibilidade

Pares de alta disponibilidade na AWS

Uma configuração de alta disponibilidade (HA) do Cloud Volumes ONTAP fornece operações ininterruptas e tolerância de falhas. Na AWS, os dados são espelhados de

forma síncrona entre os dois nós.

Visão geral

Na AWS, as configurações do Cloud Volumes ONTAP HA incluem os seguintes componentes:

- Dois nós de Cloud Volumes ONTAP cujos dados são espelhados de forma síncrona entre si.
- Uma instância de mediador que fornece um canal de comunicação entre os nós para auxiliar nos processos de takeover do storage e giveback.

> A instância mediadora executa o sistema operacional Linux em uma instância T2.micro e usa um disco magnético EBS que é de aproximadamente 8 GB.

Takeover de storage e giveback

Se um nó ficar inativo, o outro nó poderá fornecer dados para que seu parceiro forneça serviços de dados contínuos. Os clientes podem acessar os mesmos dados do nó do parceiro porque os dados foram espelhados de forma síncrona para o parceiro.

Depois que o nó for reiniciado, o parceiro deverá sincronizar novamente os dados antes que ele possa retornar o armazenamento. O tempo necessário para sincronizar novamente os dados depende da quantidade de dados alterados enquanto o nó estava inativo.

RPO e rto

Uma configuração de HA mantém a alta disponibilidade dos dados da seguinte forma:

- O objetivo do ponto de restauração (RPO) é de 0 segundos. Seus dados são consistentes transacionalmente, sem perda de dados.
- O objetivo de tempo de recuperação (rto) é de 60 segundos. Em caso de interrupção, os dados devem estar disponíveis em 60 segundos ou menos.

Modelos de IMPLANTAÇÃO DE HA

Você pode garantir a alta disponibilidade de seus dados implantando uma configuração de HA em várias zonas de disponibilidade (AZs) ou em uma única AZ. Você deve rever mais detalhes sobre cada configuração para escolher qual melhor se adapta às suas necessidades.

Cloud Volumes ONTAP HA em várias zonas de disponibilidade

A implantação de uma configuração de HA em várias zonas de disponibilidade (AZs) garante alta disponibilidade de seus dados se ocorrer uma falha com uma AZ ou uma instância que execute um nó Cloud Volumes ONTAP. Você deve entender como os endereços IP nas afetam o acesso aos dados e o failover de storage.

Acesso a dados NFS e CIFS

Quando uma configuração de HA é espalhada por várias zonas de disponibilidade, *endereços IP flutuantes* ativa o acesso do cliente nas. Os endereços IP flutuantes, que devem estar fora dos blocos CIDR para todos os VPCs na região, podem migrar entre nós quando ocorrem falhas. Eles não são acessíveis nativamente para clientes que estão fora da VPC, a menos que você "Configure um gateway de trânsito da AWS".

Se não for possível configurar um gateway de trânsito, os endereços IP privados estarão disponíveis para

clientes nas que estejam fora da VPC. No entanto, esses endereços IP são estáticos – eles não podem fazer failover entre nós.

Você deve analisar os requisitos para endereços IP flutuantes e tabelas de rota antes de implantar uma configuração de HA em várias zonas de disponibilidade. Você deve especificar os endereços IP flutuantes ao implantar a configuração. Os endereços IP privados são criados automaticamente pelo Cloud Manager.

Para obter detalhes, "Requisitos de rede da AWS para o Cloud Volumes ONTAP HA em vários AZs"consulte .

Acesso a dados iSCSI

A comunicação de dados entre VPC não é um problema, uma vez que o iSCSI não usa endereços IP flutuantes.

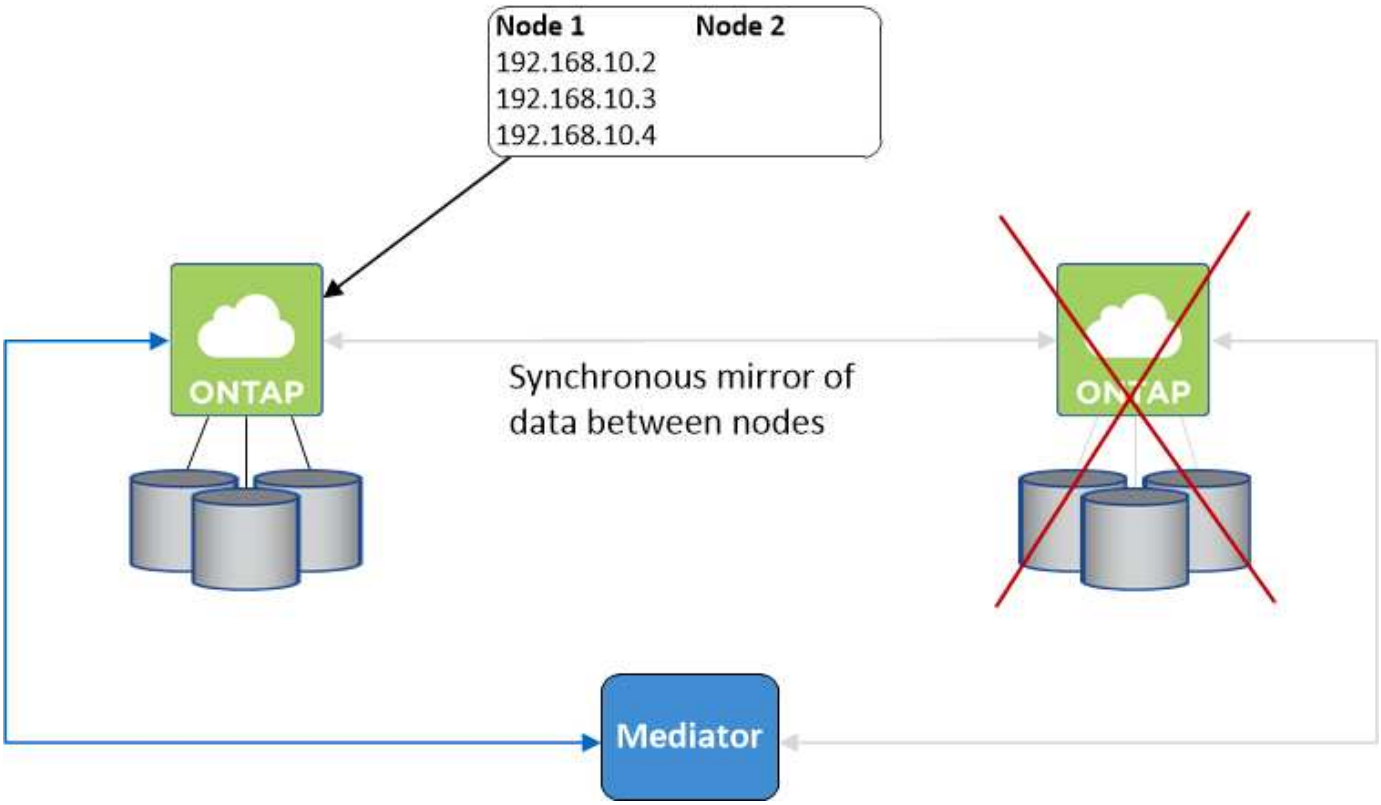
Takeover de storage e giveback para iSCSI

Para iSCSI, o Cloud Volumes ONTAP usa e/S multipath (MPIO) e Acesso de Unidade lógica assimétrica (ALUA) para gerenciar o failover de caminho entre os caminhos otimizados para ativos e não otimizados.

Para obter informações sobre quais configurações de host específicas suportam ALUA, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp" e o Guia de instalação e configuração de Utilitários de host do sistema operacional do seu host.

Takeover de storage e giveback para nas

Quando o controle ocorre em uma configuração nas usando IPs flutuantes, o endereço IP flutuante do nó que os clientes usam para acessar dados se move para o outro nó. A imagem a seguir mostra a aquisição de armazenamento em uma configuração nas usando IPs flutuantes. Se o nó 2 descer, o endereço IP flutuante do nó 2 será movido para o nó 1.



Os IPs de dados nas usados para acesso VPC externo não podem migrar entre nós se ocorrerem falhas. Se um nó ficar offline, você deverá remontar manualmente os volumes para clientes fora da VPC usando o endereço IP no outro nó.

Depois que o nó com falha voltar online, remonte os clientes para volumes usando o endereço IP original. Essa etapa é necessária para evitar a transferência de dados desnecessários entre dois nós de HA, o que pode causar impactos significativo no desempenho e na estabilidade.

Você pode identificar facilmente o endereço IP correto do Cloud Manager selecionando o volume e clicando em **Mount Command**.

Cloud Volumes ONTAP HA em uma única zona de disponibilidade

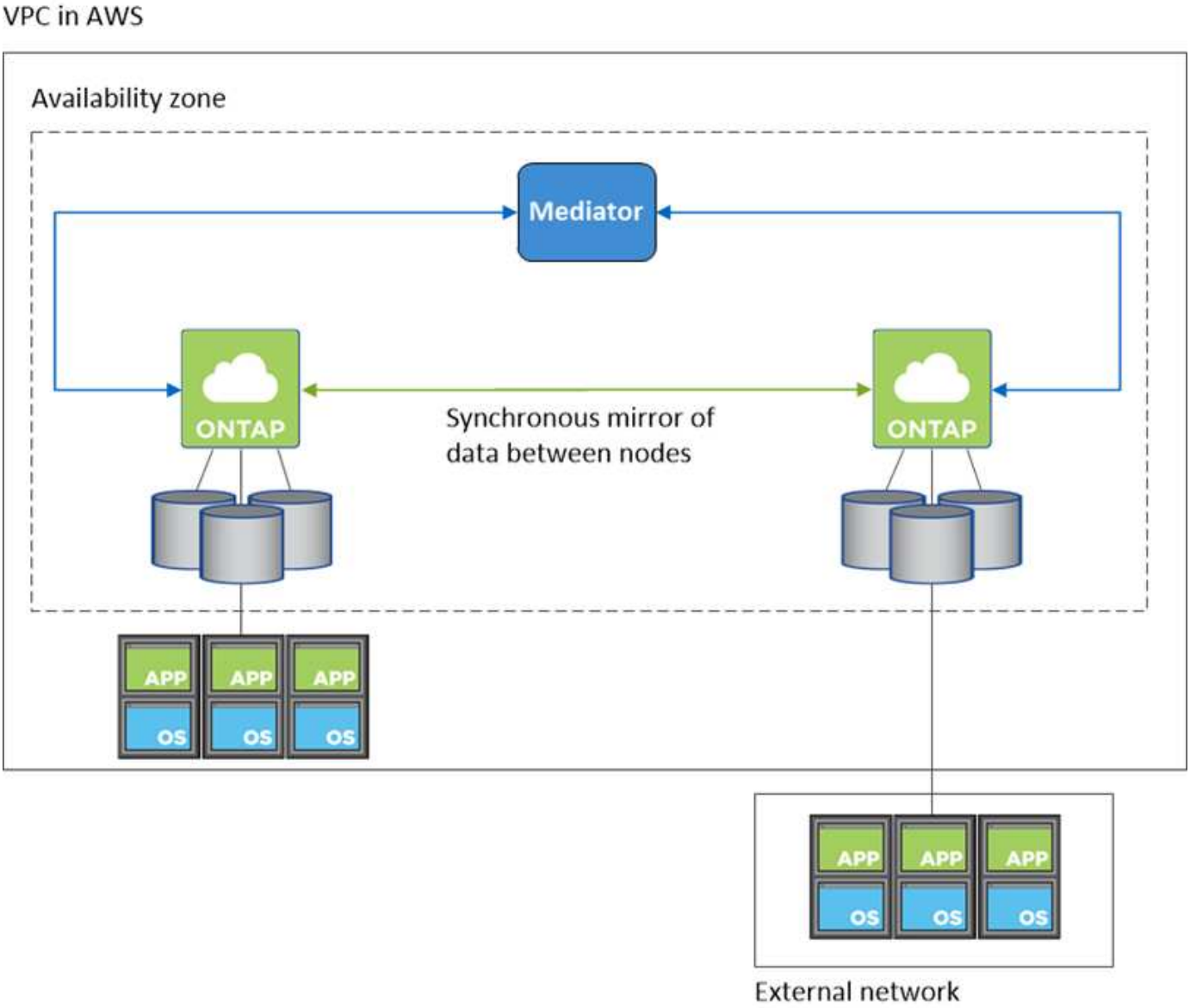
A implantação de uma configuração de HA em uma única zona de disponibilidade (AZ) pode garantir alta disponibilidade de seus dados se uma instância que executa um nó Cloud Volumes ONTAP falhar. Todos os dados podem ser acessados de forma nativa de fora da VPC.

> O Cloud Manager cria um "Grupo de posicionamento do AWS Spread" e lança os dois nós de HA nesse grupo de posicionamento. O grupo de posicionamento reduz o risco de falhas simultâneas, espalhando as instâncias por um hardware subjacente distinto. Esse recurso melhora a redundância do ponto de vista da computação e não do ponto de vista da falha de disco.

Acesso a dados

Como essa configuração está em uma única AZ, ela não requer endereços IP flutuantes. Você pode usar o mesmo endereço IP para acesso a dados a partir da VPC e de fora da VPC.

A imagem a seguir mostra uma configuração de HA em uma única AZ. Os dados são acessíveis a partir da VPC e de fora da VPC.



Takeover de storage e giveback

Para iSCSI, o Cloud Volumes ONTAP usa e/S multipath (MPIO) e Acesso de Unidade lógica assimétrica (ALUA) para gerenciar o failover de caminho entre os caminhos otimizados para ativos e não otimizados.

> Para obter informações sobre quais configurações de host específicas suportam ALUA, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp" e o Guia de instalação e configuração de Utilitários de host do sistema operacional do seu host.

Para configurações nas, os endereços IP de dados podem migrar entre nós de HA se ocorrerem falhas. Isso garante o acesso do cliente ao armazenamento.

Como o storage funciona em um par de HA

Ao contrário de um cluster do ONTAP, o storage em um par de HA do Cloud Volumes ONTAP não é compartilhado entre nós. Em vez disso, os dados são espelhados de forma síncrona entre os nós para que os dados estejam disponíveis em caso de falha.

Alocação de armazenamento

Quando você cria um novo volume e são necessários discos adicionais, o Cloud Manager aloca o mesmo número de discos para ambos os nós, cria um agregado espelhado e cria o novo volume. Por exemplo, se forem necessários dois discos para o volume, o Cloud Manager aloca dois discos por nó para um total de quatro discos.

Configurações de storage

Você pode usar um par de HA como uma configuração ativo-ativo, na qual ambos os nós fornecem dados aos clientes ou como uma configuração ativo-passivo, na qual o nó passivo responde a solicitações de dados somente se ele tiver ocupado o storage para o nó ativo.

Você só pode configurar uma configuração ativo-ativo quando usar o Cloud Manager na visualização do sistema de armazenamento.

Expectativas de performance para uma configuração de HA

Uma configuração do Cloud Volumes ONTAP HA replica sincronamente os dados entre nós, o que consome a largura de banda da rede. Como resultado, você pode esperar o seguinte desempenho em comparação com uma configuração de Cloud Volumes ONTAP de nó único:

- Para configurações de HA que atendem dados de apenas um nó, a performance de leitura é comparável à performance de leitura de uma configuração de nó único, enquanto a performance de gravação é menor.
- Para configurações de HA que atendem dados de ambos os nós, a performance de leitura é superior à performance de leitura de uma configuração de nó único, e a performance de gravação é igual ou superior.

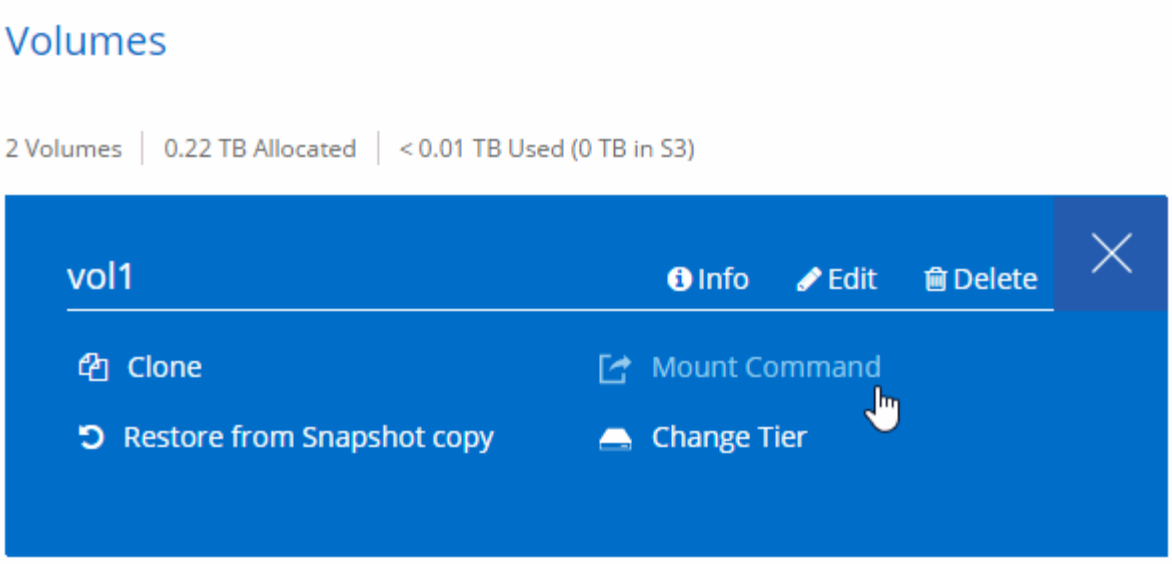
Para obter mais detalhes sobre o desempenho do Cloud Volumes ONTAP, "Desempenho"consulte .

Acesso do cliente ao armazenamento

Os clientes devem acessar volumes NFS e CIFS usando o endereço IP de dados do nó no qual o volume reside. Se os clientes nas acessarem um volume usando o endereço IP do nó do parceiro, o tráfego vai entre os dois nós, o que reduz o desempenho.

Se você mover um volume entre nós em um par de HA, remonte o volume usando o endereço IP do outro nó. Caso contrário, você pode experimentar desempenho reduzido. Se os clientes suportarem referências NFSv4 ou redirecionamento de pastas para CIFS, você pode habilitar esses recursos nos sistemas Cloud Volumes ONTAP para evitar a reinstalação do volume. Para obter detalhes, consulte a documentação do ONTAP.

Você pode identificar facilmente o endereço IP correto do Cloud Manager:

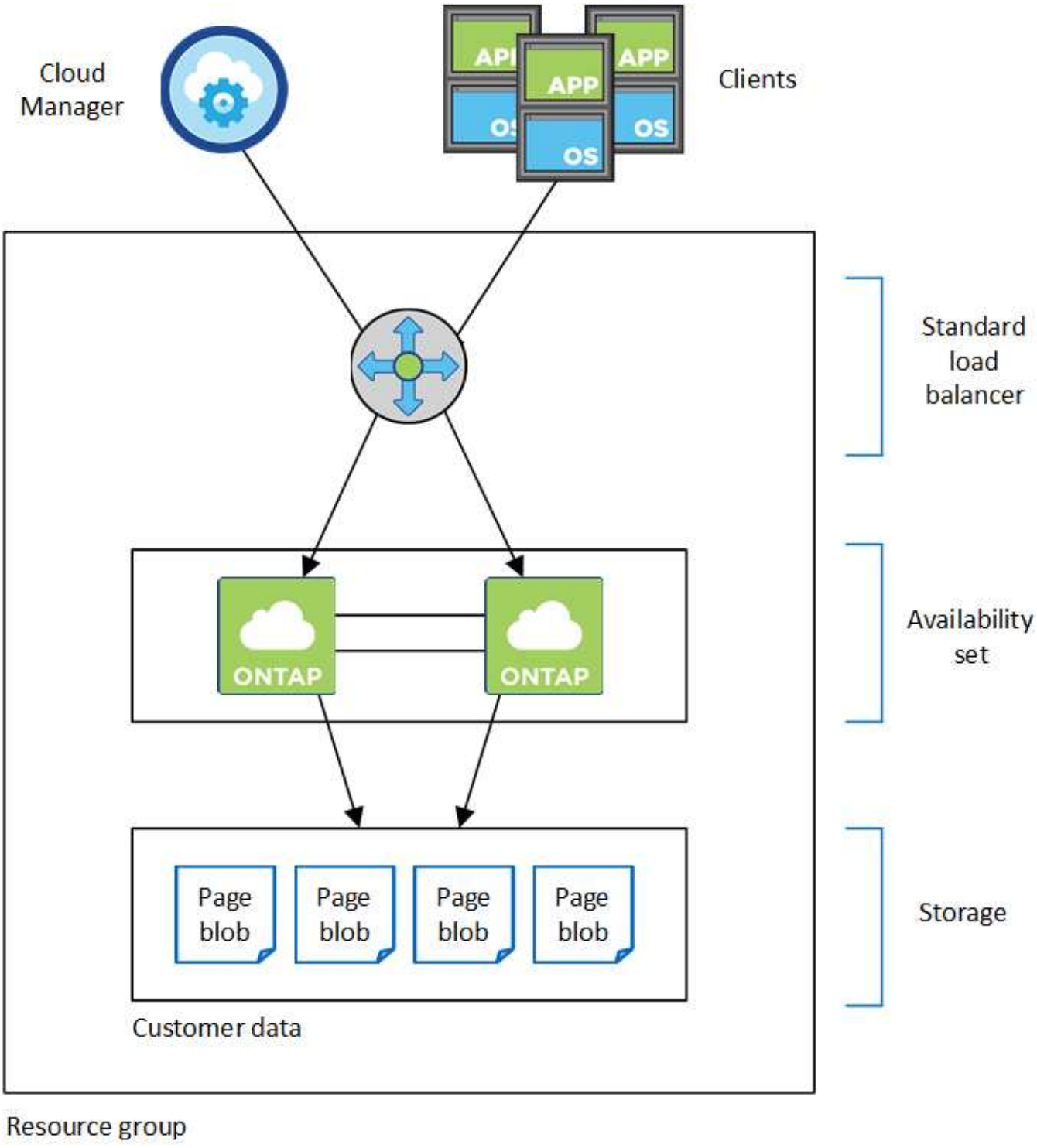


Pares de alta disponibilidade no Azure

Um par de alta disponibilidade (HA) da Cloud Volumes ONTAP fornece confiabilidade empresarial e operações contínuas em caso de falhas em seu ambiente de nuvem. No Azure, o storage é compartilhado entre os dois nós.

Componentes HA

Uma configuração do Cloud Volumes ONTAP HA no Azure inclui os seguintes componentes:



Observe o seguinte sobre os componentes do Azure que o Cloud Manager implanta para você:

Azure Standard Load Balancer

O balanceador de carga gerencia o tráfego de entrada para o par de HA do Cloud Volumes ONTAP.

Disponibilidade definida

O conjunto de disponibilidade garante que os nós estejam em diferentes domínios de falha e atualização.

Discos

Os dados do cliente residem nos blobs da página do Premium Storage. Cada nó tem acesso ao storage do outro nó. Também é necessário armazenamento adicional para "dados de inicialização, raiz e núcleo"o .

Contas de armazenamento

- Uma conta de armazenamento é necessária para discos gerenciados.
- Uma ou mais contas de armazenamento são necessárias para os blobs de página de armazenamento Premium, uma vez que o limite de capacidade de disco por conta de armazenamento é atingido.

  "Documentação do Azure: Escalabilidade do Azure Storage e metas de desempenho para contas de storage".

- Uma conta de storage é necessária para a disposição de dados em categorias no storage Azure Blob.
- A partir do Cloud Volumes ONTAP 9,7, as contas de storage criadas pelo Cloud Manager para pares de HA são contas de storage v2 de uso geral.
- Você pode habilitar uma conexão HTTPS de um par de HA do Cloud Volumes ONTAP 9,7 para contas de storage do Azure ao criar um ambiente de trabalho. Observe que ativar essa opção pode afetar o desempenho de gravação. Não é possível alterar a configuração depois de criar o ambiente de trabalho.

RPO e rto

Uma configuração de HA mantém a alta disponibilidade dos dados da seguinte forma:

- O objetivo do ponto de restauração (RPO) é de 0 segundos. Seus dados são consistentes transacionalmente, sem perda de dados.
- O objetivo de tempo de recuperação (rto) é de 60 segundos. Em caso de interrupção, os dados devem estar disponíveis em 60 segundos ou menos.

Takeover de storage e giveback

Semelhante a um cluster físico do ONTAP, o storage em um par de HA do Azure é compartilhado entre nós. As conexões com o armazenamento do parceiro permitem que cada nó acesse o armazenamento do outro no caso de um *takeover*. Os mecanismos de failover de caminho de rede garantem que os clientes e hosts continuem a se comunicar com o nó sobrevivente. O parceiro *devolve* armazenamento quando o nó é colocado de volta na linha.

Para configurações nas, os endereços IP de dados são migrados automaticamente entre nós de HA se ocorrerem falhas.

Para iSCSI, o Cloud Volumes ONTAP usa e/S multipath (MPIO) e Acesso de Unidade lógica assimétrica (ALUA) para gerenciar o failover de caminho entre os caminhos otimizados para ativos e não otimizados.

Para obter informações sobre quais configurações de host específicas suportam ALUA, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp" e o Guia de instalação e configuração de Utilitários de host do sistema operacional do seu host.

Configurações de storage

Você pode usar um par de HA como uma configuração ativo-ativo, na qual ambos os nós fornecem dados aos clientes ou como uma configuração ativo-passivo, na qual o nó passivo responde a solicitações de dados somente se ele tiver ocupado o storage para o nó ativo.

Limitações DE HA

As limitações a seguir afetam os pares de HA do Cloud Volumes ONTAP no Azure:

- Os pares DE HA são compatíveis com o padrão Cloud Volumes ONTAP, Premium e BYOL. Explorar não é suportado.
- NFSv4 não é suportado. NFSv3 é suportado.
- Pares HA não são suportados em algumas regiões.

  "Consulte a lista de regiões do Azure suportadas".

"Saiba como implantar um sistema HA no Azure".

A avaliar

Você pode avaliar o Cloud Volumes ONTAP antes de pagar pelo software. A maneira mais comum é lançar a versão PAYGO do seu primeiro sistema Cloud Volumes ONTAP para obter uma avaliação gratuita de 30 dias. Uma licença BYOL de avaliação também é uma opção.

Se você precisar de ajuda com sua prova de conceito, entre em Contato "A equipa de vendas" ou entre em Contato com a opção de bate-papo disponível "Centro de nuvem da NetApp" de e no Cloud Manager.

Avaliações gratuitas de 30 dias para PAYGO

Uma avaliação gratuita de 30 dias está disponível se você planeja pagar pelo Cloud Volumes ONTAP conforme você for. Você pode iniciar uma avaliação gratuita de 30 dias do Cloud Volumes ONTAP usando o Cloud Manager criando seu primeiro sistema Cloud Volumes ONTAP na conta de um pagador.

Não há cobranças de licença de software por hora para a instância, mas as cobranças de infraestrutura do seu provedor de nuvem ainda se aplicam.

Uma avaliação gratuita se converte automaticamente em uma assinatura paga por hora quando expira. Se você encerrar a instância dentro do limite de tempo, a próxima instância que você implantar não faz parte da avaliação gratuita (mesmo que ela seja implantada dentro desses 30 dias).

Os testes de pagamento conforme o uso são concedidos por meio de um fornecedor de nuvem e não podem ser estendidos de forma alguma.

Licenças de avaliação para BYOL

Uma licença BYOL de avaliação é uma opção para clientes que esperam pagar pelo Cloud Volumes ONTAP comprando uma licença denominada da NetApp. Você pode obter uma licença de avaliação de sua equipe de conta, seu engenheiro de vendas ou seu parceiro.

A chave de avaliação é boa por 30 dias, e pode ser usada várias vezes, cada uma por 30 dias (independentemente do dia de criação).

No final de 30 dias, desligamentos diários ocorrerão, por isso é melhor Planejar com antecedência. Você pode aplicar uma nova licença BYOL em cima da licença de avaliação para uma atualização no local (isso requer uma reinicialização de sistemas de nó único). Seus dados hospedados são **não** excluídos no final do período de teste.

Não é possível atualizar o software Cloud Volumes ONTAP ao usar uma licença de avaliação.

Licenciamento

Cada sistema BYOL do Cloud Volumes ONTAP deve ter uma licença de sistema instalada com uma assinatura ativa. O Cloud Manager simplifica o processo gerenciando licenças para você e notificando-o antes que elas expirem. As licenças BYOL também estão disponíveis para o Backup to Cloud.

Licenças de sistema BYOL

Você pode comprar várias licenças para um sistema BYOL da Cloud Volumes ONTAP para alocar mais de 368 TB de capacidade. Por exemplo, você pode comprar duas licenças para alocar até 736 TB de capacidade para o Cloud Volumes ONTAP. Ou você pode comprar quatro licenças para obter até 1,4 PB.

O número de licenças que você pode comprar para um único sistema de nó ou par de HA é ilimitado.

Esteja ciente de que os limites de disco podem impedir que você alcance o limite de capacidade usando discos sozinhos. Você pode ir além do limite de disco pelo "disposição em camadas dos dados inativos no storage de objetos". Para obter informações sobre limites de disco, "Limites de armazenamento nas Notas de versão do Cloud Volumes ONTAP" consulte .

Gerenciamento de licenças para um novo sistema

Quando você cria um sistema BYOL, o Cloud Manager solicita o número de série da licença e da conta do site de suporte da NetApp. O Cloud Manager usa a conta para baixar o arquivo de licença do NetApp e instalá-lo no sistema Cloud Volumes ONTAP.

"Saiba como adicionar contas do site de suporte da NetApp ao Cloud Manager".

Se o Cloud Manager não puder acessar o arquivo de licença pela conexão segura à Internet, você poderá obter o arquivo sozinho e, em seguida, fazer o upload manual do arquivo para o Cloud Manager. Para obter instruções, "Gerenciamento de licenças BYOL para Cloud Volumes ONTAP"consulte .

Aviso de expiração da licença

O Cloud Manager avisa-o 30 dias antes de uma licença expirar e novamente quando a licença expirar. A imagem a seguir mostra um aviso de expiração de 30 dias:

Pode selecionar o ambiente de trabalho para rever a mensagem.

Se não renovar a licença a tempo, o sistema Cloud Volumes ONTAP desliga-se. Se você reiniciá-lo, ele se desliga novamente.

O Cloud Volumes ONTAP também pode notificá-lo por e-mail, um traphost SNMP ou servidor syslog usando notificações de eventos do EMS (sistema de Gerenciamento de Eventos). Para obter instruções, consulte "Guia expresso de configuração de EMS do ONTAP 9" .

Renovação da licença

Quando você renova uma assinatura BYOL entrando em Contato com um representante da NetApp, o Cloud Manager obtém automaticamente a nova licença do NetApp e a instala no sistema Cloud Volumes ONTAP.

Se o Cloud Manager não puder acessar o arquivo de licença pela conexão segura à Internet, você poderá obter o arquivo sozinho e, em seguida, fazer o upload manual do arquivo para o Cloud Manager. Para obter instruções, "Gerenciamento de licenças BYOL para Cloud Volumes ONTAP"consulte .

Licenças de backup BYOL

Uma licença de backup BYOL permite que você compre uma licença da NetApp para usar o backup na nuvem por um determinado período de tempo e por um espaço máximo de backup. Quando um dos limites for atingido, você precisará renovar a licença.

"Saiba mais sobre a licença BYOL do Backup to Cloud".

Segurança

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

Criptografia de dados em repouso

O Cloud Volumes ONTAP oferece suporte às seguintes tecnologias de criptografia:

- Soluções de criptografia NetApp (NVE e NAE)
- AWS Key Management Service
- Criptografia do Serviço de storage do Azure
- Criptografia padrão do Google Cloud Platform

Você pode usar as soluções de criptografia NetApp com criptografia nativa da AWS, Azure ou GCP, que criptografam dados no nível do hipervisor. Fazer isso forneceria criptografia dupla, que pode ser desejada para dados muito confidenciais. Quando os dados criptografados são acessados, eles não são criptografados duas vezes, uma no nível do hipervisor (usando chaves do provedor de nuvem) e outra vez usando soluções de criptografia NetApp (usando chaves de um gerenciador de chaves externo).

Soluções de criptografia NetApp (NVE e NAE)

O Cloud Volumes ONTAP é compatível com criptografia de volume NetApp (NVE) e criptografia agregada NetApp (NAE) com um gerenciador de chaves externo. NVE e NAE são soluções baseadas em software que permitem a criptografia de volumes em repouso compatível com FIPS (140-2) em conformidade com dados em repouso de volumes.

- O NVE criptografa os dados em repouso um volume por vez. Cada volume de dados tem sua própria chave de criptografia exclusiva.
- O NVE é uma extensão do NVE - ele criptografa os dados para cada volume e os volumes compartilham uma chave no agregado. O NAE também permite que blocos comuns em todos os volumes do agregado

sejam desduplicados.

Tanto o NVE quanto o NAE usam criptografia AES de 256 bits.

"Saiba mais sobre criptografia de volume NetApp e criptografia agregada NetApp".

A partir do Cloud Volumes ONTAP 9,7, os novos agregados terão a encriptação agregada NetApp (NAE) ativada por predefinição depois de configurar um gestor de chaves externo. Novos volumes que não fazem parte de um agregado NAE terão a criptografia de volume NetApp (NVE) ativada por padrão (por exemplo, se você tiver agregados existentes que foram criados antes de configurar um gerenciador de chaves externo).

Configurar um gerenciador de chaves suportado é o único passo necessário. Para obter instruções de configuração, "Criptografando volumes com soluções de criptografia NetApp"consulte .

AWS Key Management Service

Ao iniciar um sistema Cloud Volumes ONTAP na AWS, é possível ativar a criptografia de dados usando o "AWS Key Management Service (KMS)". O Cloud Manager solicita chaves de dados usando uma chave mestra do cliente (CMK).

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

Se você quiser usar essa opção de criptografia, certifique-se de que o AWS KMS esteja configurado adequadamente. Para obter detalhes, "Configurando o AWS KMS"consulte .

Criptografia do Serviço de storage do Azure

"Criptografia do Serviço de storage do Azure" Para dados em repouso é habilitado por padrão para dados do Cloud Volumes ONTAP no Azure. Nenhuma configuração é necessária.

Você pode criptografar discos gerenciados do Azure em sistemas Cloud Volumes ONTAP de nó único usando chaves externas de outra conta. Esse recurso é compatível com APIs do Cloud Manager.

Você só precisa adicionar o seguinte à solicitação de API ao criar o sistema de nó único:

```
"azureEncryptionParameters": {
      "key": <azure id of encryptionset>
  }
```

Chaves gerenciadas pelo cliente não são compatíveis com pares de HA do Cloud Volumes ONTAP.

Criptografia padrão do Google Cloud Platform

"Criptografia de dados em repouso do Google Cloud Platform" É ativado por padrão para o Cloud Volumes ONTAP. Nenhuma configuração é necessária.

Embora o Google Cloud Storage sempre criptografe seus dados antes de serem gravados no disco, você pode usar as APIs do Cloud Manager para criar um sistema Cloud Volumes ONTAP que use *chaves de criptografia gerenciadas pelo cliente*. Essas são as chaves que você gera e gerencia no GCP usando o Cloud Key Management Service. "Saiba mais".

Verificação de vírus ONTAP

Você pode usar a funcionalidade de antivírus integrada em sistemas ONTAP para proteger os dados contra o comprometimento por vírus ou outros códigos maliciosos.

A verificação de vírus do ONTAP, chamada *Vscan*, combina o melhor software antivírus de terceiros com recursos do ONTAP que oferecem a flexibilidade necessária para controlar quais arquivos são verificados e quando.

Para obter informações sobre fornecedores, software e versões compatíveis com o Vscan, consulte "Matriz de interoperabilidade do NetApp".

Para obter informações sobre como configurar e gerenciar a funcionalidade antivírus em sistemas ONTAP, consulte "Guia de configuração do antivírus do ONTAP 9".

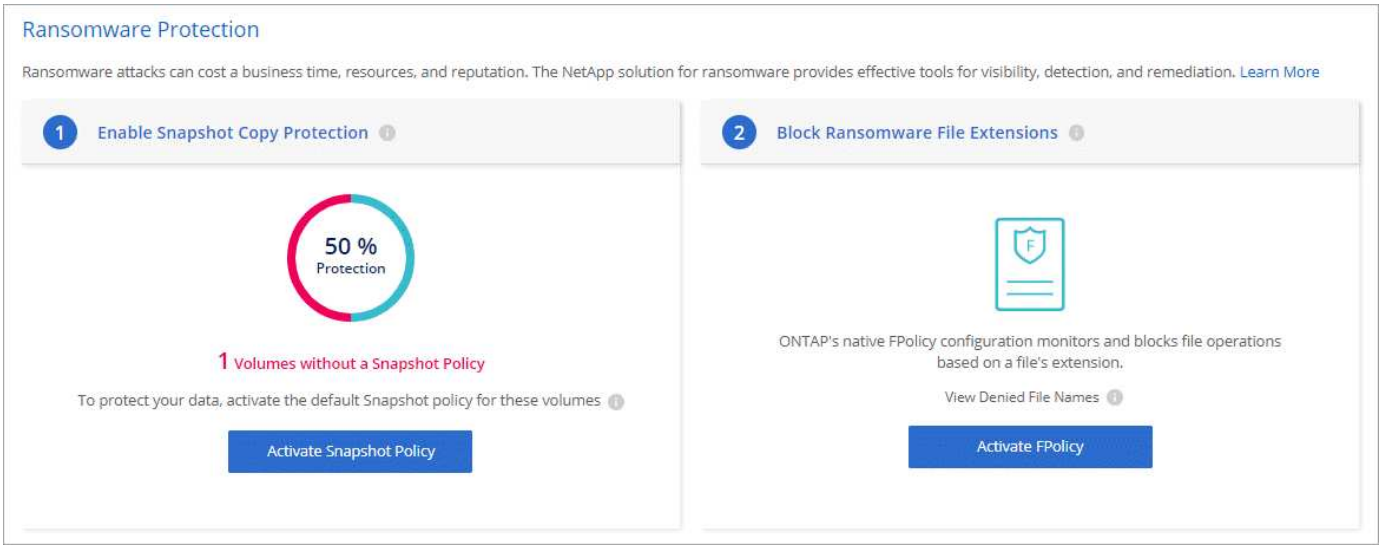
Proteção contra ransomware

Os ataques de ransomware podem custar tempo, recursos e reputação aos negócios. Com o Cloud Manager, você implementa a solução NetApp para ransomware, que fornece ferramentas eficazes de visibilidade, detecção e correção.

- O Cloud Manager identifica volumes que não estão protegidos por uma política do Snapshot e permite ativar a política padrão do Snapshot nesses volumes.

  As cópias snapshot são somente leitura, o que impede a corrupção de ransomware. Eles também podem fornecer a granularidade para criar imagens de uma única cópia de arquivo ou uma solução completa de recuperação de desastres.

- O Cloud Manager também permite bloquear extensões comuns de arquivos de ransomware habilitando a solução FPolicy da ONTAP.



"Saiba como implementar a solução NetApp para ransomware".

Desempenho

Você pode analisar os resultados de performance para decidir quais workloads são apropriados para o Cloud Volumes ONTAP.

- Cloud Volumes ONTAP para AWS

  "Relatório Técnico da NetApp 4383: Caraterização de desempenho do Cloud Volumes ONTAP em Serviços Web da Amazon com cargas de trabalho de aplicativos".

- Cloud Volumes ONTAP para Microsoft Azure

  "Relatório técnico da NetApp 4671: Caraterização de desempenho do Cloud Volumes ONTAP no Azure com cargas de trabalho de aplicação".

- Cloud Volumes ONTAP para Google Cloud

  "Relatório técnico da NetApp 4816: Caraterização de desempenho do Cloud Volumes ONTAP para o Google Cloud".

Configuração padrão para Cloud Volumes ONTAP

Entender como o Cloud Volumes ONTAP é configurado por padrão pode ajudá-lo a configurar e administrar seus sistemas, especialmente se você estiver familiarizado com o ONTAP porque a configuração padrão do Cloud Volumes ONTAP é diferente do ONTAP.

Predefinições

- O Cloud Volumes ONTAP está disponível como um sistema de nó único na AWS, Azure e GCP, além de par de HA na AWS e no Azure.
- O Cloud Manager cria uma VM de storage de fornecimento de dados quando implanta o Cloud Volumes ONTAP. Algumas configurações suportam VMs de storage adicionais. "Saiba mais sobre como gerenciar VMs de armazenamento".
- O Cloud Manager instala automaticamente as seguintes licenças de recurso do ONTAP no Cloud Volumes ONTAP:
  - CIFS
  - FlexCache
  - FlexClone
  - ISCSI
  - Criptografia de volume NetApp (somente para sistemas BYOL ou PAYGO registrados)
  - NFS
  - SnapMirror
  - SnapRestore
  - SnapVault
- Várias interfaces de rede são criadas por padrão:
  - Um LIF de gerenciamento de clusters
  - Um LIF entre clusters
  - LIF de gerenciamento de SVM em sistemas de HA no Azure, sistemas de nó único na AWS e, opcionalmente, em sistemas de HA em várias zonas de disponibilidade da AWS

- Um LIF de gerenciamento de nós
- Um iSCSI data LIF
- LIF de dados CIFS e NFS

> O failover de LIF é desativado por padrão para o Cloud Volumes ONTAP devido aos requisitos do EC2. A migração de um LIF para uma porta diferente rompe o mapeamento externo entre endereços IP e interfaces de rede na instância, tornando o LIF inacessível.

- O Cloud Volumes ONTAP envia backups de configuração para o conetor usando HTTPS.

  Os backups são acessíveis de https://ipaddress/occm/offboxconfig/ onde *ipaddress* é o endereço IP do host do conetor.

- O Cloud Manager define alguns atributos de volume de maneira diferente de outras ferramentas de gerenciamento (System Manager ou CLI, por exemplo).

  A tabela a seguir lista os atributos de volume que o Cloud Manager define de forma diferente dos padrões:

Atributo	Valor definido pelo Cloud Manager
Modo de tamanho automático	crescer
Dimensionamento automático máximo	1.000 por cento O Administrador da conta pode modificar este valor a partir da página Configurações.
Estilo de segurança	NTFS para volumes CIFS UNIX para volumes NFS
Estilo de garantia de espaço	nenhum
Permissões UNIX (somente NFS)	777

  Consulte a página man *volume create* para obter informações sobre esses atributos.

Dados de inicialização e raiz para Cloud Volumes ONTAP

Além do storage para dados de usuário, o Cloud Manager também compra storage de nuvem para dados de inicialização e raiz em cada sistema Cloud Volumes ONTAP.

AWS

- Dois discos por nó para dados de inicialização e raiz:

    - 9,7: Disco IO1 de 160 gb para dados de inicialização e um disco GP2 de 220 gb para dados de raiz
    - 9,6: Disco IO1 de 93 gb para dados de inicialização e um disco GP2 de 140 gb para dados de raiz
    - 9,5: Disco IO1 de 45 gb para dados de inicialização e um disco GP2 de 140 gb para dados de raiz
- Um instantâneo EBS para cada disco de arranque e disco raiz
- Para pares HA, um volume EBS para a instância Mediator, que é de aproximadamente 8 GB

Azure (nó único)

- Três discos SSD premium:
    - Um disco de 10 GB para dados de inicialização
    - Um disco de 140 GB para dados de raiz
    - Um disco de 128 GB para NVRAM

      Se a máquina virtual que você escolheu para o Cloud Volumes ONTAP oferecer suporte a SSDs Ultra, o sistema usará um SSD Ultra para NVRAM, em vez de um SSD Premium.
- Um disco rígido padrão de 1024 GB para guardar núcleos
- Um snapshot do Azure para cada disco de inicialização e disco raiz

Azure (pares de HA)

- Dois discos SSD premium de 10 GB para o volume de inicialização (um por nó)
- Dois blobs de página de armazenamento Premium de 140 GB para o volume raiz (um por nó)
- Dois discos HDD padrão de 1024 GB para guardar núcleos (um por nó)
- Dois discos SSD premium de 128 GB para NVRAM (um por nó)
- Um snapshot do Azure para cada disco de inicialização e disco raiz

GCP

- Um disco persistente padrão de 10 GB para dados de inicialização
- Um disco persistente padrão de 64 GB para dados de raiz
- Um disco persistente padrão de 500 GB para NVRAM
- Um disco persistente padrão de 216 GB para guardar núcleos
- Um snapshot do GCP para o disco de inicialização e o disco raiz

Onde residem os discos

O Cloud Manager estabelece o storage da seguinte forma:

- Os dados de inicialização residem em um disco conetado à instância ou à máquina virtual.

  Este disco, que contém a imagem de arranque, não está disponível para o Cloud Volumes ONTAP.
- Os dados de raiz, que contêm a configuração e os logs do sistema, residem no aggr0.
- O volume raiz da máquina virtual de storage (SVM) reside no aggr1.
- Os volumes de dados também residem em aggr1.

Criptografia

Os discos de inicialização e raiz são sempre criptografados no Azure e no Google Cloud Platform porque a criptografia é habilitada por padrão nesses provedores de nuvem.

Quando você ativa a criptografia de dados na AWS usando o Serviço de Gerenciamento de chaves (KMS), os discos de inicialização e raiz do Cloud Volumes ONTAP também são criptografados. Isso inclui o disco de inicialização da instância de mediador em um par de HA. Os discos são criptografados usando o CMK selecionado quando você cria o ambiente de trabalho.

Comece a usar a AWS

Introdução ao Cloud Volumes ONTAP para AWS

Comece a usar o Cloud Volumes ONTAP para AWS em algumas etapas.

Crie um conetor

Se você ainda não tem um"Conetor", um administrador de conta precisa criar um. "Saiba como criar um conetor na AWS".

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

Planeje sua configuração

O Cloud Manager oferece pacotes pré-configurados que correspondem aos seus requisitos de carga de trabalho, ou você pode criar sua própria configuração. Se você escolher sua própria configuração, você deve entender as opções disponíveis para você. "Saiba mais".

Configure a rede

1. Certifique-se de que a VPC e as sub-redes suportem a conetividade entre o conetor e o Cloud Volumes ONTAP.
2. Ative o acesso de saída à Internet a partir da VPC de destino para que o conetor e o Cloud Volumes ONTAP possam entrar em Contato com vários endpoints.

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

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

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

"Saiba mais sobre os requisitos de rede".

Configure o AWS KMS

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

Inicie o Cloud Volumes ONTAP usando o Cloud Manager

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

Links relacionados

- "A avaliar"
- "Criando um conetor do Cloud Manager"
- "Iniciando um conetor no AWS Marketplace"
- "Instalar o software Connector em um host Linux"
- "O que o Cloud Manager faz com as permissões da AWS"

Planejando sua configuração do Cloud Volumes ONTAP na AWS

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

Escolhendo um tipo de licença

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

"Configurações compatíveis com o Cloud Volumes ONTAP 9,7 na AWS"

Compreender os limites de armazenamento

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

"Limites de storage para o Cloud Volumes ONTAP 9,7 na AWS"

Dimensionamento do seu sistema na AWS

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

Tipo de instância

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

Tipo de disco EBS

SSDs de uso geral são o tipo de disco mais comum para Cloud Volumes ONTAP. Para visualizar os casos de uso de discos EBS, "Documentação da AWS: Tipos de volume do EBS" consulte .

Tamanho do disco EBS

Você precisa escolher um tamanho de disco inicial ao iniciar um sistema Cloud Volumes ONTAP. Depois disso, você pode "Deixe o Cloud Manager gerenciar a capacidade de um sistema para você", mas se quiser "construa agregados você mesmo", estar ciente do seguinte:

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

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

Assista ao vídeo a seguir para obter mais detalhes sobre como dimensionar seu sistema Cloud Volumes ONTAP na AWS:

[] | *https://img.youtube.com/vi/GELcXmOuYPw/maxresdefault.jpg*

Escolhendo uma configuração compatível com Flash Cache

Algumas configurações do Cloud Volumes ONTAP na AWS incluem o storage NVMe local, que o Cloud Volumes ONTAP usa como *Flash Cache* para obter melhor desempenho. "Saiba mais sobre o Flash Cache".

Planilha de informações de rede da AWS

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

Informações de rede para Cloud Volumes ONTAP

Informações da AWS	O seu valor
Região	

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

Informações de rede para um par de HA em várias AZs

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

Escolhendo uma velocidade de escrita

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

Diferença entre velocidade de gravação normal e alta velocidade de gravação

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

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

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

Quando usar alta velocidade de gravação

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

Recomendações ao usar alta velocidade de gravação

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

Escolhendo um perfil de uso de volume

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

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

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

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

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

Configure a rede

Requisitos de rede para o Cloud Volumes ONTAP na AWS

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

Requisitos gerais para o Cloud Volumes ONTAP

Os requisitos a seguir devem ser atendidos na AWS.

Acesso de saída à Internet para nós Cloud Volumes ONTAP

Os nós do Cloud Volumes ONTAP exigem acesso de saída à Internet para enviar mensagens para o NetApp AutoSupport, que monitora proativamente a integridade do storage.

As políticas de roteamento e firewall devem permitir o tráfego HTTP/HTTPS da AWS para os seguintes endpoints, para que o Cloud Volumes ONTAP possa enviar mensagens do AutoSupport:

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

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

  "Saiba como configurar o AutoSupport".

Acesso de saída à Internet para o mediador HA

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

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

Número de endereços IP

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

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

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

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

Grupos de segurança

Você não precisa criar grupos de segurança porque o Cloud Manager faz isso por você. Se você precisar usar o seu próprio, "Regras do grupo de segurança"consulte .

Conexão do Cloud Volumes ONTAP ao AWS S3 para categorização de dados

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

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

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

Conexões com sistemas ONTAP em outras redes

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

DNS e ative Directory para CIFS

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

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

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

Requisitos para pares de HA em várias AZs

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

Para entender como os pares de HA funcionam, "Pares de alta disponibilidade"consulte .

Zonas de disponibilidade

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

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

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

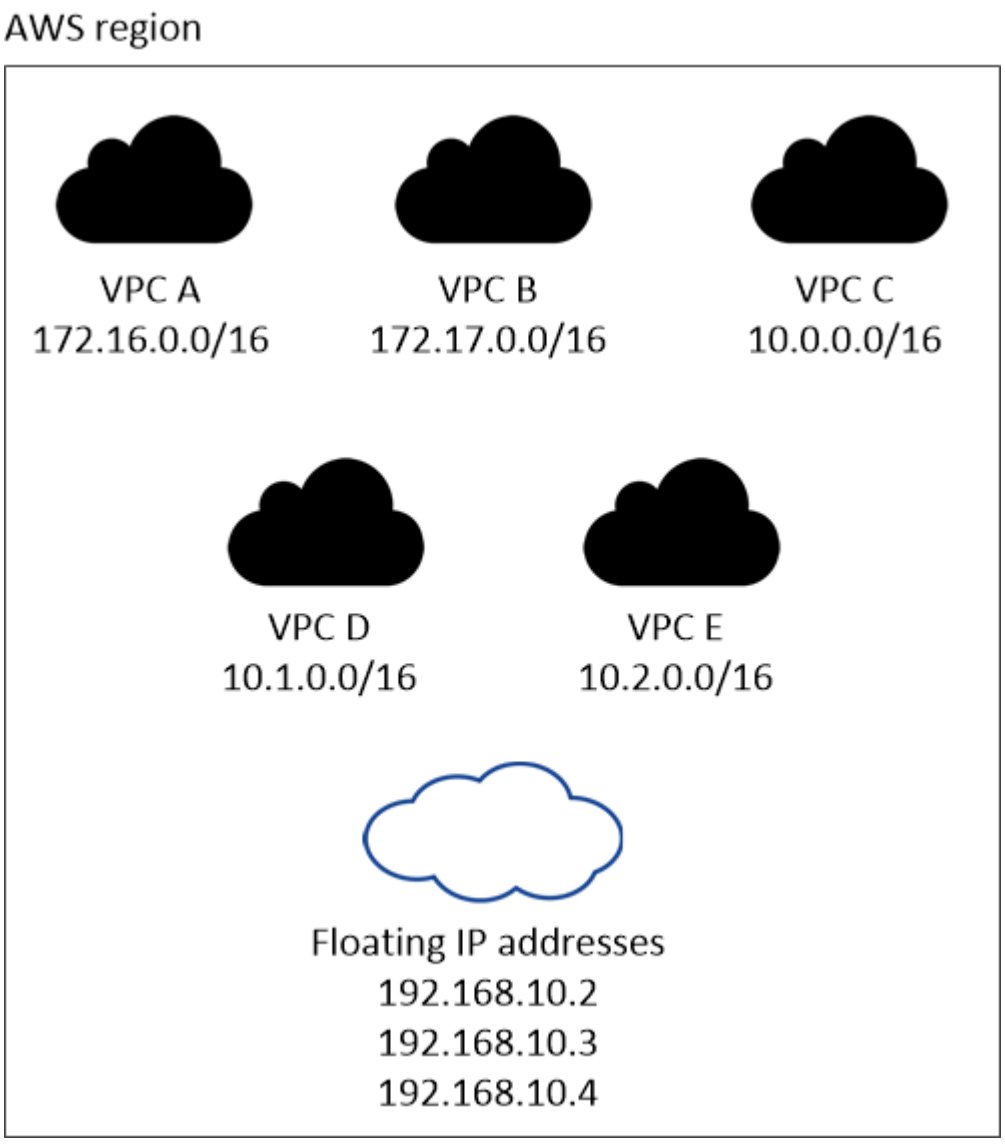
Um endereço IP flutuante é para gerenciamento de cluster, um para dados NFS/CIFS no nó 1 e outro para dados NFS/CIFS no nó 2. Um quarto endereço IP flutuante para gerenciamento de SVM é opcional.

> Um endereço IP flutuante é necessário para o LIF de gerenciamento da SVM se você usar o SnapDrive para Windows ou SnapCenter com o par de HA. Se você não especificar o endereço IP ao implantar o sistema, poderá criar o LIF mais tarde. Para obter detalhes, "Configurar o Cloud Volumes ONTAP"consulte .

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

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

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



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

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

"Configure um gateway de trânsito da AWS" Para habilitar o acesso aos endereços IP flutuantes de um par de HA de fora da VPC onde o par de HA reside.

Tabelas de rotas

Depois de especificar os endereços IP flutuantes no Cloud Manager, você precisa selecionar as tabelas de rota que devem incluir rotas para os endereços IP flutuantes. Isso permite o acesso do cliente ao par de

HA.

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

Por exemplo, você pode ter duas sub-redes associadas a tabelas de rota diferentes. Se você selecionar a tabela de rota A, mas não a tabela de rota B, os clientes na sub-rede associada à tabela de rota A podem acessar o par de HA, mas os clientes na sub-rede associada à tabela de rota B.

Para obter mais informações sobre tabelas de rotas, "Documentação da AWS: Tabelas de rotas" consulte .

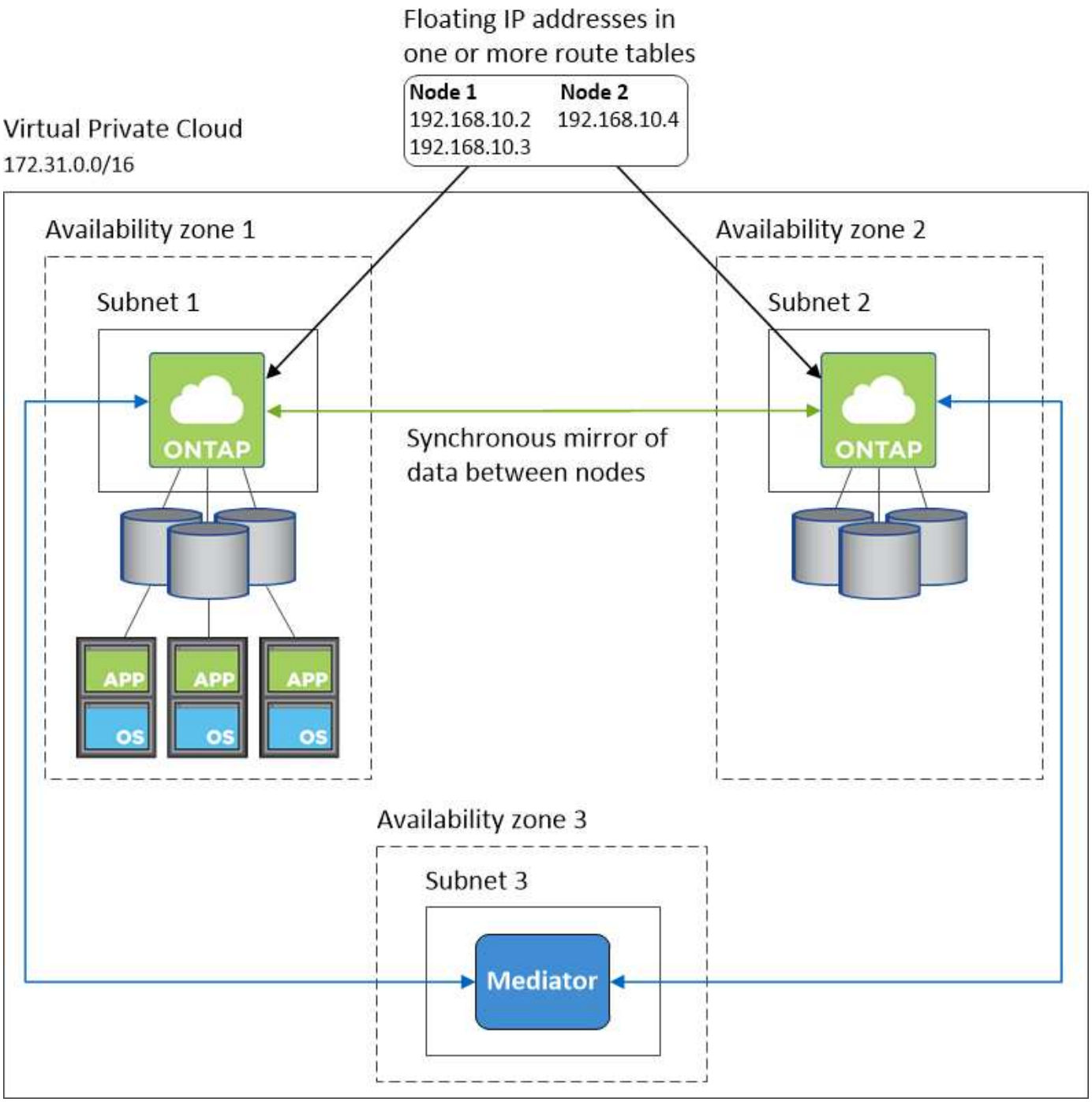
Conexão com ferramentas de gerenciamento do NetApp

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

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

Exemplo de configuração de HA

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



Requisitos para o conetor

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

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

Conexão com redes de destino

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

Volumes ONTAP.

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

Acesso de saída à Internet

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

Endpoints	Finalidade
Serviços da AWS (amazonaws.com): • CloudFormation • Nuvem de computação elástica (EC2) • Key Management Service (KMS) • Serviço de token de segurança (STS) • Serviço de armazenamento simples (S3) O endpoint exato depende da região em que você implementa o Cloud Volumes ONTAP. "Consulte a documentação da AWS para obter detalhes."	Permite que o Cloud Manager implante e gerencie o Cloud Volumes ONTAP na AWS.
https://api.services.cloud.NetApp.com:443	Solicitações de API para o NetApp Cloud Central.
https://cloud.support.NetApp.com.s3.us-west-1.amazonaws.com	Fornece acesso a imagens de software, manifestos e modelos.
https://repo.cloud.support.NetApp.com	Usado para baixar dependências do Cloud Manager.
http://repo.mysql.com/	Usado para baixar MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-NetApp-com-accelerated.s3.amazonaws.com	Permite que o Cloud Manager acesse e baixe manifestos, modelos e imagens de atualização do Cloud Volumes ONTAP.
https://cloudmanagerinfraprod.azurecr.io	Acesso a imagens de software de componentes de contentor para uma infraestrutura que esteja executando o Docker e fornece uma solução para integrações de serviços com o Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permite que o NetApp transmita dados de Registros de auditoria.
https://cloudmanager.cloud.NetApp.com	Comunicação com o serviço Cloud Manager, que inclui contas do Cloud Central.
https://NetApp-cloud-account.auth0.com	Comunicação com o NetApp Cloud Central para autenticação centralizada de usuários.

Endpoints	Finalidade
https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist	Usado para adicionar seu ID de conta da AWS à lista de usuários permitidos para Backup em S3.
https://support.NetApp.com/aods/asupmessage https://support.NetApp.com/asupprod/post/1,0/postAsup	Comunicação com NetApp AutoSupport.
https://support.NetApp.com/svcgw - https://support.NetApp.com/ServiceGW/Entitlement - https://eval.lic.NetApp.com.s3.us-west-1.amazonaws.com - https://cloud-support-NetApp-com.s3.us-west-1.amazonaws.com	Comunicação com o NetApp para licenciamento de sistema e Registro de suporte.
https://ipa-signer.cloudmanager.NetApp.com	Permite que o Cloud Manager gere licenças (por exemplo, uma licença FlexCache para Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/Trident/Releases/download/	Necessário para conectar sistemas Cloud Volumes ONTAP a um cluster Kubernetes. Os endpoints permitem a instalação do NetApp Trident.
Vários locais de terceiros, por exemplo: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org Locais de terceiros estão sujeitos a alterações.	Durante as atualizações, o Cloud Manager baixa os pacotes mais recentes para dependências de terceiros.

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

Endpoints	Finalidade
O host do conetor	Você deve inserir o endereço IP do host de um navegador da Web para carregar o console do Cloud Manager. Dependendo da sua conetividade com o seu provedor de nuvem, você pode usar o IP privado ou um IP público atribuído ao host: • Um IP privado funciona se você tiver uma VPN e acesso direto à sua rede virtual • Um IP público funciona em qualquer cenário de rede Em qualquer caso, você deve proteger o acesso à rede, garantindo que as regras do grupo de segurança permitam o acesso somente de IPs ou sub-redes autorizados.

Endpoints	Finalidade
https://auth0.com https://cdn.auth0.com://NetApp-cloud-account.auth0.com https://services.cloud.NetApp.com	Seu navegador da Web se coneta a esses endpoints para autenticação de usuário centralizada por meio do NetApp Cloud Central.
https://widget.intercom.io	Para um bate-papo no produto que permite conversar com especialistas em nuvem da NetApp.

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

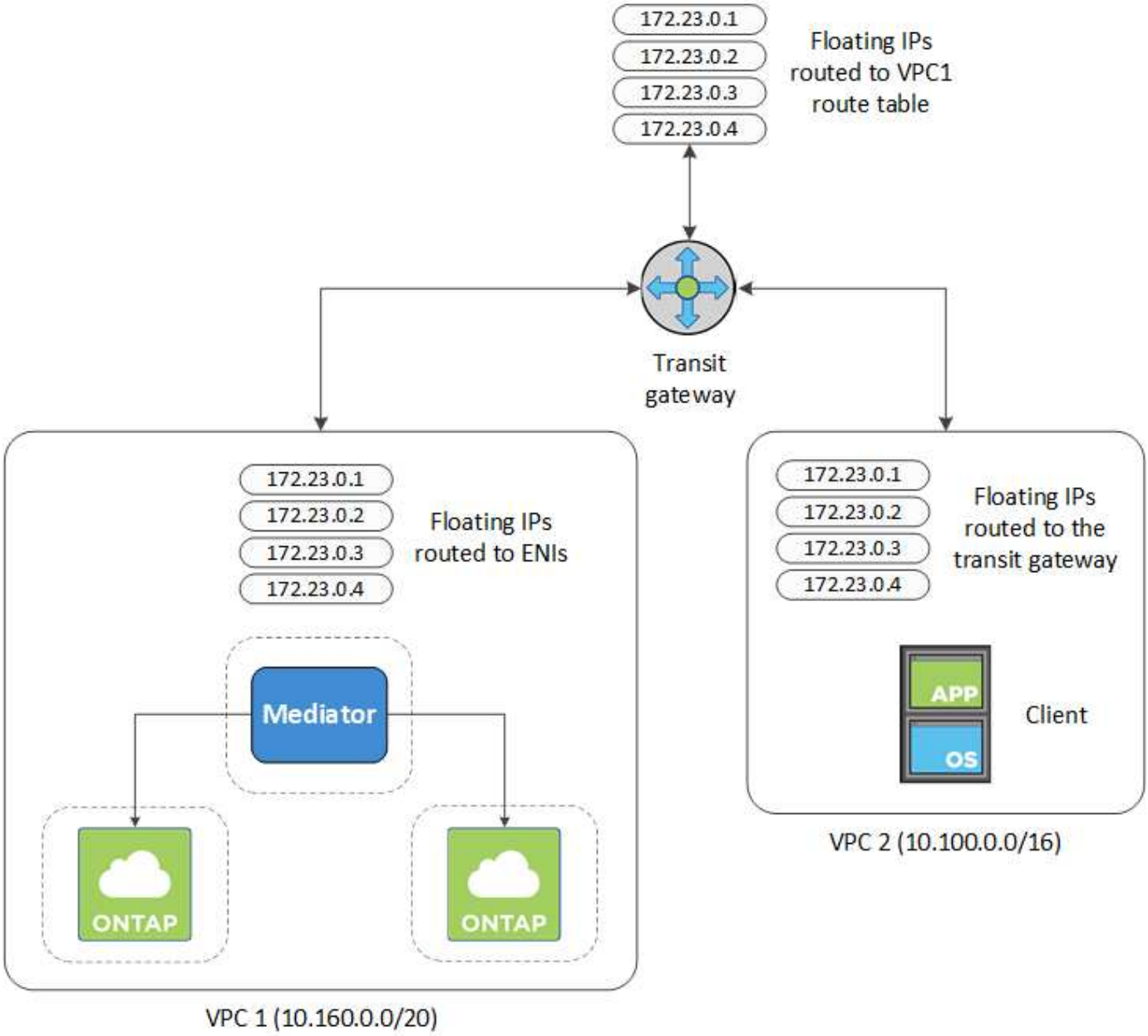
Configure um gateway de trânsito da AWS para permitir o acesso a um par de HA "Endereços IP flutuantes"de fora da VPC onde o par de HA reside.

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

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

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

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

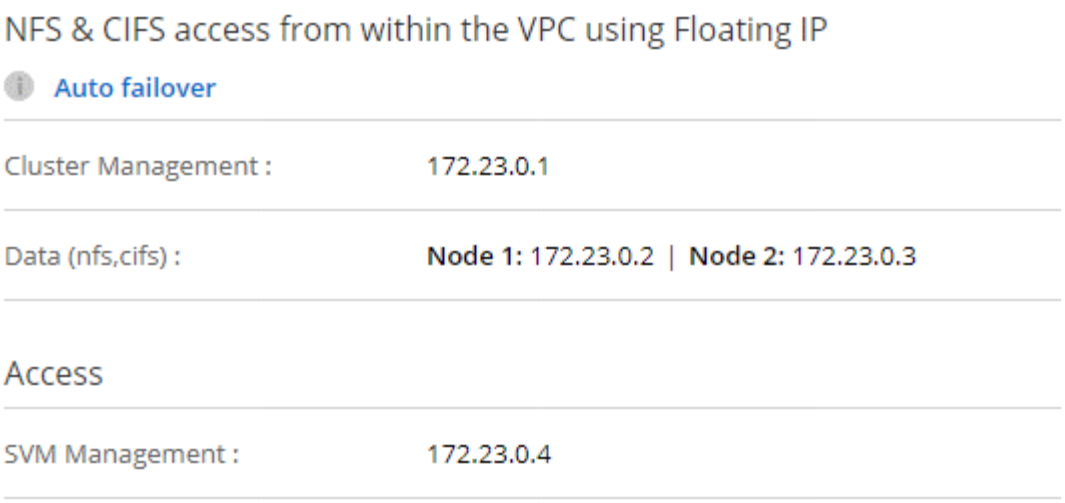


As etapas a seguir ilustram como configurar uma configuração semelhante.

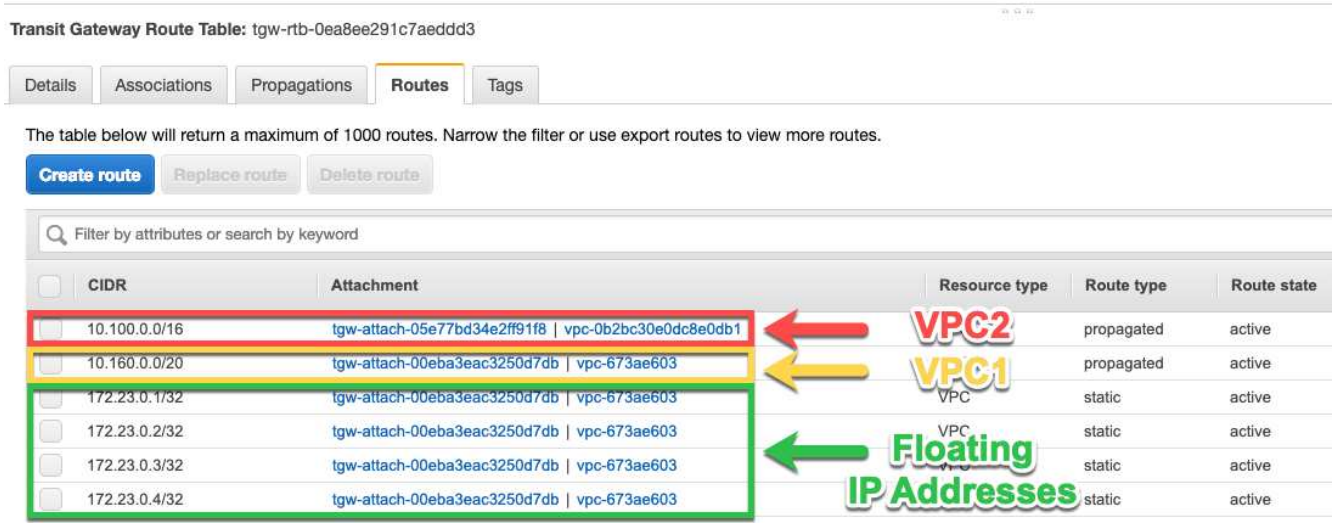
Passos

1. "Crie um gateway de trânsito e conete os VPCs ao gateway".
2. Crie rotas na tabela de rotas do gateway de trânsito especificando os endereços IP flutuantes do par HA.

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



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

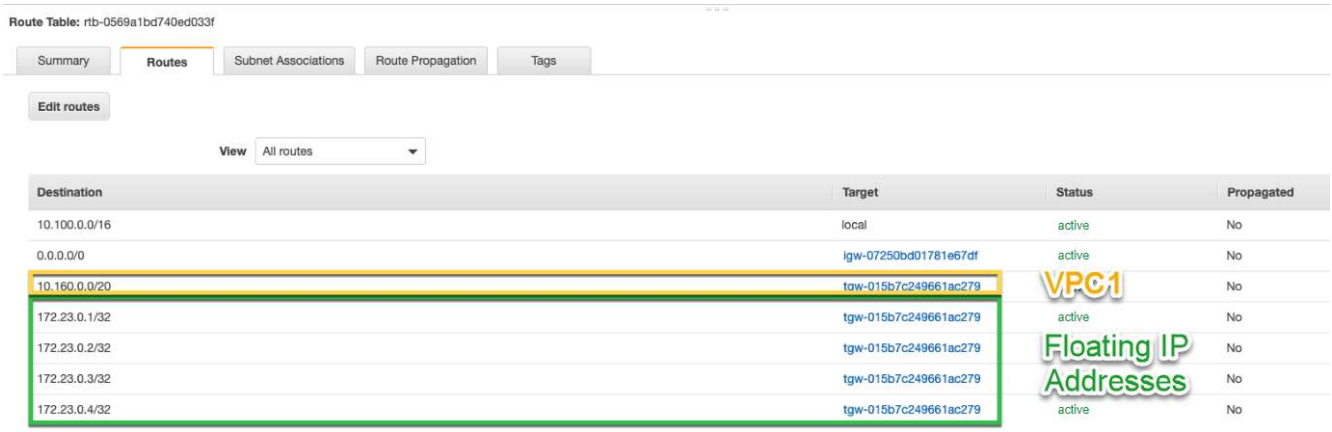


3. Modifique a tabela de rotas dos VPCs que precisam acessar os endereços IP flutuantes.

   a. Adicione entradas de rota aos endereços IP flutuantes.

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

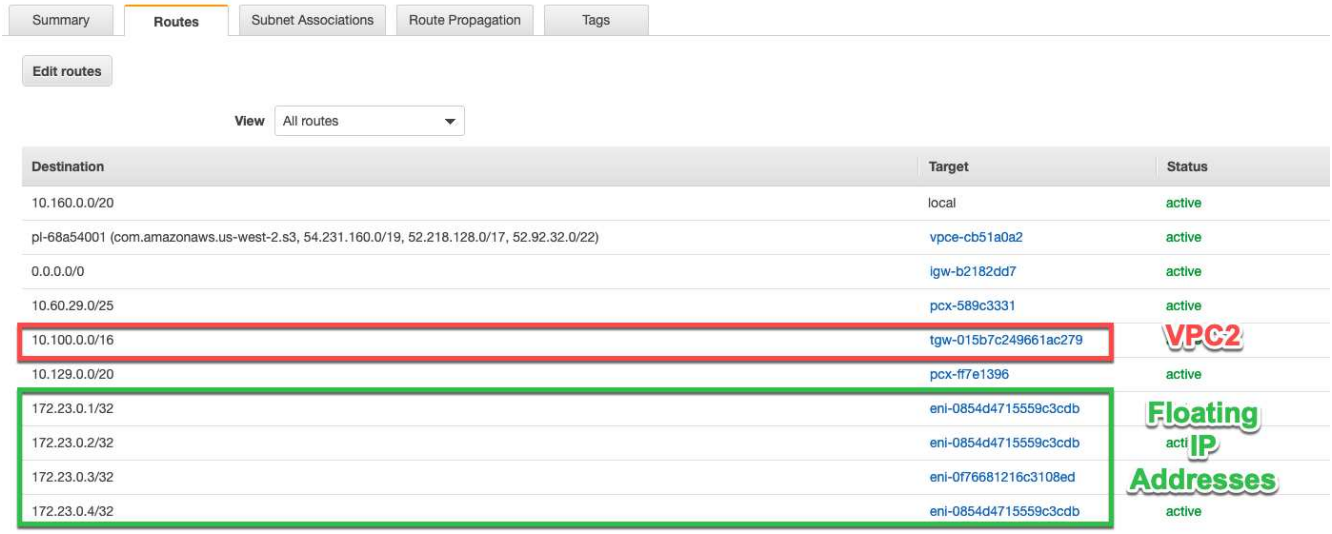
      A imagem de exemplo a seguir mostra a tabela de rotas para a VPC 2, que inclui rotas para a VPC 1 e os endereços IP flutuantes.



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

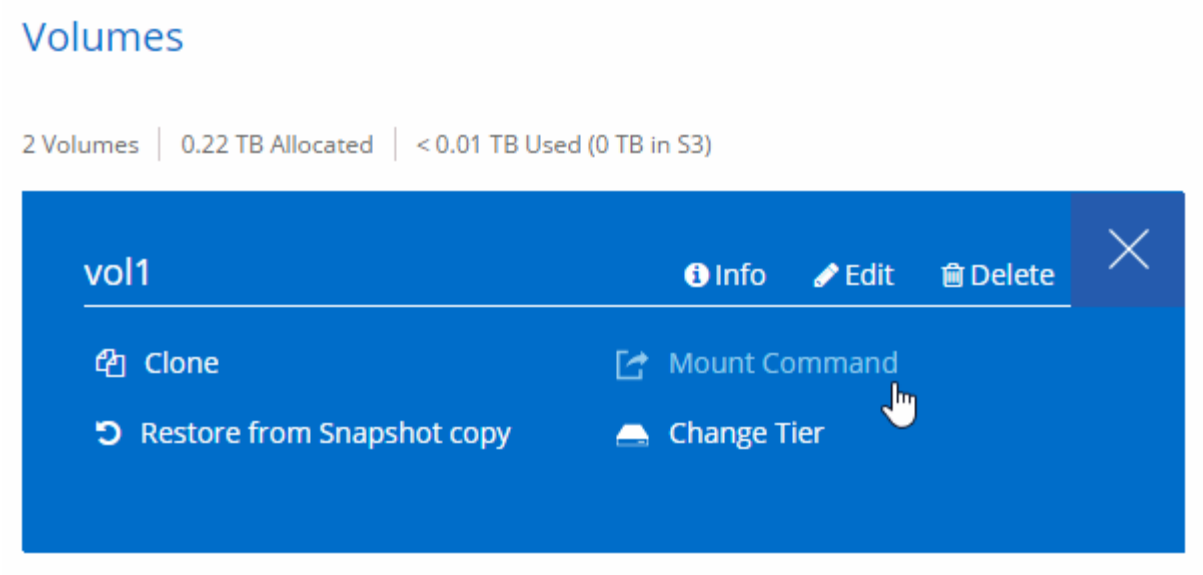
   Esta etapa é importante porque completa o roteamento entre os VPCs.

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



5. Monte volumes em clientes usando o endereço IP flutuante.

   Você pode encontrar o endereço IP correto no Cloud Manager selecionando um volume e clicando em **Mount Command**.



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

Regras do grupo de segurança para a AWS

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

Regras para Cloud Volumes ONTAP

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

Regras de entrada

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

Protocolo	Porta	Finalidade
Todo o ICMP	Tudo	Fazer ping na instância
HTTP	80	Acesso HTTP ao console da Web do System Manager usando o endereço IP do LIF de gerenciamento de cluster
HTTPS	443	Acesso HTTPS ao console da Web do System Manager usando o endereço IP do LIF de gerenciamento de cluster
SSH	22	Acesso SSH ao endereço IP do LIF de gerenciamento de cluster ou um LIF de gerenciamento de nó
TCP	111	Chamada de procedimento remoto para NFS
TCP	139	Sessão de serviço NetBIOS para CIFS

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

Regras de saída

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

Regras básicas de saída

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

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

Regras de saída avançadas

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

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

Serviço	Protocolo	Porta	Fonte	Destino	Finalidade
Ative Directory					

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

Serviço	Protocolo	Porta	Fonte	Destino	Finalidade
SNMP	TCP	161	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
	UDP	161	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
	TCP	162	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
	UDP	162	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
SnapMirror	TCP	11104	LIF entre clusters	LIFs ONTAP entre clusters	Gestão de sessões de comunicação entre clusters para SnapMirror
	TCP	11105	LIF entre clusters	LIFs ONTAP entre clusters	Transferência de dados SnapMirror
Syslog	UDP	514	LIF de gerenciamento de nós	Servidor syslog	Mensagens de encaminhamento do syslog

Regras para o grupo de segurança externa do mediador HA

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

Regras de entrada

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

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

Regras de saída

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

Regras básicas de saída

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

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

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

Regras de saída avançadas

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

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

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

Regras para o grupo de segurança interna do mediador HA

O grupo de segurança interno predefinido do mediador Cloud Volumes ONTAP HA inclui as seguintes regras. O Cloud Manager sempre cria esse grupo de segurança. Você não tem a opção de usar o seu próprio.

Regras de entrada

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

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

Regras de saída

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

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

Regras para o conetor

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

Regras de entrada

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

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

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

Regras de saída

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

Regras básicas de saída

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

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

Regras de saída avançadas

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

O endereço IP de origem é o host do conetor.

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

Configurando o AWS KMS

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

Passos

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

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

   "Documentação da AWS: Chaves mestras do cliente (CMKs)"

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

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

   "Documentação da AWS: Editando chaves"

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

   a. Vá para o console do KMS a partir da conta onde o CMK reside.

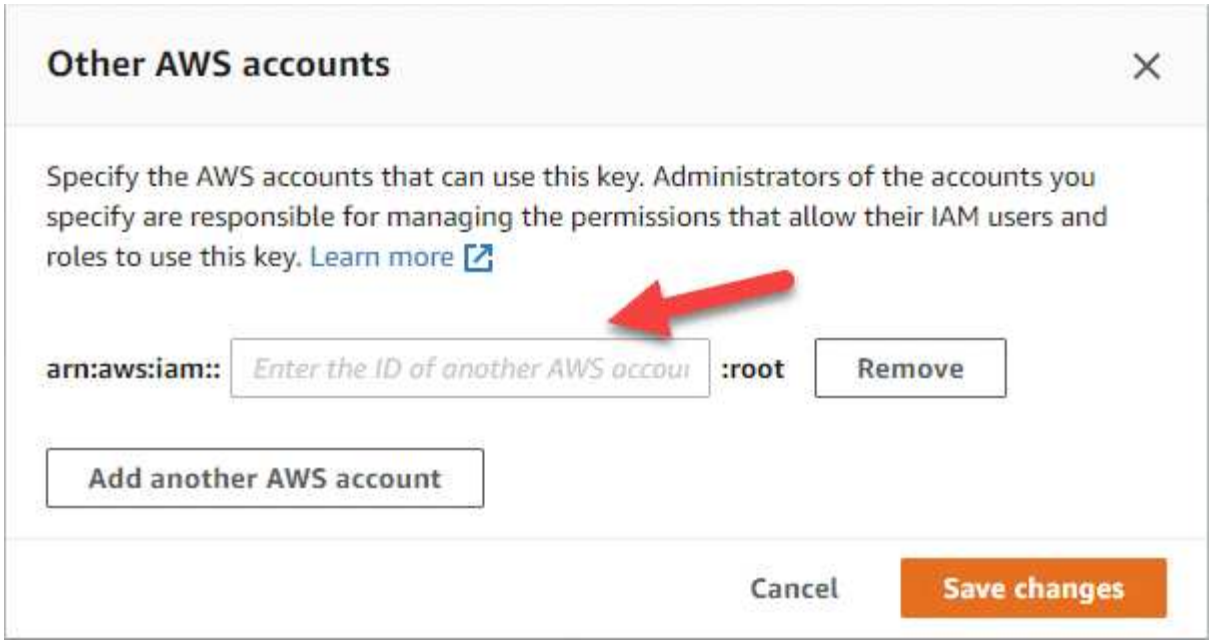
   b. Selecione a tecla .

   c. No painel **General Configuration** (Configuração geral), copie o ARN da chave.

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

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

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



e. Agora mude para a conta da AWS que fornece permissões ao Cloud Manager 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 Cloud Manager.

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

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

+
Para obter detalhes adicionais sobre esse processo, "Documentação da AWS: Permitindo que contas externas da AWS acessem um CMK"consulte .

Iniciando o Cloud Volumes ONTAP na AWS

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

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

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

Antes de começar

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

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

- "Você deve estar preparado para deixar o conetor funcionando o tempo todo".
- Você deve se preparar escolhendo uma configuração e obtendo informações de rede da AWS de seu administrador. Para obter detalhes, "Planejando sua configuração do Cloud Volumes ONTAP"consulte .
- Se você quiser iniciar um sistema BYOL, você deve ter o número de série de 20 dígitos (chave de licença).
- Se você quiser usar CIFS, você deve ter configurado DNS e ative Directory. Para obter detalhes, "Requisitos de rede para o Cloud Volumes ONTAP na AWS"consulte .

Sobre esta tarefa

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

Passos

1. Na página ambientes de trabalho, clique em **Adicionar ambiente de trabalho** e siga as instruções.
2. **Escolha um local**: Selecione **Serviços da Amazon** e **nó único Cloud Volumes ONTAP**.
3. **Detalhes e credenciais**: Opcionalmente, altere as credenciais e a assinatura da AWS, insira um nome de ambiente de trabalho, adicione tags, se necessário, e insira uma senha.

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

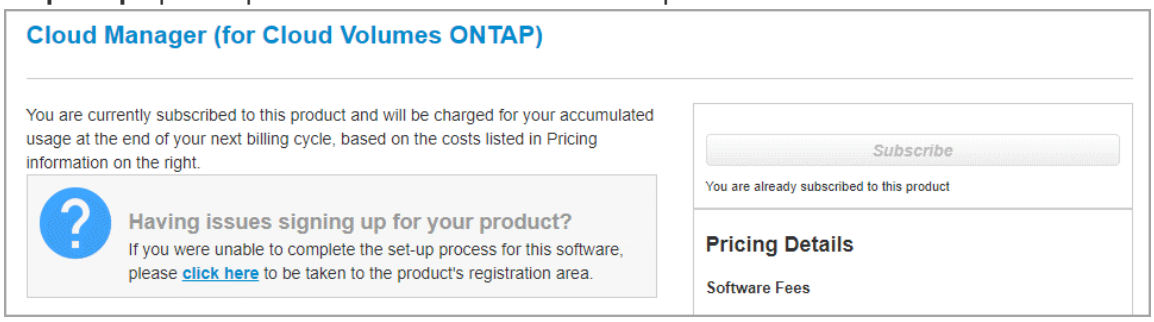
Campo	Descrição
Nome do ambiente de trabalho	O Cloud Manager usa o nome do ambiente de trabalho para nomear o sistema Cloud Volumes ONTAP e a instância do Amazon EC2. Ele também usa o nome como prefixo para o grupo de segurança predefinido, se você selecionar essa opção.

Campo	Descrição
Adicionar etiquetas	As tags AWS são metadados para seus recursos da AWS. O Cloud Manager adiciona as tags à instância do Cloud Volumes ONTAP e a cada recurso da AWS associado à instância. Você pode adicionar até quatro tags da interface do usuário ao criar um ambiente de trabalho e, em seguida, você pode adicionar mais após a criação. Observe que a API não limita a quatro tags ao criar um ambiente de trabalho. Para obter informações sobre tags, "Documentação da AWS: Marcando seus recursos do Amazon EC2" consulte .
Nome de utilizador e palavra-passe	Essas são as credenciais da conta de administrador do cluster do Cloud Volumes ONTAP. Você pode usar essas credenciais para se conetar ao Cloud Volumes ONTAP por meio do OnCommand System Manager ou da CLI.
Editar credenciais	Escolha as credenciais da AWS e a assinatura do mercado a serem usadas com este sistema Cloud Volumes ONTAP. Clique em **Adicionar assinatura** para associar as credenciais selecionadas a uma assinatura. Para criar um sistema Cloud Volumes ONTAP de pagamento conforme o uso, você precisa selecionar as credenciais da AWS associadas a uma assinatura do Cloud Volumes ONTAP no mercado AWS. Você será cobrado a partir desta assinatura para cada sistema PAYGO Cloud Volumes ONTAP 9,6 e posterior que você criar e cada recurso de complemento que ativar. "Saiba como adicionar credenciais adicionais da AWS ao Cloud Manager".

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

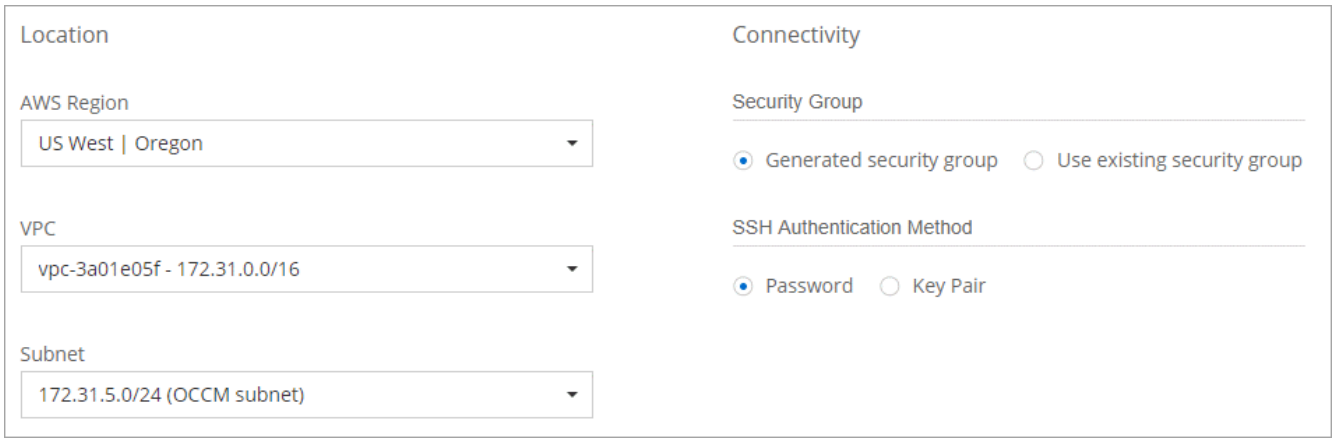
► https://docs.netapp.com/pt-br/occm38//media/video_subscribing_aws.mp4 *(video)*

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



4. **Serviços**: Mantenha os serviços ativados ou desative os serviços individuais que você não deseja usar com o Cloud Volumes ONTAP.
   - "Saiba mais sobre o Cloud Compliance".
   - "Saiba mais sobre o Backup to Cloud".
   - "Saiba mais sobre Monitoramento".
5. **Localização e conetividade**: Insira as informações de rede registradas na Planilha da AWS.

   A imagem a seguir mostra a página preenchida:



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

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

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

   "Saiba como configurar o AWS KMS para Cloud Volumes ONTAP".

   "Saiba mais sobre as tecnologias de criptografia suportadas".

7. **Conta do site de suporte e licença**: Especifique se você deseja usar o pagamento conforme o uso ou o BYOL e especifique uma conta do site de suporte da NetApp.

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

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

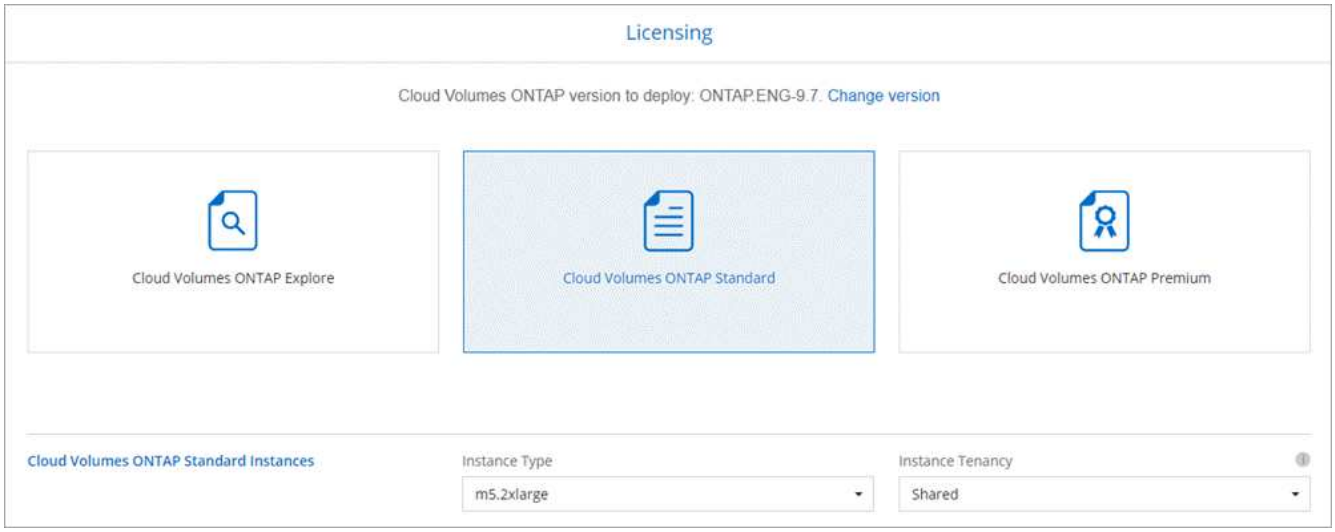
8. **Pacotes pré-configurados**: Selecione um dos pacotes para iniciar rapidamente o Cloud Volumes ONTAP ou clique em **criar minha própria configuração**.

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

9. **Função IAM**: Você deve manter a opção padrão para permitir que o Cloud Manager crie a função para você.

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

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



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

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

11. **Recursos de armazenamento subjacentes**: Escolha configurações para o agregado inicial: Um tipo de disco, um tamanho para cada disco e se a disposição de dados deve ser ativada.

    Observe o seguinte:

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

      Para obter ajuda sobre como escolher um tipo e tamanho de disco, "Dimensionamento do seu sistema na AWS"consulte .

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

      "Saiba como funciona a disposição em camadas de dados".

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

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

    "Saiba mais sobre a velocidade de escrita".

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

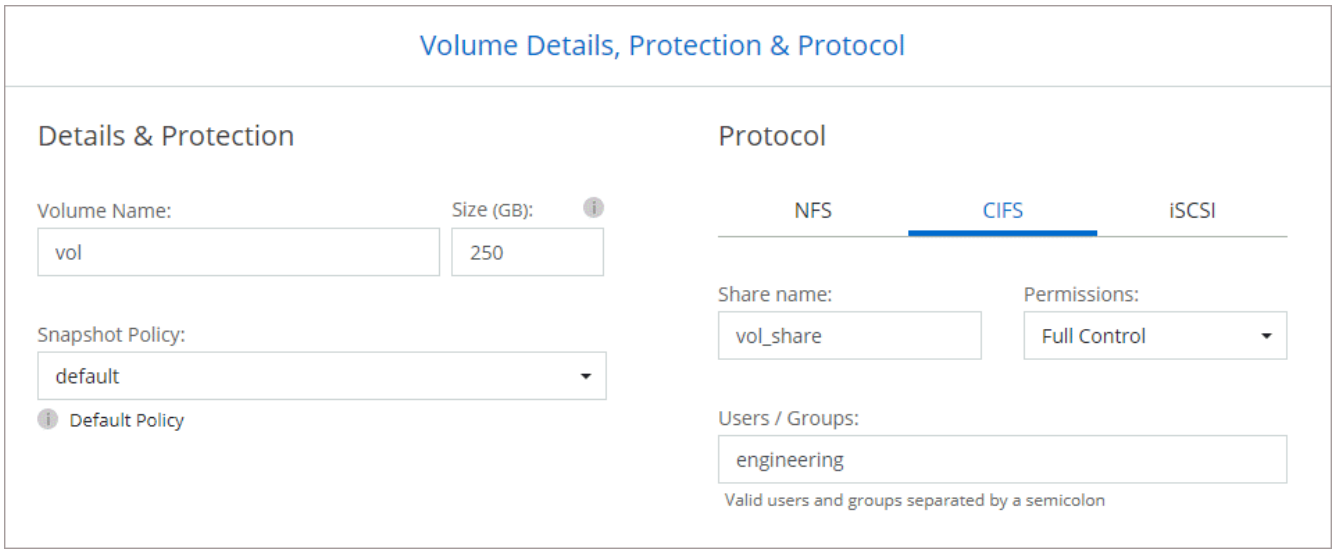
"Saiba mais sobre o armazenamento WORM".

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

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

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

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



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

Campo	Descrição
Endereço IP primário e secundário do DNS	Os endereços IP dos servidores DNS que fornecem resolução de nomes para o servidor CIFS. Os servidores DNS listados devem conter os Registros de localização de serviço (SRV) necessários para localizar os servidores LDAP do ative Directory e os controladores de domínio para o domínio em que o servidor CIFS irá ingressar.
Ative Directory Domain para aderir	O FQDN do domínio do ative Directory (AD) ao qual você deseja que o servidor CIFS se associe.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores à unidade organizacional especificada (ou) dentro do domínio do AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio AD.
Unidade organizacional	A unidade organizacional dentro do domínio AD a associar ao servidor CIFS. A predefinição é computadores. Se você configurar o AWS Managed Microsoft AD como o servidor AD para o Cloud Volumes ONTAP, deverá inserir neste campo **ou computadores**.
Domínio DNS	O domínio DNS da máquina virtual de storage (SVM) do Cloud Volumes ONTAP. Na maioria dos casos, o domínio é o mesmo que o domínio AD.
NTP Server	Selecione **Use ative Directory Domain** para configurar um servidor NTP usando o DNS do ative Directory. Se você precisa configurar um servidor NTP usando um endereço diferente, então você deve usar a API. Consulte "Guia do desenvolvedor de API do Cloud Manager"para obter detalhes.

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

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

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

Resultado

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

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

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

Depois de terminar

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

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

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

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

Antes de começar

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

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

- "Você deve estar preparado para deixar o conetor funcionando o tempo todo".
- Você deve se preparar escolhendo uma configuração e obtendo informações de rede da AWS de seu administrador. Para obter detalhes, "Planejando sua configuração do Cloud Volumes ONTAP"consulte .
- Se você comprou licenças BYOL, você deve ter um número de série de 20 dígitos (chave de licença) para cada nó.
- Se você quiser usar CIFS, você deve ter configurado DNS e ative Directory. Para obter detalhes, "Requisitos de rede para o Cloud Volumes ONTAP na AWS"consulte .

Limitação

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

Sobre esta tarefa

Imediatamente após a criação do ambiente de trabalho, o Cloud Manager inicia uma instância de teste na

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

Passos

1. Na página ambientes de trabalho, clique em **Adicionar ambiente de trabalho** e siga as instruções.
2. **Escolha um local**: Selecione **Serviços da Amazon** e **nó único Cloud Volumes ONTAP**.
3. **Detalhes e credenciais**: Opcionalmente, altere as credenciais e a assinatura da AWS, insira um nome de ambiente de trabalho, adicione tags, se necessário, e insira uma senha.

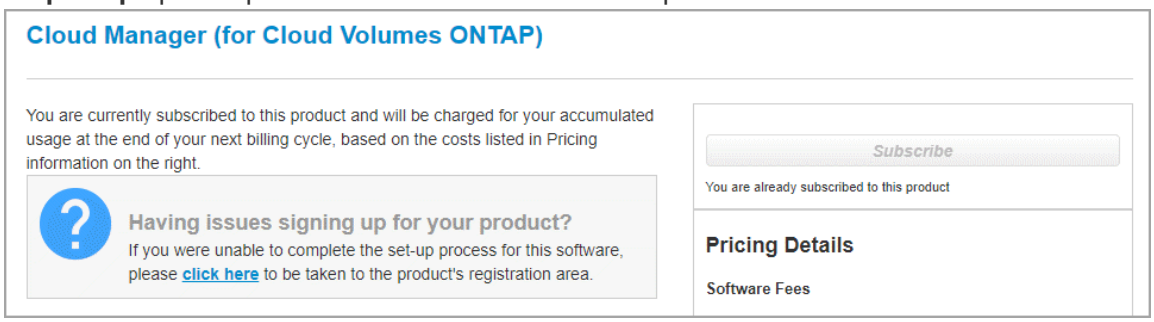
   Alguns dos campos desta página são auto-explicativos. A tabela a seguir descreve os campos para os quais você pode precisar de orientação:

Campo	Descrição
Nome do ambiente de trabalho	O Cloud Manager usa o nome do ambiente de trabalho 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 etiquetas	As tags AWS são metadados para seus recursos da AWS. O Cloud Manager adiciona as tags à instância do Cloud Volumes ONTAP e a cada recurso da AWS associado à instância. Você pode adicionar até quatro tags da interface do usuário ao criar um ambiente de trabalho e, em seguida, você pode adicionar mais após a criação. Observe que a API não limita a quatro tags ao criar um ambiente de trabalho. Para obter informações sobre tags, "Documentação da AWS: Marcando seus recursos do Amazon EC2" consulte .
Nome de utilizador e palavra-passe	Essas são as credenciais da conta de administrador do cluster do Cloud Volumes ONTAP. Você pode usar essas credenciais para se conetar ao Cloud Volumes ONTAP por meio do OnCommand System Manager ou da CLI.
Editar credenciais	Escolha as credenciais da AWS e a assinatura do mercado a serem usadas com este sistema Cloud Volumes ONTAP. Clique em **Adicionar assinatura** para associar as credenciais selecionadas a uma assinatura. Para criar um sistema Cloud Volumes ONTAP de pagamento conforme o uso, você precisa selecionar as credenciais da AWS associadas a uma assinatura do Cloud Volumes ONTAP no mercado AWS. Você será cobrado a partir desta assinatura para cada sistema PAYGO Cloud Volumes ONTAP 9,6 e posterior que você criar e cada recurso de complemento que ativar. "Saiba como adicionar credenciais adicionais da AWS ao Cloud Manager".

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

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

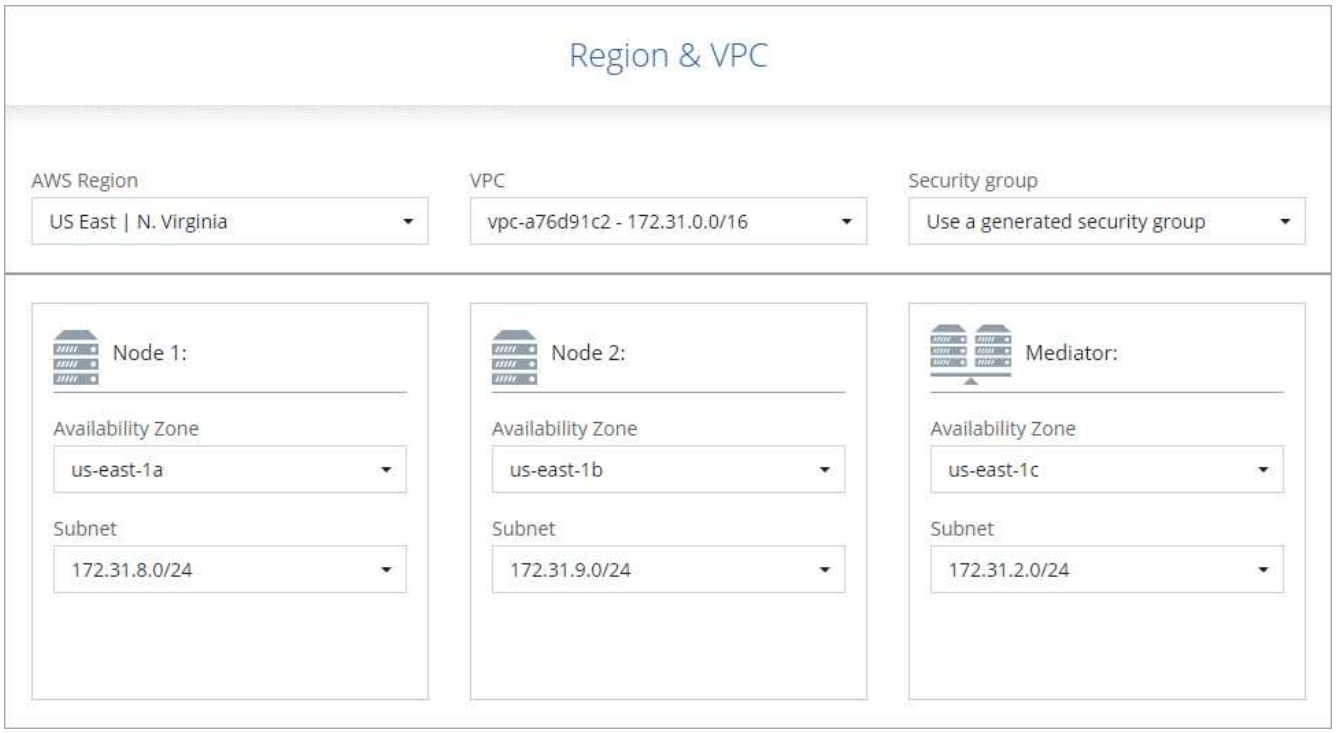
Se vários usuários do IAM trabalharem na mesma conta da AWS, cada usuário precisará se inscrever. Depois que o primeiro usuário se inscreve, o AWS Marketplace informa aos usuários subsequentes que eles já estão inscritos, como mostrado na imagem abaixo. Enquanto uma assinatura está em vigor para a AWS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



4. **Serviços**: Mantenha os serviços ativados ou desative os serviços individuais que você não deseja usar com este sistema Cloud Volumes ONTAP.
   - "Saiba mais sobre o Cloud Compliance".
   - "Saiba mais sobre o Backup to Cloud".
   - "Saiba mais sobre Monitoramento".
5. **Modelos de implantação HA**: Escolha uma configuração de HA.

   Para obter uma visão geral dos modelos de implantação, "Cloud Volumes ONTAP HA para AWS"consulte .
6. **Região e VPC**: Insira as informações de rede registradas na Planilha da AWS.

   A imagem a seguir mostra a página preenchida para uma configuração de AZ múltipla:



7. **Conetividade e Autenticação SSH**: Escolha métodos de conexão para o par HA e o mediador.

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

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

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

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

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

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

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

    "Saiba como configurar o AWS KMS para Cloud Volumes ONTAP".

    "Saiba mais sobre as tecnologias de criptografia suportadas".

11. **Conta do site de suporte e licença**: Especifique se você deseja usar o pagamento conforme o uso ou o BYOL e especifique uma conta do site de suporte da NetApp.

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

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

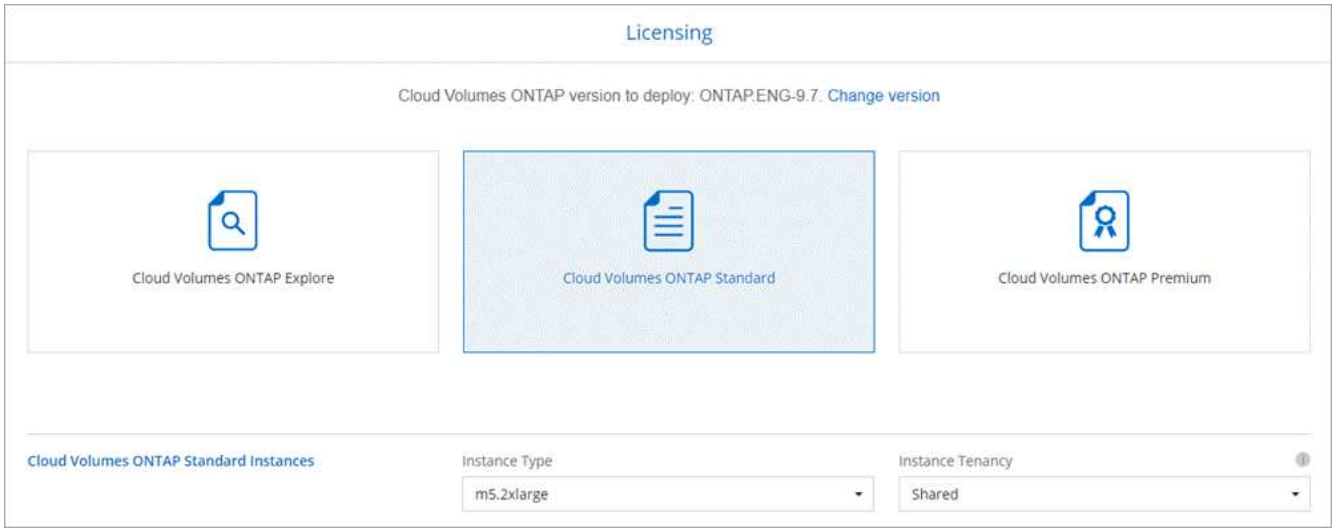
12. **Pacotes pré-configurados**: Selecione um dos pacotes para iniciar rapidamente um sistema Cloud Volumes ONTAP ou clique em **criar minha própria configuração**.

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

13. **Função IAM**: Você deve manter a opção padrão para permitir que o Cloud Manager crie as funções para você.

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

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



Se suas necessidades mudarem depois de iniciar as instâncias, você poderá modificar a licença ou o tipo de instância mais tarde.

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

15. **Recursos de armazenamento subjacentes**: Escolha configurações para o agregado inicial: Um tipo de disco, um tamanho para cada disco e se a disposição de dados deve ser ativada.

    Observe o seguinte:

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

      Para obter ajuda sobre como escolher um tipo e tamanho de disco, "Dimensionamento do seu sistema na AWS"consulte .

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

      "Saiba como funciona a disposição em camadas de dados".

16. **WORM**: Ative o armazenamento WORM (uma gravação, muitas leituras), se desejado.

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

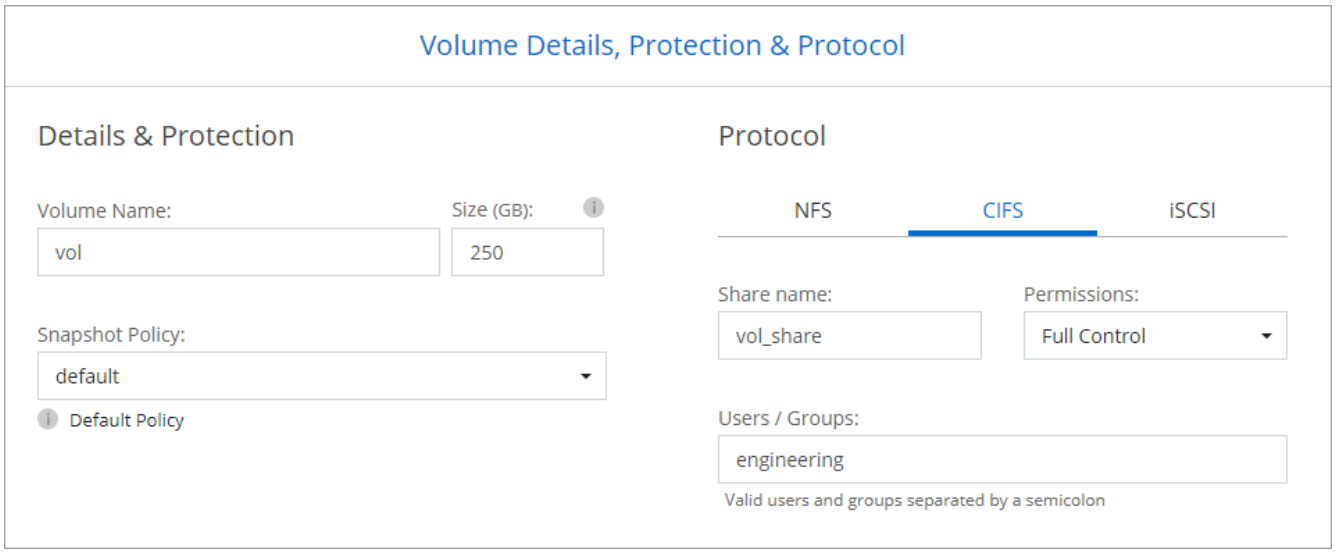
    "Saiba mais sobre o armazenamento WORM".

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

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

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

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



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

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

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

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

Resultado

O Cloud Manager lança o par de HA da Cloud Volumes ONTAP. Você pode acompanhar o progresso na linha do tempo.

Se tiver algum problema ao iniciar o par de HA, reveja a mensagem de falha. Você também pode selecionar o ambiente de trabalho e clicar em recriar ambiente.

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

Depois de terminar

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

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

Comece a usar o Azure

Introdução ao Cloud Volumes ONTAP para Azure

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

Crie um conetor

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

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

Planeje sua configuração

O Cloud Manager oferece pacotes pré-configurados que correspondem aos seus requisitos de carga de trabalho, ou você pode criar sua própria configuração. Se você escolher sua própria configuração, você deve entender as opções disponíveis para você. "Saiba mais".

Configure a rede

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

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

"Saiba mais sobre os requisitos de rede".

Inicie o Cloud Volumes ONTAP usando o Cloud Manager

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

Links relacionados

- "A avaliar"
- "Criando um conetor do Cloud Manager"
- "Criando um conetor a partir do Azure Marketplace"
- "Instalar o software Connector em um host Linux"
- "O que o Cloud Manager faz com as permissões do Azure"

Planejando sua configuração do Cloud Volumes ONTAP no Azure

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

Escolhendo um tipo de licença

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

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

Compreender os limites de armazenamento

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

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

Dimensionamento do seu sistema no Azure

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

Tipo de máquina virtual

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

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

Tipo de disco Azure

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

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

- *Discos gerenciados SSD premium* fornecem alto desempenho para cargas de trabalho com uso intenso de e/S a um custo mais alto.
- *Discos gerenciados SSD padrão* fornecem desempenho consistente para cargas de trabalho que exigem IOPS baixo.
- *Discos gerenciados HDD padrão* são uma boa escolha se você não precisa de IOPS alto e quer reduzir seus custos.

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

Tamanho do disco do Azure

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

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

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

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

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

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

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

Escolhendo uma configuração compatível com Flash Cache

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

Planilha de informações de rede do Azure

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

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

Escolhendo uma velocidade de escrita

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

Diferença entre velocidade de gravação normal e alta velocidade de gravação

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

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

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

Quando usar alta velocidade de gravação

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

Recomendações ao usar alta velocidade de gravação

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

Escolhendo um perfil de uso de volume

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

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

Thin Provisioning

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

Deduplicação

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

Compactação

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

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

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

Requisitos para o Cloud Volumes ONTAP

Os seguintes requisitos de rede devem ser atendidos no Azure.

Acesso de saída à Internet para Cloud Volumes ONTAP

O Cloud Volumes ONTAP requer acesso de saída à Internet para enviar mensagens para o NetApp AutoSupport, que monitora proativamente a integridade do seu armazenamento.

As políticas de roteamento e firewall devem permitir o tráfego HTTP/HTTPS para os seguintes endpoints para que o Cloud Volumes ONTAP possa enviar mensagens AutoSupport:

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

"Saiba como configurar o AutoSupport".

Grupos de segurança

Você não precisa criar grupos de segurança porque o Cloud Manager faz isso por você. Se você precisar usar o seu próprio, consulte as regras do grupo de segurança listadas abaixo.

Número de endereços IP

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

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

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

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

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

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

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

Essas permissões estão incluídas no último "Política do Cloud Manager".

Para obter detalhes sobre como configurar a disposição de dados em camadas, "Disposição em camadas de dados inativos no storage de objetos de baixo custo"consulte .

Conexões com sistemas ONTAP em outras redes

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

Para obter instruções, "Documentação do Microsoft Azure: Crie uma conexão Site-to-Site no portal do Azure" consulte .

Requisitos para o conetor

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

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

Conexões com redes de destino

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

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

Acesso de saída à Internet

O conetor requer acesso de saída à Internet para gerenciar recursos e processos em seu ambiente de nuvem pública. Um conetor entra em Contato com os seguintes endpoints ao gerenciar recursos no Azure:

Endpoints	Finalidade
https://management.azure.com https://login.microsoftonline.com	Permite que o Cloud Manager implante e gerencie o Cloud Volumes ONTAP na maioria das regiões do Azure.
https://management.microsoftazure.de https://login.microsoftonline.de	Permite que o Cloud Manager implante e gerencie o Cloud Volumes ONTAP nas regiões Azure Alemanha.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Permite que o Cloud Manager implante e gerencie o Cloud Volumes ONTAP nas regiões Azure US Gov.
https://api.services.cloud.NetApp.com:443	Solicitações de API para o NetApp Cloud Central.
https://cloud.support.NetApp.com.s3.us-west-1.amazonaws.com	Fornece acesso a imagens de software, manifestos e modelos.
https://repo.cloud.support.NetApp.com	Usado para baixar dependências do Cloud Manager.
http://repo.mysql.com/	Usado para baixar MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-NetApp-com-accelerated.s3.amazonaws.com	Permite que o Cloud Manager acesse e baixe manifestos, modelos e imagens de atualização do Cloud Volumes ONTAP.
https://cloudmanagerinfraprod.azurecr.io	Acesso a imagens de software de componentes de contentor para uma infraestrutura que esteja executando o Docker e fornece uma solução para integrações de serviços com o Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permite que o NetApp transmita dados de Registros de auditoria.
https://cloudmanager.cloud.NetApp.com	Comunicação com o serviço Cloud Manager, que inclui contas do Cloud Central.
https://NetApp-cloud-account.auth0.com	Comunicação com o NetApp Cloud Central para autenticação centralizada de usuários.
https://mysupport.NetApp.com	Comunicação com NetApp AutoSupport.
https://support.NetApp.com/svcgw - https://support.NetApp.com/ServiceGW/Entitlement - https://eval.lic.NetApp.com.s3.us-west-1.amazonaws.com - https://cloud-support-NetApp-com.s3.us-west-1.amazonaws.com	Comunicação com o NetApp para licenciamento de sistema e Registro de suporte.
https://ipa-signer.cloudmanager.NetApp.com	Permite que o Cloud Manager gere licenças (por exemplo, uma licença FlexCache para Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/Trident/Releases/download/	Necessário para conectar sistemas Cloud Volumes ONTAP a um cluster Kubernetes. Os endpoints permitem a instalação do NetApp Trident.

Endpoints	Finalidade
*.blob.core.windows.net	Necessário para pares de HA ao usar um proxy.
Vários locais de terceiros, por exemplo: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org Locais de terceiros estão sujeitos a alterações.	Durante as atualizações, o Cloud Manager baixa os pacotes mais recentes para dependências de terceiros.

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

Endpoints	Finalidade
O host do conetor	Você deve inserir o endereço IP do host de um navegador da Web para carregar o console do Cloud Manager. Dependendo da sua conetividade com o seu provedor de nuvem, você pode usar o IP privado ou um IP público atribuído ao host: • Um IP privado funciona se você tiver uma VPN e acesso direto à sua rede virtual • Um IP público funciona em qualquer cenário de rede Em qualquer caso, você deve proteger o acesso à rede, garantindo que as regras do grupo de segurança permitam o acesso somente de IPs ou sub-redes autorizados.
https://auth0.com https://cdn.auth0.com://NetApp-cloud-account.auth0.com https://services.cloud.NetApp.com	Seu navegador da Web se coneta a esses endpoints para autenticação de usuário centralizada por meio do NetApp Cloud Central.
https://widget.intercom.io	Para um bate-papo no produto que permite conversar com especialistas em nuvem da NetApp.

Regras do grupo de segurança para o Cloud Volumes ONTAP

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

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

Regras de entrada para sistemas de nó único

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

Prioridade e nome	Porta e protocolo	Origem e destino	Descrição
1000 inbound_ssh	22 TCP	Qualquer a qualquer	Acesso SSH ao endereço IP do LIF de gerenciamento de cluster ou um LIF de gerenciamento de nó
1001 inbound_http	80 TCP	Qualquer a qualquer	Acesso HTTP ao console da Web do System Manager usando o endereço IP do LIF de gerenciamento de cluster
1002 inbound_111_tcp	111 TCP	Qualquer a qualquer	Chamada de procedimento remoto para NFS
1003 inbound_111_udp	111 UDP	Qualquer a qualquer	Chamada de procedimento remoto para NFS
1004 inbound_139	139 TCP	Qualquer a qualquer	Sessão de serviço NetBIOS para CIFS
1005 inbound_161-162 _tcp	161-162 TCP	Qualquer a qualquer	Protocolo de gerenciamento de rede simples
1006 inbound_161-162 _udp	161-162 UDP	Qualquer a qualquer	Protocolo de gerenciamento de rede simples
1007 inbound_443	443 TCP	Qualquer a qualquer	Acesso HTTPS ao console da Web do System Manager usando o endereço IP do LIF de gerenciamento de cluster
1008 inbound_445	445 TCP	Qualquer a qualquer	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
1009 inbound_635_tcp	635 TCP	Qualquer a qualquer	Montagem em NFS
1010 inbound_635_udp	635 UDP	Qualquer a qualquer	Montagem em NFS
1011 inbound_749	749 TCP	Qualquer a qualquer	Kerberos
1012 inbound_2049_tcp	2049 TCP	Qualquer a qualquer	Daemon do servidor NFS
1013 inbound_2049_udp	2049 UDP	Qualquer a qualquer	Daemon do servidor NFS
1014 inbound_3260	3260 TCP	Qualquer a qualquer	Acesso iSCSI através do iSCSI data LIF

Prioridade e nome	Porta e protocolo	Origem e destino	Descrição
1015 inbound_4045-4046_tcp	4045-4046 TCP	Qualquer a qualquer	Daemon de bloqueio NFS e monitor de status da rede
1016 inbound_4045-4046_udp	4045-4046 UDP	Qualquer a qualquer	Daemon de bloqueio NFS e monitor de status da rede
1017 inbound_10000	10000 TCP	Qualquer a qualquer	Backup usando NDMP
1018 inbound_11104-11105	11104-11105 TCP	Qualquer a qualquer	Transferência de dados SnapMirror
3000 inbound_deny _all_tcp	Qualquer porta TCP	Qualquer a qualquer	Bloquear todo o outro tráfego de entrada TCP
3001 inbound_deny _all_udp	Qualquer porta UDP	Qualquer a qualquer	Bloqueie todo o outro tráfego de entrada UDP
65000 AllowVnetInBound	Qualquer porta de qualquer protocolo	VirtualNetwork para VirtualNetwork	Tráfego de entrada de dentro da VNet
65001 AllowAzureLoad BalancerInBound	Qualquer porta de qualquer protocolo	AzureLoadBalancer para qualquer	Tráfego de dados do Azure Standard Load Balancer
65500 DenyAllInBound	Qualquer porta de qualquer protocolo	Qualquer a qualquer	Bloquear todo o outro tráfego de entrada

Regras de entrada para sistemas HA

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

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

Prioridade e nome	Porta e protocolo	Origem e destino	Descrição
100 inbound_443	443 qualquer protocolo	Qualquer a qualquer	Acesso HTTPS ao console da Web do System Manager usando o endereço IP do LIF de gerenciamento de cluster
101 inbound_111_tcp	111 qualquer protocolo	Qualquer a qualquer	Chamada de procedimento remoto para NFS
102 inbound_2049_tcp	2049 qualquer protocolo	Qualquer a qualquer	Daemon do servidor NFS

Prioridade e nome	Porta e protocolo	Origem e destino	Descrição
111 inbound_ssh	22 qualquer protocolo	Qualquer a qualquer	Acesso SSH ao endereço IP do LIF de gerenciamento de cluster ou um LIF de gerenciamento de nó
121 inbound_53	53 qualquer protocolo	Qualquer a qualquer	DNS e CIFS
65000 AllowVnetInBound	Qualquer porta de qualquer protocolo	VirtualNetwork para VirtualNetwork	Tráfego de entrada de dentro da VNet
65001 AllowAzureLoad BalancerInBound	Qualquer porta de qualquer protocolo	AzureLoadBalancer para qualquer	Tráfego de dados do Azure Standard Load Balancer
65500 DenyAllInBound	Qualquer porta de qualquer protocolo	Qualquer a qualquer	Bloquear todo o outro tráfego de entrada

Regras de saída

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

Regras básicas de saída

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

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

Regras de saída avançadas

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

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

Serviço	Porta	Protocolo	Fonte	Destino	Finalidade
Ative Directory					

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

Regras do grupo de segurança para o conetor

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

Regras de entrada

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

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

Regras de saída

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

Regras básicas de saída

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

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

Regras de saída avançadas

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

O endereço IP de origem é o host do conetor.

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

Iniciar o Cloud Volumes ONTAP no Azure

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

Antes de começar

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

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

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

Sobre esta tarefa

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

Potencial para perda de dados

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

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

Passos

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

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

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

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

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

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

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

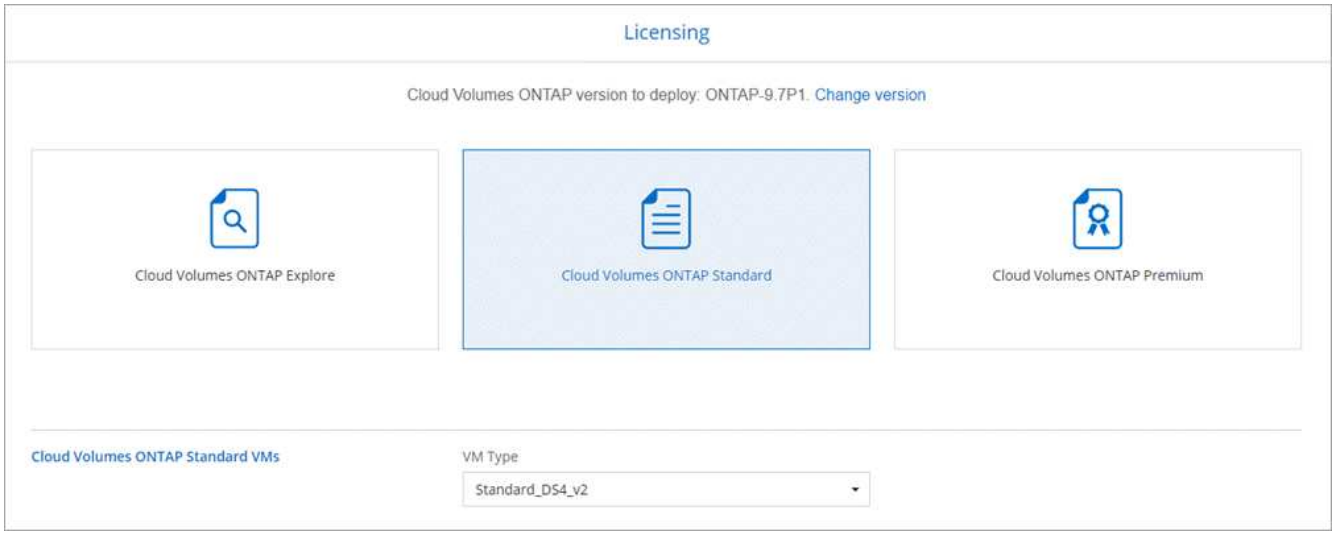
   Para entender como as licenças funcionam, "Licenciamento"consulte .

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

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

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

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



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

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

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

    Observe o seguinte:

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

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

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

      "Saiba mais sobre categorização de dados".

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

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

"Saiba mais sobre a velocidade de escrita".

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

"Saiba mais sobre o armazenamento WORM".

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

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

    "Saiba mais sobre o armazenamento WORM".

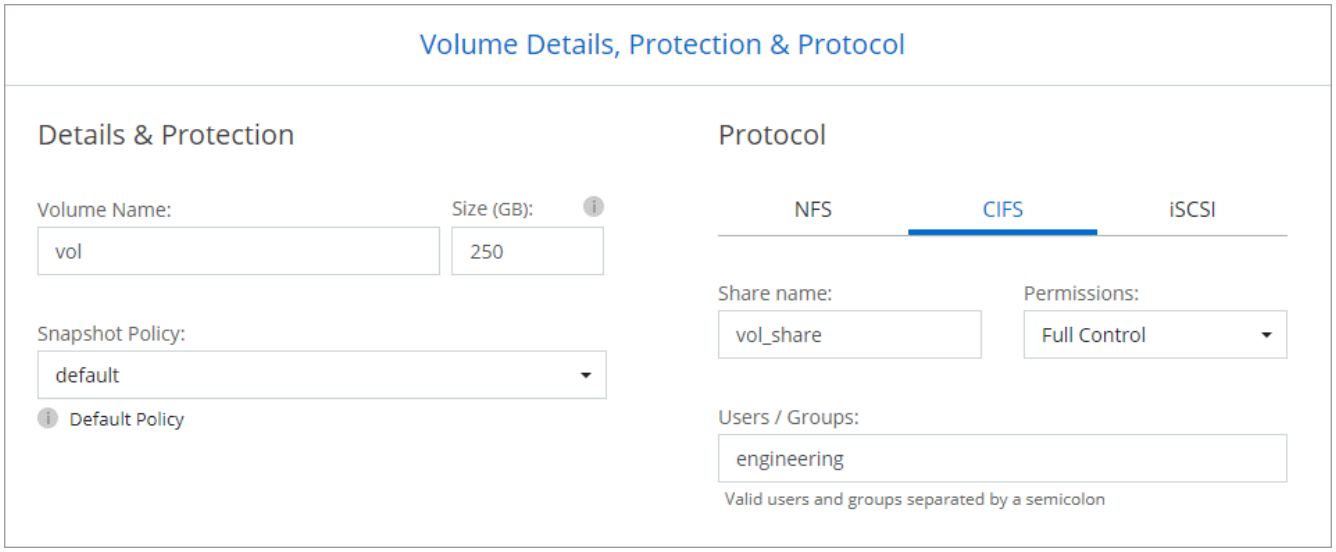
13. **Criar volume**: Insira os detalhes do novo volume ou clique em **Ignorar**.

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

Campo	Descrição
Tamanho	O tamanho máximo que você pode inserir depende, em grande parte, se você ativar o provisionamento de thin, o que permite criar um volume maior do que o armazenamento físico atualmente disponível para ele.
Controle de acesso (somente para NFS)	Uma política de exportação define os clientes na sub-rede que podem acessar o volume. Por padrão, o Cloud Manager insere um valor que fornece acesso a todas as instâncias na sub-rede.
Permissões e utilizadores/grupos (apenas para CIFS)	Esses campos permitem controlar o nível de acesso a um compartilhamento para usuários e grupos (também chamados de listas de controle de acesso ou ACLs). Você pode especificar usuários ou grupos do Windows locais ou de domínio, ou usuários ou grupos UNIX. Se você especificar um nome de usuário do domínio do Windows, você deve incluir o domínio do usuário usando o nome de domínio do formato.
Política de instantâneos	Uma política de cópia Snapshot especifica a frequência e o número de cópias snapshot do NetApp criadas automaticamente. Uma cópia Snapshot do NetApp é uma imagem pontual do sistema de arquivos que não afeta a performance e exige o mínimo de storage. Você pode escolher a política padrão ou nenhuma. Você pode escolher nenhum para dados transitórios: Por exemplo, tempdb para Microsoft SQL Server.
Opções avançadas (somente para NFS)	Selecione uma versão NFS para o volume: NFSv3 ou NFSv4.

Campo	Descrição
Grupo de iniciadores e IQN (apenas para iSCSI)	Os destinos de armazenamento iSCSI são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Os grupos de iniciadores são tabelas de nomes de nós de host iSCSI e controlam quais iniciadores têm acesso a quais LUNs. Os destinos iSCSI se conetam à rede por meio de adaptadores de rede Ethernet (NICs) padrão, placas de mecanismo de descarga TCP (TOE) com iniciadores de software, adaptadores de rede convergidos (CNAs) ou adaptadores de barramento de host dedicados (HBAs) e são identificados por IQNs (iSCSI Qualified Names). Quando você cria um volume iSCSI, o Cloud Manager cria automaticamente um LUN para você. Simplificamos a criação de apenas um LUN por volume, para que não haja gerenciamento envolvido. Depois de criar o volume, "Use o IQN para se conetar ao LUN a partir de seus hosts".

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



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

Campo	Descrição
Endereço IP primário e secundário do DNS	Os endereços IP dos servidores DNS que fornecem resolução de nomes para o servidor CIFS. Os servidores DNS listados devem conter os Registros de localização de serviço (SRV) necessários para localizar os servidores LDAP do ative Directory e os controladores de domínio para o domínio em que o servidor CIFS irá ingressar.
Ative Directory Domain para aderir	O FQDN do domínio do ative Directory (AD) ao qual você deseja que o servidor CIFS se associe.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores à unidade organizacional especificada (ou) dentro do domínio do AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio AD.

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

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

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

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

Resultado

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

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

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

Depois de terminar

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

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

Comece a usar o GCP

Introdução ao Cloud Volumes ONTAP para Google Cloud

Comece a usar o Cloud Volumes ONTAP para GCP em algumas etapas.

Crie um conetor

Se você ainda não tem um"Conetor", um administrador de conta precisa criar um. "Saiba como criar um conetor na GCP".

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

Planeje sua configuração

O Cloud Manager oferece pacotes pré-configurados que correspondem aos seus requisitos de carga de trabalho, ou você pode criar sua própria configuração. Se você escolher sua própria configuração, você deve entender as opções disponíveis para você. "Saiba mais".

Configure a rede

1. Certifique-se de que a VPC e as sub-redes suportem a conetividade entre o conetor e o Cloud Volumes ONTAP.
2. Ative o acesso de saída à Internet a partir da VPC de destino para que o conetor e o Cloud Volumes ONTAP possam entrar em Contato com vários endpoints.

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

"Saiba mais sobre os requisitos de rede".

Configurar o GCP para categorização de dados

Dois requisitos devem ser atendidos para categorizar dados inativos do Cloud Volumes ONTAP para storage de objetos de baixo custo (um bucket do Google Cloud Storage):

1. "Configure a sub-rede do Cloud Volumes ONTAP para o acesso privado do Google".
2. "Configurar uma conta de serviço para categorização de dados":
   - Atribua a função predefinida *Storage Admin* à conta de serviço de disposição em camadas.
   - Adicione a conta de serviço do conetor como um *Usuário da conta de serviço* à conta de serviço em camadas.

     Você pode fornecer a função de usuário "na etapa 3 do assistente quando você cria a conta de serviço de disposição em camadas" , ou "conceda a função após a criação da conta de serviço".

Você precisará selecionar a conta de serviço de disposição em camadas mais tarde ao criar um ambiente de trabalho do Cloud Volumes ONTAP.

Se você não habilitar a disposição de dados em categorias e selecionar uma conta de serviço ao criar o sistema Cloud Volumes ONTAP, será necessário desativar o sistema e adicionar a conta de serviço ao Cloud Volumes ONTAP a partir do console do GCP.

Habilite as APIs do Google Cloud

"Ative as seguintes APIs do Google Cloud em seu projeto". Essas APIs são necessárias para implantar o conetor e o Cloud Volumes ONTAP.

- API do Cloud Deployment Manager V2
- API Cloud Logging
- API do Cloud Resource Manager
- API do mecanismo de computação
- API de gerenciamento de identidade e acesso (IAM)

Inicie o Cloud Volumes ONTAP usando o Cloud Manager

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

Links relacionados

- "A avaliar"
- "Criando um conetor do Cloud Manager"
- "Instalar o software Connector em um host Linux"
- "O que o Cloud Manager faz com as permissões do GCP"

Planejando sua configuração do Cloud Volumes ONTAP no Google Cloud

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

Escolhendo um tipo de licença

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

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

Compreender os limites de armazenamento

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

"Limites de armazenamento para o Cloud Volumes ONTAP 9,7 no GCP"

Dimensionamento do seu sistema na GCP

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

Tipo de máquina

Veja os tipos de máquina suportados no "Notas de versão do Cloud Volumes ONTAP" e, em seguida, reveja os detalhes do Google sobre cada tipo de máquina suportado. Combine seus requisitos de carga de trabalho com o número de vCPUs e memória para o tipo de máquina. Observe que cada núcleo da CPU aumenta o desempenho da rede.

Consulte o seguinte para obter mais detalhes:

- "Documentação do Google Cloud: N1 tipos de máquina padrão"
- "Documentação do Google Cloud: Desempenho"

Tipo de disco do GCP

Ao criar volumes para Cloud Volumes ONTAP, você precisa escolher o storage de nuvem subjacente que o Cloud Volumes ONTAP usa para um disco. O tipo de disco pode ser *Zonal SSD Persistent Disks* ou *Zonal Standard Persistent Disks*.

Os discos persistentes SSD são os melhores para workloads que exigem altas taxas de IOPS aleatório, enquanto os discos persistentes padrão são econômicos e podem lidar com operações de leitura/gravação sequenciais. Para obter mais detalhes, "Documentação do Google Cloud: Discos persistentes zonais (padrão e SSD)" consulte .

Tamanho do disco do GCP

Você precisa escolher um tamanho de disco inicial ao implantar um sistema Cloud Volumes ONTAP. Depois disso, você pode permitir que o Cloud Manager gerencie a capacidade de um sistema para você, mas se quiser criar agregados, esteja ciente do seguinte:

- Todos os discos em um agregado devem ter o mesmo tamanho.
- Determine o espaço de que você precisa, levando em consideração o desempenho.
- O desempenho dos discos persistentes é dimensionado automaticamente com o tamanho do disco e o número de vCPUs disponíveis para o sistema.

  Consulte o seguinte para obter mais detalhes:

  - "Documentação do Google Cloud: Discos persistentes zonais (padrão e SSD)"
  - "Documentação do Google Cloud: Otimizando o desempenho do disco persistente e do SSD local"

Planilha de informações de rede do GCP

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

Informações do GCP	O seu valor
Região	
Zona	
Rede VPC	
Sub-rede	
Política de firewall (se estiver usando a sua própria)	

Escolhendo uma velocidade de escrita

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

Diferença entre velocidade de gravação normal e alta velocidade de gravação

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

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

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

Quando usar alta velocidade de gravação

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

Recomendações ao usar alta velocidade de gravação

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

Escolhendo um perfil de uso de volume

O ONTAP inclui vários recursos de eficiência de storage que podem reduzir a quantidade total de storage de que você precisa. Ao criar um volume no Cloud Manager, você pode escolher um perfil que ative esses

recursos ou um perfil que os desabilite. Você deve aprender mais sobre esses recursos para ajudá-lo a decidir qual perfil usar.

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

Thin Provisioning

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

Deduplicação

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

Compactação

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

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

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

Requisitos para o Cloud Volumes ONTAP

Os requisitos a seguir devem ser atendidos na GCP.

Nuvem privada virtual

O Cloud Volumes ONTAP e o conetor são suportados em uma VPC compartilhada do Google Cloud e também em VPCs não compartilhados.

Uma VPC compartilhada permite que você configure e gerencie centralmente redes virtuais em vários projetos. Você pode configurar redes VPC compartilhadas no *projeto host* e implantar as instâncias de máquina virtual Connector e Cloud Volumes ONTAP em um *projeto de serviço*. "Documentação do Google Cloud: Visão geral da VPC compartilhada".

O único requisito ao usar uma VPC compartilhada é fornecer o "Função de usuário da rede de computação" à conta de serviço do Connector. O Cloud Manager precisa dessas permissões para consultar firewalls, VPC e sub-redes no projeto host.

Acesso de saída à Internet para Cloud Volumes ONTAP

O Cloud Volumes ONTAP requer acesso de saída à Internet para enviar mensagens para o NetApp AutoSupport, que monitora proativamente a integridade do seu armazenamento.

As políticas de roteamento e firewall devem permitir o tráfego HTTP/HTTPS para os seguintes endpoints para que o Cloud Volumes ONTAP possa enviar mensagens AutoSupport:

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

"Saiba como configurar o AutoSupport".

Número de endereços IP

O Cloud Manager aloca 5 endereços IP para o Cloud Volumes ONTAP no GCP.

Observe que o Cloud Manager não cria um LIF de gerenciamento de SVM para Cloud Volumes ONTAP no GCP.

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

Regras de firewall

Você não precisa criar regras de firewall porque o Cloud Manager faz isso por você. Se você precisar usar o seu próprio, consulte as regras de firewall listadas abaixo.

Conexão do Cloud Volumes ONTAP ao Google Cloud Storage para categorização de dados

Se você quiser categorizar dados inativos em um intervalo do Google Cloud Storage, a sub-rede na qual o Cloud Volumes ONTAP reside deve ser configurada para acesso privado do Google. Para obter instruções, "Documentação do Google Cloud: Configurando o acesso privado do Google" consulte .

Para obter as etapas adicionais necessárias para configurar a disposição de dados em categorias no Cloud Manager, "Disposição em camadas de dados inativos no storage de objetos de baixo custo"consulte .

Conexões com sistemas ONTAP em outras redes

Para replicar dados entre um sistema Cloud Volumes ONTAP no GCP e sistemas ONTAP em outras redes, é necessário ter uma conexão VPN entre a VPC e a outra rede, por exemplo, sua rede corporativa.

Para obter instruções, "Documentação do Google Cloud: Visão geral do Cloud VPN" consulte .

Requisitos para o conetor

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

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

Conexão com redes de destino

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

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

Acesso de saída à Internet

O conetor requer acesso de saída à Internet para gerenciar recursos e processos em seu ambiente de nuvem pública. Um conetor entra em Contato com os seguintes endpoints ao gerenciar recursos no GCP:

Endpoints	Finalidade
https://www.googleapis.com	Permite que o conetor entre em Contato com as APIs do Google para implantar e gerenciar o Cloud Volumes ONTAP no GCP.
https://api.services.cloud.NetApp.com:443	Solicitações de API para o NetApp Cloud Central.
https://cloud.support.NetApp.com.s3.us-west-1.amazonaws.com	Fornece acesso a imagens de software, manifestos e modelos.
https://repo.cloud.support.NetApp.com	Usado para baixar dependências do Cloud Manager.
http://repo.mysql.com/	Usado para baixar MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-NetApp-com-accelerated.s3.amazonaws.com	Permite que o conetor acesse e baixe manifestos, modelos e imagens de atualização do Cloud Volumes ONTAP.
https://cloudmanagerinfraprod.azurecr.io	Acesso a imagens de software de componentes de contentor para uma infraestrutura que esteja executando o Docker e fornece uma solução para integrações de serviços com o Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permite que o NetApp transmita dados de Registros de auditoria.
https://cloudmanager.cloud.NetApp.com	Comunicação com o serviço Cloud Manager, que inclui contas do Cloud Central.
https://NetApp-cloud-account.auth0.com	Comunicação com o NetApp Cloud Central para autenticação centralizada de usuários.
https://mysupport.NetApp.com	Comunicação com NetApp AutoSupport.
https://support.NetApp.com/svcgw - https://support.NetApp.com/ServiceGW/Entitlement - https://eval.lic.NetApp.com.s3.us-west-1.amazonaws.com - https://cloud-support-NetApp-com.s3.us-west-1.amazonaws.com	Comunicação com o NetApp para licenciamento de sistema e Registro de suporte.
https://ipa-signer.cloudmanager.NetApp.com	Permite que o Cloud Manager gere licenças (por exemplo, uma licença FlexCache para Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/Trident/Releases/download/	Necessário para conectar sistemas Cloud Volumes ONTAP a um cluster Kubernetes. Os endpoints permitem a instalação do NetApp Trident.

Endpoints	Finalidade
Vários locais de terceiros, por exemplo: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org Locais de terceiros estão sujeitos a alterações.	Durante as atualizações, o Cloud Manager baixa os pacotes mais recentes para dependências de terceiros.

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

Endpoints	Finalidade
O host do conetor	Você deve inserir o endereço IP do host de um navegador da Web para carregar o console do Cloud Manager. Dependendo da sua conetividade com o seu provedor de nuvem, você pode usar o IP privado ou um IP público atribuído ao host: • Um IP privado funciona se você tiver uma VPN e acesso direto à sua rede virtual • Um IP público funciona em qualquer cenário de rede Em qualquer caso, você deve proteger o acesso à rede, garantindo que as regras do grupo de segurança permitam o acesso somente de IPs ou sub-redes autorizados.
https://auth0.com https://cdn.auth0.com://NetApp-cloud-account.auth0.com https://services.cloud.NetApp.com	Seu navegador da Web se coneta a esses endpoints para autenticação de usuário centralizada por meio do NetApp Cloud Central.
https://widget.intercom.io	Para um bate-papo no produto que permite conversar com especialistas em nuvem da NetApp.

Regras de firewall para Cloud Volumes ONTAP

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

As regras de firewall para o Cloud Volumes ONTAP exigem regras de entrada e saída.

Regras de entrada

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

Protocolo	Porta	Finalidade
Todo o ICMP	Tudo	Fazer ping na instância
HTTP	80	Acesso HTTP ao console da Web do System Manager usando o endereço IP do LIF de gerenciamento de cluster
HTTPS	443	Acesso HTTPS ao console da Web do System Manager usando o endereço IP do LIF de gerenciamento de cluster
SSH	22	Acesso SSH ao endereço IP do LIF de gerenciamento de cluster ou um LIF de gerenciamento de nó
TCP	111	Chamada de procedimento remoto para NFS
TCP	139	Sessão de serviço NetBIOS para CIFS
TCP	161-162	Protocolo de gerenciamento de rede simples
TCP	445	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
TCP	635	Montagem em NFS
TCP	749	Kerberos
TCP	2049	Daemon do servidor NFS
TCP	3260	Acesso iSCSI através do iSCSI data LIF
TCP	4045	Daemon de bloqueio NFS
TCP	4046	Monitor de status da rede para NFS
TCP	10000	Backup usando NDMP
TCP	11104	Gestão de sessões de comunicação entre clusters para SnapMirror
TCP	11105	Transferência de dados SnapMirror usando LIFs entre clusters
UDP	111	Chamada de procedimento remoto para NFS
UDP	161-162	Protocolo de gerenciamento de rede simples
UDP	635	Montagem em NFS
UDP	2049	Daemon do servidor NFS
UDP	4045	Daemon de bloqueio NFS
UDP	4046	Monitor de status da rede para NFS
UDP	4049	Protocolo rquotad NFS

Regras de saída

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

Regras básicas de saída

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

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

Regras de saída avançadas

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

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

Serviço	Protocolo	Porta	Fonte	Destino	Finalidade
Ative Directory					

	TCP	445	DATA LIF (NFS, CIFS)	Floresta do ative Directory	Microsoft SMB/CIFS sobre TCP com enquadramento NetBIOS
Serviço	**Protocolo**	**Porta**	**Fonte**	**Destino**	**Finalidade**
	TCP	464	DATA LIF (NFS, CIFS)	Floresta do ative Directory	Kerberos V alterar e definir senha (SET_CHANGE)
	UDP	464	DATA LIF (NFS, CIFS)	Floresta do ative Directory	Administração de chaves Kerberos
	TCP	749	DATA LIF (NFS, CIFS)	Floresta do ative Directory	Palavra-passe de alteração e definição Kerberos V (RPCSEC_GSS)
Cluster	Todo o tráfego	Todo o tráfego	Todos os LIFs em um nó	Todos os LIFs no outro nó	Comunicações entre clusters (apenas Cloud Volumes ONTAP HA)
	TCP	3000	LIF de gerenciamento de nós	Ha mediador	Chamadas ZAPI (somente Cloud Volumes ONTAP HA)
	ICMP	1	LIF de gerenciamento de nós	Ha mediador	Manter vivo (apenas Cloud Volumes ONTAP HA)
DHCP	UDP	68	LIF de gerenciamento de nós	DHCP	Cliente DHCP para configuração pela primeira vez
DHCPS	UDP	67	LIF de gerenciamento de nós	DHCP	Servidor DHCP
DNS	UDP	53	LIF e LIF de dados de gerenciamento de nós (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	LIF de gerenciamento de nós	Servidores de destino	Cópia NDMP
SMTP	TCP	25	LIF de gerenciamento de nós	Servidor de correio	Alertas SMTP, podem ser usados para AutoSupport
SNMP	TCP	161	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
	UDP	161	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
	TCP	162	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP
	UDP	162	LIF de gerenciamento de nós	Monitorar o servidor	Monitoramento por traps SNMP

Serviço	Protocolo	Porta	Fonte	Destino	Finalidade
SnapMirror	TCP	11104	LIF entre clusters	LIFs ONTAP entre clusters	Gestão de sessões de comunicação entre clusters para SnapMirror
	TCP	11105	LIF entre clusters	LIFs ONTAP entre clusters	Transferência de dados SnapMirror
Syslog	UDP	514	LIF de gerenciamento de nós	Servidor syslog	Mensagens de encaminhamento do syslog

Regras de firewall para o conetor

As regras de firewall para o conetor exigem regras de entrada e saída.

Regras de entrada

A origem das regras de entrada nas regras de firewall predefinidas é 0,0.0,0/0.

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

Regras de saída

As regras de firewall predefinidas para o conetor abrem todo o tráfego de saída. Se isso for aceitável, siga as regras básicas de saída. Se você precisar de regras mais rígidas, use as regras de saída avançadas.

Regras básicas de saída

As regras de firewall predefinidas para o conetor incluem as seguintes regras de saída.

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

Regras de saída avançadas

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

O endereço IP de origem é o host do conetor.

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

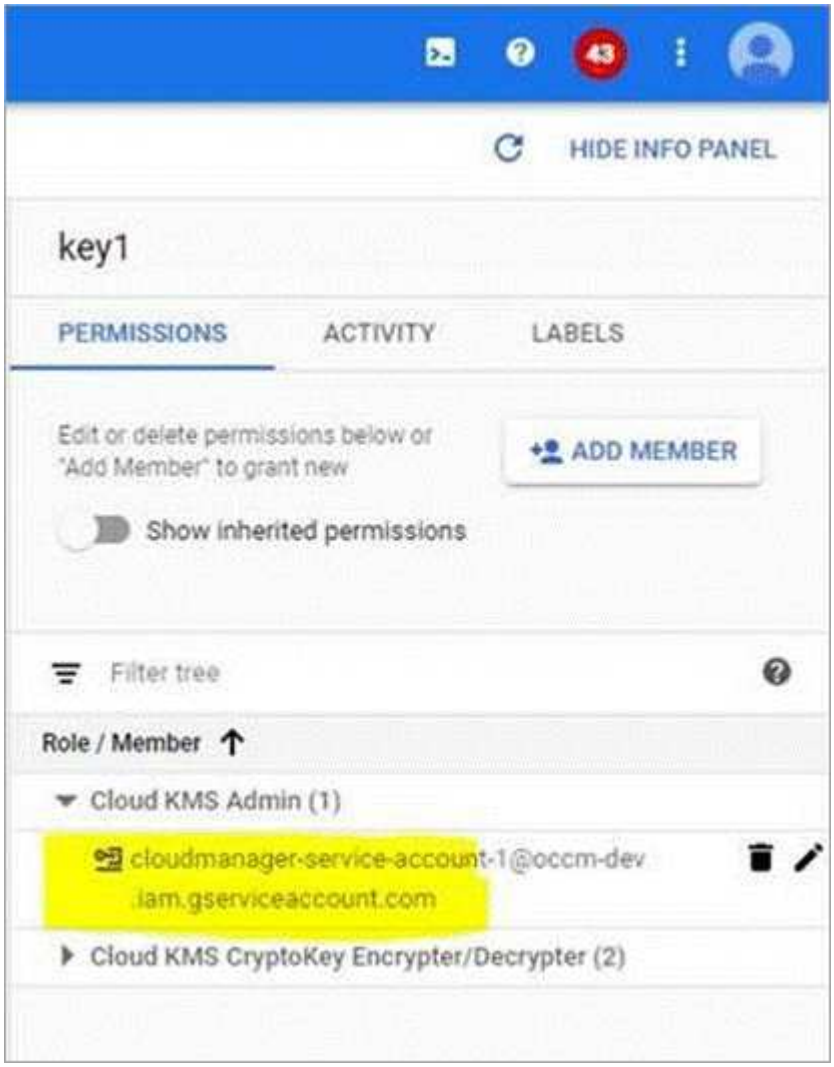
Usando chaves de criptografia gerenciadas pelo cliente com o Cloud Volumes ONTAP

Embora o Google Cloud Storage sempre criptografe seus dados antes de serem gravados no disco, você pode usar as APIs do Cloud Manager para criar um sistema Cloud Volumes ONTAP que use *chaves de criptografia gerenciadas pelo cliente*. Essas são as chaves que você gera e gerencia no GCP usando o Cloud Key Management

Service.

Passos

1. Dê permissão à conta de serviço do conetor para usar a chave de criptografia.



2. Obtenha o "id" da chave invocando o comando GET para a API /gcp/vsa/metadata/gcp-Encryption-keys.
3. Use o parâmetro "GcpEncryption" com sua solicitação de API ao criar um ambiente de trabalho.

Exemplo

```
"gcpEncryptionParameters": {
    "key": "projects/tlv-support/locations/us-
east4/keyRings/Nikiskeys/cryptoKeys/generatedkey1"
  }
```

Consulte a "Guia do desenvolvedor de API"para obter mais detalhes sobre como utilizar o parâmetro "GcpEncryption".

Iniciando o Cloud Volumes ONTAP na GCP

É possível iniciar um sistema Cloud Volumes ONTAP de nó único no GCP criando um ambiente de trabalho.

O que você vai precisar

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

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

- "Você deve estar preparado para deixar o conetor funcionando o tempo todo".
- Você deve ter escolhido uma configuração e obtido informações de rede do GCP do administrador. Para obter detalhes, "Planejando sua configuração do Cloud Volumes ONTAP"consulte .
- Para implantar um sistema BYOL, você precisa do número de série de 20 dígitos (chave de licença) para cada nó.
- As seguintes APIs do Google Cloud devem ser "habilitado em seu projeto":
  - API do Cloud Deployment Manager V2
  - API Cloud Logging
  - API do Cloud Resource Manager
  - API do mecanismo de computação
  - API de gerenciamento de identidade e acesso (IAM)

Passos

1. Na página ambientes de trabalho, clique em **Adicionar ambiente de trabalho** e siga as instruções.
2. **Escolha um local**: Selecione **Google Cloud** e **Cloud Volumes ONTAP**.
3. **Detalhes e credenciais**: Selecione um projeto, especifique um nome de cluster, adicione rótulos opcionalmente e especifique credenciais.

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

Campo	Descrição
Nome do ambiente de trabalho	O Cloud Manager usa o nome do ambiente de trabalho para nomear o sistema Cloud Volumes ONTAP e a instância de VM do GCP. Ele também usa o nome como prefixo para o grupo de segurança predefinido, se você selecionar essa opção.
Adicionar etiquetas	Os rótulos são metadados para seus recursos do GCP. O Cloud Manager adiciona os rótulos ao sistema Cloud Volumes ONTAP e aos recursos do GCP associados ao sistema. Você pode adicionar até quatro rótulos da interface do usuário ao criar um ambiente de trabalho e, em seguida, adicionar mais após a criação. Observe que a API não limita a quatro rótulos ao criar um ambiente de trabalho. Para obter informações sobre etiquetas, "Documentação do Google Cloud: Etiquetagem de recursos" consulte .

Campo	Descrição
Nome de utilizador e palavra-passe	Essas são as credenciais da conta de administrador do cluster do Cloud Volumes ONTAP. Você pode usar essas credenciais para se conetar ao Cloud Volumes ONTAP por meio do Gerenciador de sistema ou da CLI dele.
Editar projeto	Selecione o projeto onde você deseja que o Cloud Volumes ONTAP resida. O projeto padrão é o projeto em que o Cloud Manager reside. Se você não vir nenhum projeto adicional na lista suspensa, ainda não associou a conta de serviço do Cloud Manager a outros projetos. Vá para o console do Google Cloud, abra o serviço IAM e selecione o projeto. Adicione a conta de serviço com a função Cloud Manager a esse projeto. Você precisará repetir esta etapa para cada projeto. Esta é a conta de serviço configurada para o Cloud Manager, "conforme descrito no passo 2b desta 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, é necessário selecionar um projeto do GCP associado a uma assinatura do Cloud Volumes ONTAP no mercado do GCP.

O vídeo a seguir mostra como associar uma assinatura do Marketplace de pagamento conforme o uso ao projeto do GCP:

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

4. **Localização e conetividade**: Selecione um local, escolha uma política de firewall e marque a caixa de seleção para confirmar a conetividade de rede com o armazenamento do Google Cloud para disposição em camadas de dados.

   Se você quiser categorizar dados inativos em um intervalo do Google Cloud Storage, a sub-rede na qual o Cloud Volumes ONTAP reside deve ser configurada para acesso privado do Google. Para obter instruções, "Documentação do Google Cloud: Configurando o acesso privado do Google" consulte .

5. **Conta do site de suporte e licença**: Especifique se você deseja usar o pagamento conforme o uso ou o BYOL e especifique uma conta do site de suporte da NetApp.

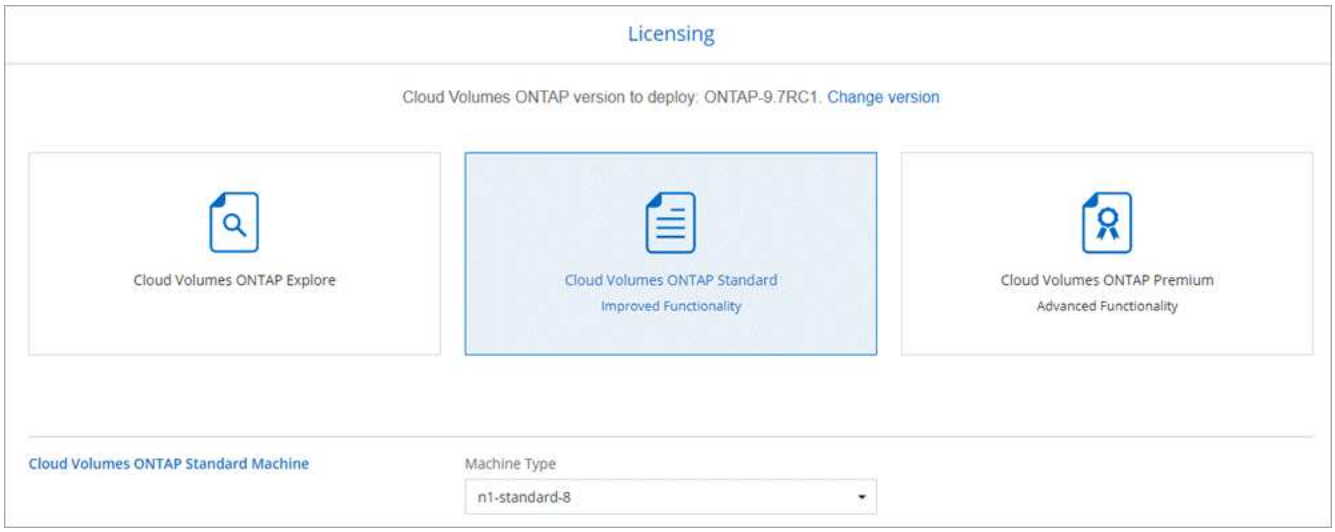
   Para entender como as licenças funcionam, "Licenciamento"consulte .

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

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

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

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



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

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

8. **Recursos de armazenamento subjacentes**: Escolha configurações para o agregado inicial: Um tipo de disco e o tamanho de cada disco.

   O tipo de disco é para o volume inicial. Você pode escolher um tipo de disco diferente para volumes subsequentes.

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

   Para obter ajuda sobre como escolher um tipo e tamanho de disco, "Dimensionamento do seu sistema na GCP"consulte .

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

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

   "Saiba mais sobre a velocidade de escrita".

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

   "Saiba mais sobre o armazenamento WORM".

10. **Disposição em camadas de dados no Google Cloud Platform**: Escolha se deseja habilitar a disposição em camadas de dados no agregado inicial, escolher uma classe de armazenamento para os dados em camadas e, em seguida, selecionar uma conta de serviço que tenha a função de administrador de armazenamento predefinida (necessária para o Cloud Volumes ONTAP 9,7) ou selecionar uma conta do GCP (necessária para o Cloud Volumes ONTAP 9,6).

Observe o seguinte:

- O Cloud Manager define a conta de serviço na instância do Cloud Volumes ONTAP. Essa conta de serviço fornece permissões para categorização de dados em um bucket do Google Cloud Storage. Certifique-se de adicionar a conta de serviço do Cloud Manager como usuário da conta de serviço em camadas, caso contrário, você não pode selecioná-la no Cloud Manager.
- Para obter ajuda com a adição de uma conta do GCP, "Configuração e adição de contas do GCP para categorização de dados com o 9,6"consulte .
- Você pode escolher uma política específica de disposição em categorias de volume ao criar ou editar um volume.
- Se você desabilitar a disposição em camadas de dados, poderá ativá-la em agregados subsequentes, mas precisará desativar o sistema e adicionar uma conta de serviço a partir do console do GCP.

  "Saiba mais sobre categorização de dados".

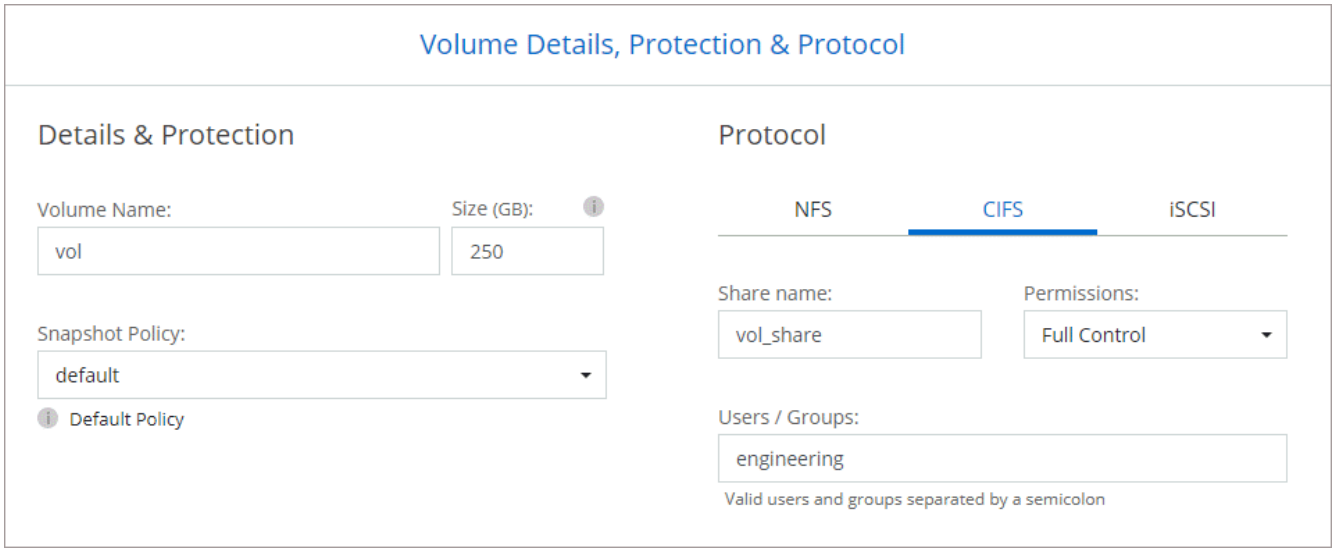
11. **Criar volume**: Insira os detalhes do novo volume ou clique em **Ignorar**.

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

Campo	Descrição
Tamanho	O tamanho máximo que você pode inserir depende, em grande parte, se você ativar o provisionamento de thin, o que permite criar um volume maior do que o armazenamento físico atualmente disponível para ele.
Controle de acesso (somente para NFS)	Uma política de exportação define os clientes na sub-rede que podem acessar o volume. Por padrão, o Cloud Manager insere um valor que fornece acesso a todas as instâncias na sub-rede.
Permissões e utilizadores/grupos (apenas para CIFS)	Esses campos permitem controlar o nível de acesso a um compartilhamento para usuários e grupos (também chamados de listas de controle de acesso ou ACLs). Você pode especificar usuários ou grupos do Windows locais ou de domínio, ou usuários ou grupos UNIX. Se você especificar um nome de usuário do domínio do Windows, você deve incluir o domínio do usuário usando o nome de domínio do formato.
Política de instantâneos	Uma política de cópia Snapshot especifica a frequência e o número de cópias snapshot do NetApp criadas automaticamente. Uma cópia Snapshot do NetApp é uma imagem pontual do sistema de arquivos que não afeta a performance e exige o mínimo de storage. Você pode escolher a política padrão ou nenhuma. Você pode escolher nenhum para dados transitórios: Por exemplo, tempdb para Microsoft SQL Server.
Opções avançadas (somente para NFS)	Selecione uma versão NFS para o volume: NFSv3 ou NFSv4.

Campo	Descrição
Grupo de iniciadores e IQN (apenas para iSCSI)	Os destinos de armazenamento iSCSI são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Os grupos de iniciadores são tabelas de nomes de nós de host iSCSI e controlam quais iniciadores têm acesso a quais LUNs. Os destinos iSCSI se conetam à rede por meio de adaptadores de rede Ethernet (NICs) padrão, placas de mecanismo de descarga TCP (TOE) com iniciadores de software, adaptadores de rede convergidos (CNAs) ou adaptadores de barramento de host dedicados (HBAs) e são identificados por IQNs (iSCSI Qualified Names). Quando você cria um volume iSCSI, o Cloud Manager cria automaticamente um LUN para você. Simplificamos a criação de apenas um LUN por volume, para que não haja gerenciamento envolvido. Depois de criar o volume, "Use o IQN para se conetar ao LUN a partir de seus hosts".

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



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

Campo	Descrição
Endereço IP primário e secundário do DNS	Os endereços IP dos servidores DNS que fornecem resolução de nomes para o servidor CIFS. Os servidores DNS listados devem conter os Registros de localização de serviço (SRV) necessários para localizar os servidores LDAP do ative Directory e os controladores de domínio para o domínio em que o servidor CIFS irá ingressar.
Ative Directory Domain para aderir	O FQDN do domínio do ative Directory (AD) ao qual você deseja que o servidor CIFS se associe.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores à unidade organizacional especificada (ou) dentro do domínio do AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio AD.
Unidade organizacional	A unidade organizacional dentro do domínio AD a associar ao servidor CIFS. A predefinição é computadores.

Campo	Descrição
Domínio DNS	O domínio DNS da máquina virtual de storage (SVM) do Cloud Volumes ONTAP. Na maioria dos casos, o domínio é o mesmo que o domínio AD.
NTP Server	Selecione **Use ative Directory Domain** para configurar um servidor NTP usando o DNS do ative Directory. Se você precisa configurar um servidor NTP usando um endereço diferente, então você deve usar a API. Consulte "Guia do desenvolvedor de API do Cloud Manager"para obter detalhes.

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

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

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

Resultado

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

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

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

Depois de terminar

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

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

Provisione e gerencie o storage

Provisionamento de storage

Você pode provisionar storage adicional para seus sistemas Cloud Volumes ONTAP usando o Cloud Manager, gerenciando volumes e agregados.

Todos os discos e agregados devem ser criados e excluídos diretamente do Cloud Manager. Você não deve executar essas ações de outra ferramenta de gerenciamento. Isso pode afetar a estabilidade do sistema, dificultar a capacidade de adicionar discos no futuro e, potencialmente, gerar taxas redundantes de provedores de nuvem.

Criando volumes FlexVol

Se você precisar de mais storage depois de iniciar um sistema Cloud Volumes ONTAP, poderá criar novos volumes FlexVol para NFS, CIFS ou iSCSI a partir do Cloud Manager.

Sobre esta tarefa

Quando você cria um volume iSCSI, o Cloud Manager cria automaticamente um LUN para você. Simplificamos a criação de apenas um LUN por volume, para que não haja gerenciamento envolvido. Depois de criar o volume, Use o IQN para se conetar ao LUN a partir de seus hosts.

Você pode criar LUNs adicionais no System Manager ou na CLI.

Antes de começar

Se você quiser usar o CIFS na AWS, você deve ter configurado o DNS e o ative Directory. Para obter detalhes, "Requisitos de rede para o Cloud Volumes ONTAP para AWS"consulte .

Passos

1. Na página ambientes de trabalho, clique duas vezes no nome do sistema Cloud Volumes ONTAP no qual você deseja provisionar volumes FlexVol.
2. Crie um novo volume em qualquer agregado ou em um agregado específico:

Ação	Passos
Crie um novo volume e deixe que o Cloud Manager escolha o agregado que contém	Clique em **Adicionar novo volume**.
Crie um novo volume em um agregado específico	a. Clique no ícone do menu e, em seguida, clique em **Avançado > Alocação avançada**. b. Clique no menu de um agregado. c. Clique em **criar volume**.

3. Insira os detalhes do novo volume e clique em **continuar**.

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

Campo	Descrição
Tamanho	O tamanho máximo que você pode inserir depende, em grande parte, se você ativar o provisionamento de thin, o que permite criar um volume maior do que o armazenamento físico atualmente disponível para ele.
Controle de acesso (somente para NFS)	Uma política de exportação define os clientes na sub-rede que podem acessar o volume. Por padrão, o Cloud Manager insere um valor que fornece acesso a todas as instâncias na sub-rede.

Campo	Descrição
Permissões e utilizadores/grupos (apenas para CIFS)	Esses campos permitem controlar o nível de acesso a um compartilhamento para usuários e grupos (também chamados de listas de controle de acesso ou ACLs). Você pode especificar usuários ou grupos do Windows locais ou de domínio, ou usuários ou grupos UNIX. Se você especificar um nome de usuário do domínio do Windows, você deve incluir o domínio do usuário usando o nome de domínio do formato.
Política de instantâneos	Uma política de cópia Snapshot especifica a frequência e o número de cópias snapshot do NetApp criadas automaticamente. Uma cópia Snapshot do NetApp é uma imagem pontual do sistema de arquivos que não afeta a performance e exige o mínimo de storage. Você pode escolher a política padrão ou nenhuma. Você pode escolher nenhum para dados transitórios: Por exemplo, tempdb para Microsoft SQL Server.
Opções avançadas (somente para NFS)	Selecione uma versão NFS para o volume: NFSv3 ou NFSv4.
Grupo de iniciadores e IQN (apenas para iSCSI)	Os destinos de armazenamento iSCSI são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Os grupos de iniciadores são tabelas de nomes de nós de host iSCSI e controlam quais iniciadores têm acesso a quais LUNs. Os destinos iSCSI se conetam à rede por meio de adaptadores de rede Ethernet (NICs) padrão, placas de mecanismo de descarga TCP (TOE) com iniciadores de software, adaptadores de rede convergidos (CNAs) ou adaptadores de barramento de host dedicados (HBAs) e são identificados por IQNs (iSCSI Qualified Names). Quando você cria um volume iSCSI, o Cloud Manager cria automaticamente um LUN para você. Simplificamos a criação de apenas um LUN por volume, para que não haja gerenciamento envolvido. Depois de criar o volume, "Use o IQN para se conetar ao LUN a partir de seus hosts".

4. Se você escolheu o protocolo CIFS e o servidor CIFS não tiver sido configurado, especifique os detalhes do servidor na caixa de diálogo criar um servidor CIFS e clique em **Salvar e continuar**:

Campo	Descrição
Endereço IP primário e secundário do DNS	Os endereços IP dos servidores DNS que fornecem resolução de nomes para o servidor CIFS. Os servidores DNS listados devem conter os Registros de localização de serviço (SRV) necessários para localizar os servidores LDAP do ative Directory e os controladores de domínio para o domínio em que o servidor CIFS irá ingressar.
Ative Directory Domain para aderir	O FQDN do domínio do ative Directory (AD) ao qual você deseja que o servidor CIFS se associe.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores à unidade organizacional especificada (ou) dentro do domínio do AD.
Nome NetBIOS do servidor CIFS	Um nome de servidor CIFS exclusivo no domínio AD.

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

5. Na página Perfil de uso, tipo de disco e Política de disposição em camadas, escolha se deseja habilitar recursos de eficiência de storage, escolher um tipo de disco e editar a política de disposição em camadas, se necessário.

   Para obter ajuda, consulte o seguinte:

   ◦ "Compreender os perfis de utilização de volume"
   ◦ "Dimensionamento do seu sistema na AWS"
   ◦ "Dimensionamento do seu sistema no Azure"
   ◦ "Visão geral de categorização de dados"

6. Clique em **Go**.

Resultado

A Cloud Volumes ONTAP provisiona o volume.

Depois de terminar

Se você provisionou um compartilhamento CIFS, dê aos usuários ou grupos permissões para os arquivos e pastas e verifique se esses usuários podem acessar o compartilhamento e criar um arquivo.

Se você quiser aplicar cotas a volumes, use o System Manager ou a CLI. As cotas permitem restringir ou rastrear o espaço em disco e o número de arquivos usados por um usuário, grupo ou qtree.

Criação de volumes FlexVol no segundo nó em uma configuração de HA

Por padrão, o Cloud Manager cria volumes no primeiro nó em uma configuração de HA. Se você precisar de uma configuração ativo-ativo, na qual ambos os nós fornecem dados aos clientes, será necessário criar agregados e volumes no segundo nó.

Passos

1. Na página ambientes de trabalho, clique duas vezes no nome do ambiente de trabalho do Cloud Volumes ONTAP no qual você deseja gerenciar agregados.
2. Clique no ícone do menu e, em seguida, clique em **Avançado > Alocação avançada**.
3. Clique em **Adicionar agregado** e, em seguida, crie o agregado.
4. No nó inicial, escolha o segundo nó no par de HA.
5. Depois que o Cloud Manager criar o agregado, selecione-o e clique em **criar volume**.
6. Insira os detalhes do novo volume e clique em **criar**.

Depois de terminar

Você pode criar volumes adicionais neste agregado, se necessário.

Para pares de HA implantados em várias zonas de disponibilidade da AWS, é necessário montar o volume nos clientes usando o endereço IP flutuante do nó no qual o volume reside.

Criando agregados

Você pode criar agregados ou permitir que o Cloud Manager faça isso por você quando cria volumes. O benefício de criar agregados por conta própria é que você pode escolher o tamanho de disco subjacente, que permite dimensionar seu agregado para a capacidade ou a performance de que precisa.

Passos

1. Na página ambientes de trabalho, clique duas vezes no nome da instância do Cloud Volumes ONTAP na qual você deseja gerenciar agregados.
2. Clique no ícone do menu e, em seguida, clique em **Avançado > Alocação avançada**.
3. Clique em **Adicionar agregado** e especifique os detalhes do agregado.

   Para obter ajuda sobre o tipo de disco e o tamanho do disco, "Planejando sua configuração"consulte .

4. Clique em **Go** e, em seguida, clique em **Approve and Purchase**.

Conetando um LUN a um host

Quando você cria um volume iSCSI, o Cloud Manager cria automaticamente um LUN para você. Simplificamos a criação de apenas um LUN por volume, para que não haja gerenciamento envolvido. Depois de criar o volume, use o IQN para se conetar ao LUN a partir de seus hosts.

Observe o seguinte:

1. O gerenciamento automático de capacidade do Cloud Manager não se aplica a LUNs. Quando o Cloud Manager cria um LUN, ele desativa o recurso de crescimento automático.
2. Você pode criar LUNs adicionais no System Manager ou na CLI.

Passos

1. Na página ambientes de trabalho, clique duas vezes no ambiente de trabalho do Cloud Volumes ONTAP no qual você deseja gerenciar volumes.
2. Selecione um volume e clique em **Target IQN**.
3. Clique em **Copiar** para copiar o nome IQN.
4. Configure uma conexão iSCSI do host para o LUN.

- "Configuração expressa ONTAP 9 iSCSI para Red Hat Enterprise Linux: Iniciando as sessões iSCSI com o destino"
- "Configuração expressa iSCSI ONTAP 9 para Windows: Iniciar sessões iSCSI com o destino"

Usando o FlexCache volumes para acelerar o acesso aos dados

Um volume FlexCache é um volume de storage que armazena em cache dados de leitura NFS de um volume de origem (ou origem). Leituras subsequentes para os dados armazenados em cache resultam em acesso mais rápido a esses dados.

Você pode usar o FlexCache volumes para acelerar o acesso aos dados ou descarregar tráfego de volumes acessados com muita facilidade. Os volumes FlexCache ajudam a melhorar o desempenho, especialmente quando os clientes precisam acessar os mesmos dados repetidamente, porque os dados podem ser fornecidos diretamente sem ter que acessar o volume de origem. O FlexCache volumes funciona bem com workloads do sistema com uso intenso de leitura.

No momento, o Cloud Manager não fornece gerenciamento do FlexCache volumes, mas você pode usar a CLI ou o Gerenciador de sistemas do ONTAP ONTAP para criar e gerenciar o FlexCache volumes:

- "Guia de energia do FlexCache volumes para acesso mais rápido aos dados"
- "Criando volumes FlexCache no Gerenciador de sistemas"

A partir da versão 3.7.2, o Cloud Manager gera uma licença FlexCache para todos os novos sistemas Cloud Volumes ONTAP. A licença inclui um limite de uso de 500 GB.

Para gerar a licença, o Cloud Manager precisa acessar o https://ipa-signer.cloudmanager.NetApp.com. Certifique-se de que este URL está acessível a partir do firewall.

Gerenciamento do storage existente

Com o Cloud Manager, você gerencia volumes, agregados e servidores CIFS. Ele também solicita que você mova volumes para evitar problemas de capacidade.

Gerenciamento de volumes existentes

Você pode gerenciar volumes existentes conforme suas necessidades de storage mudam. Você pode exibir, editar, clonar, restaurar e excluir volumes.

Passos

1. Na página ambientes de trabalho, clique duas vezes no ambiente de trabalho do Cloud Volumes ONTAP no qual você deseja gerenciar volumes.
2. Gerencie seus volumes:

Tarefa	Ação
Exibir informações sobre um volume	Selecione um volume e clique em **Info**.
Editar um volume (somente volumes de leitura e gravação)	a. Selecione um volume e clique em **Editar**. b. Modifique a política Snapshot do volume, a versão do protocolo NFS, a lista de controle de acesso NFS ou as permissões de compartilhamento e clique em **Atualizar**. Se você precisar de políticas Snapshot personalizadas, poderá criá-las usando o System Manager.
Clonar um volume	a. Selecione um volume e clique em **Clone**. b. Modifique o nome do clone conforme necessário e clique em **Clone**. Esse processo cria um volume FlexClone. Um volume FlexClone é uma cópia gravável e pontual que usa espaço reduzido porque usa um pouco de espaço para metadados e, em seguida, consome espaço adicional apenas à medida que os dados são alterados ou adicionados. Para saber mais sobre o FlexClone volumes, consulte "Guia de gerenciamento de storage lógico do ONTAP 9".
Restaure os dados de uma cópia Snapshot para um novo volume	a. Selecione um volume e clique em **Restaurar a partir da cópia Snapshot**. b. Selecione uma cópia Snapshot, insira um nome para o novo volume e clique em **Restore**.
Criar uma cópia Snapshot sob demanda	a. Selecione um volume e clique em **criar uma cópia Snapshot**. b. Altere o nome, se necessário, e clique em **criar**.

Tarefa	Ação
Obtenha o comando NFS mount	a. Selecione um volume e clique em **Mount Command**. b. Clique em **Copiar**.
Visualize o IQN alvo para um volume iSCSI	a. Selecione um volume e clique em **Target IQN**. b. Clique em **Copiar**. c. "Use o IQN para se conetar ao LUN a partir de seus hosts".
Altere o tipo de disco subjacente	a. Selecione um volume e, em seguida, clique em **alterar tipo de disco e Política de disposição em categorias**. b. Selecione o tipo de disco e clique em **alterar**. O Cloud Manager 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 disposição em camadas	a. Selecione um volume e, em seguida, clique em **alterar tipo de disco e Política de disposição em categorias**. b. Clique em **Editar política**. c. Selecione uma política diferente e clique em **alterar**. O Cloud Manager move o volume para um agregado existente que usa o tipo de disco selecionado com disposição em camadas ou cria um novo agregado para o volume.
Eliminar um volume	a. Selecione um volume e, em seguida, clique em **Delete**. b. Clique em **Delete** novamente para confirmar.

Gerenciamento de agregados existentes

Gerencie os agregados adicionando discos, visualizando informações sobre os agregados e excluindo-os.

Antes de começar

Se você quiser excluir um agregado, primeiro você deve ter excluído os volumes no agregado.

Sobre esta tarefa

Se um agregado estiver sem espaço, você poderá mover volumes para outro agregado usando o OnCommand System Manager.

Passos

1. Na página ambientes de trabalho, clique duas vezes no ambiente de trabalho do Cloud Volumes ONTAP no qual você deseja gerenciar agregados.
2. Clique no ícone do menu e, em seguida, clique em **Avançado > Alocação avançada**.

3. Gerencie seus agregados:

Tarefa	Ação
Exibir informações sobre um agregado	Selecione um agregado e clique em **Info**.
Crie um volume em um agregado específico	Selecione um agregado e clique em **criar volume**.
Adicione discos a um agregado	a. Selecione um agregado e clique em **Adicionar discos AWS** ou **Adicionar discos Azure**. b. Selecione o número de discos que deseja adicionar e clique em **Adicionar**.  Todos os discos em um agregado devem ter o mesmo tamanho.
Excluir um agregado	a. Selecione um agregado que não contenha volumes e clique em **Excluir**. b. Clique em **Delete** novamente para confirmar.

Modificação do servidor CIFS

Se você alterar seus servidores DNS ou domínio do ative Directory, será necessário modificar o servidor CIFS no Cloud Volumes ONTAP para que ele possa continuar a servir armazenamento aos clientes.

Passos

1. No ambiente de trabalho, clique no ícone do menu e, em seguida, clique em **Avançado > Configuração CIFS**.
2. Especifique as configurações para o servidor CIFS:

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

Tarefa	Ação
Unidade organizacional	A unidade organizacional dentro do domínio AD a associar ao servidor CIFS. A predefinição é computadores. Se você configurar o AWS Managed Microsoft AD como o servidor AD para o Cloud Volumes ONTAP, deverá inserir neste campo **ou computadores**.
Domínio DNS	O domínio DNS da máquina virtual de storage (SVM) do Cloud Volumes ONTAP. Na maioria dos casos, o domínio é o mesmo que o domínio AD.
NTP Server	Selecione **Use ative Directory Domain** para configurar um servidor NTP usando o DNS do ative Directory. Se você precisa configurar um servidor NTP usando um endereço diferente, então você deve usar a API. Consulte "Guia do desenvolvedor de API do Cloud Manager"para obter detalhes.

3. Clique em **Salvar**.

Resultado

O Cloud Volumes ONTAP atualiza o servidor CIFS com as alterações.

Mover um volume

Mova volumes para utilização de capacidade, performance aprimorada e atender a contratos de nível de serviço.

Você pode mover um volume no System Manager selecionando um volume e o agregado de destino, iniciando a operação de movimentação de volume e, opcionalmente, monitorando a tarefa de movimentação de volume. Ao usar o System Manager, uma operação de movimentação de volume é concluída automaticamente.

Passos

1. Use o System Manager ou a CLI para mover os volumes para o agregado.

   Na maioria das situações, você pode usar o System Manager para mover volumes.

   Para obter instruções, consulte "Guia expresso de movimentação de volume do ONTAP 9" .

Movimentação de um volume quando o Cloud Manager exibe uma mensagem Ação necessária

O Cloud Manager pode exibir uma mensagem Ação necessária que diz que mover um volume é necessário para evitar problemas de capacidade, mas que não pode fornecer recomendações para corrigir o problema. Se isso acontecer, você precisa identificar como corrigir o problema e mover um ou mais volumes.

Passos

1. Identifique como corrigir o problema.
2. Com base em suas análises, mova volumes para evitar problemas de capacidade:
   - Mover volumes para outro sistema.
   - Mova volumes para outro agregado no mesmo sistema.

Identificar como corrigir problemas de capacidade

Se o Cloud Manager não puder fornecer recomendações para mover um volume para evitar problemas de capacidade, identifique os volumes que você precisa mover e se deve movê-los para outro agregado no

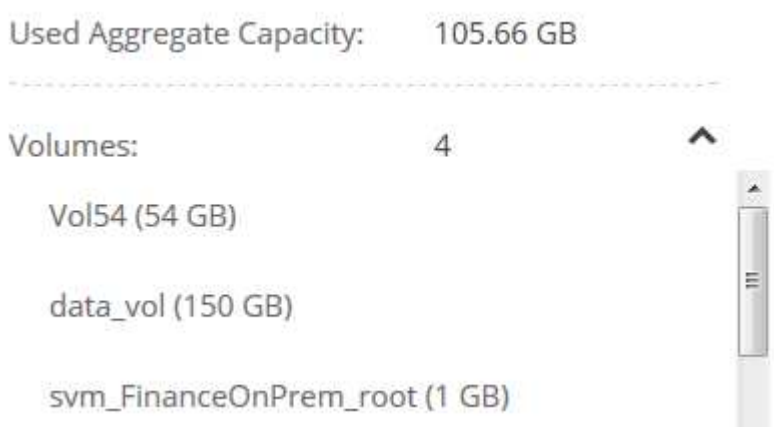
mesmo sistema ou para outro sistema.

Passos

1. Exiba as informações avançadas na mensagem Ação necessária para identificar o agregado que atingiu seu limite de capacidade.

   Por exemplo, as informações avançadas devem dizer algo semelhante ao seguinte: O agregado aggr1 atingiu seu limite de capacidade.

2. Identifique um ou mais volumes para sair do agregado:
   a. No ambiente de trabalho, clique no ícone do menu e, em seguida, clique em **Avançado > Alocação avançada**.
   b. Selecione o agregado e clique em **Info**.
   c. Expanda a lista de volumes.



   d. Revise o tamanho de cada volume e escolha um ou mais volumes para sair do agregado.

      Você deve escolher volumes grandes o suficiente para liberar espaço no agregado para evitar problemas de capacidade adicionais no futuro.

3. Se o sistema não tiver atingido o limite de disco, você deve mover os volumes para um agregado existente ou um novo agregado no mesmo sistema.

   Para obter detalhes, "Mover volumes para outro agregado para evitar problemas de capacidade"consulte .

4. Se o sistema tiver atingido o limite de disco, proceda de uma das seguintes formas:
   a. Exclua todos os volumes não utilizados.
   b. Reorganize volumes para liberar espaço em um agregado.

      Para obter detalhes, "Mover volumes para outro agregado para evitar problemas de capacidade"consulte .

   c. Mova dois ou mais volumes para outro sistema que tenha espaço.

      Para obter detalhes, "Mover volumes para outro sistema para evitar problemas de capacidade"consulte .

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 se o sistema atingir seu limite de disco.

Sobre esta tarefa

Pode seguir os passos desta tarefa para corrigir a seguinte mensagem Ação necessária:

```
 Moving a volume is necessary to avoid capacity issues; however, Cloud
Manager cannot perform this action for you because the system has reached
the disk limit.
.Passos
. Identifique um sistema Cloud Volumes ONTAP que tenha capacidade
disponível ou implante um novo sistema.
. Arraste e solte o ambiente de trabalho de origem no ambiente de trabalho
de destino para executar uma replicação de dados única do volume.
```

+
Para obter detalhes, "Replicação de dados entre sistemas"consulte .

1. Vá para a página Status da replicação e, em seguida, quebre a relação do SnapMirror para converter o volume replicado de um volume de proteção de dados para um volume de leitura/gravação.

   Para obter detalhes, "Gerenciamento de cronogramas e relacionamentos de replicação de dados"consulte .

2. Configure o volume para acesso aos dados.

   Para obter informações sobre como configurar um volume de destino para acesso a dados, consulte "Guia expresso de recuperação de desastres em volume do ONTAP 9" .

3. Eliminar o volume original.

   Para obter detalhes, "Gerenciamento de volumes existentes"consulte .

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

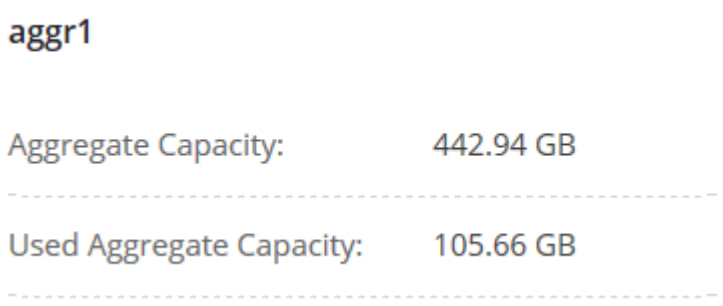
Pode seguir os passos desta tarefa para corrigir a seguinte mensagem Ação necessária:

```
 Moving two or more volumes is necessary to avoid capacity issues;
however, Cloud Manager cannot perform this action for you.
.Passos
. Verifique se um agregado existente tem capacidade disponível para os
volumes que você precisa mover:
```

+

.. No ambiente de trabalho, clique no ícone do menu e, em seguida, clique em **Avançado > Alocação avançada**.
.. Selecione cada agregado, clique em **Info** e, em seguida, visualize a capacidade disponível (capacidade agregada menos capacidade agregada utilizada).

+



1. Se necessário, adicione discos a um agregado existente:
   a. Selecione o agregado e clique em **Adicionar discos**.
   b. Selecione o número de discos a serem adicionados e clique em **Add**.
2. Se nenhum agregado tiver capacidade disponível, crie um novo agregado.

   Para obter detalhes, "Criando agregados"consulte .
3. Use o System Manager ou a CLI para mover os volumes para o agregado.
4. Na maioria das situações, você pode usar o System Manager para mover volumes.

   Para obter instruções, consulte "Guia expresso de movimentação de volume do ONTAP 9" .

Razões pelas quais um movimento de volume pode ter um desempenho lento

Mover um volume pode demorar mais tempo do que o esperado se qualquer uma das seguintes condições for verdadeira para o Cloud Volumes ONTAP:

- O volume é um clone.
- O volume é um pai de um clone.
- O agregado de origem ou destino tem um disco HDD (st1) otimizado para taxa de transferência única.
- O sistema Cloud Volumes ONTAP está na AWS e um agregado usa um esquema de nomenclatura mais antigo para objetos. Ambos os agregados têm que usar o mesmo formato de nome.

  Um esquema de nomenclatura mais antigo é usado se a categorização de dados tiver sido habilitada em um agregado na versão 9,4 ou anterior.
- As configurações de criptografia não correspondem aos agregados de origem e destino, ou uma rechavear está em andamento.
- A opção *-Tiering-policy* foi especificada na movimentação de volume para alterar a política de disposição em camadas.
- A opção *-generate-destination-key* foi especificada na movimentação de volume.

Disposição em camadas dos dados inativos em storage de objetos de baixo custo

Você pode reduzir os custos de storage do Cloud Volumes ONTAP combinando uma camada de desempenho de SSD ou HDD para dados ativos com uma camada de capacidade de storage de objetos para dados inativos. Para obter uma visão geral de alto nível, "Visão geral de categorização de dados"consulte .

Para configurar a disposição de dados em categorias, basta fazer o seguinte:

Escolha uma configuração suportada

A maioria das configurações é compatível. Se você tiver um sistema padrão, Premium ou BYOL da Cloud Volumes ONTAP executando a versão mais recente, então você deve estar pronto. "Saiba mais".

Garanta a conectividade entre o Cloud Volumes ONTAP e o storage de objetos

- Para a AWS, você precisará de um VPC Endpoint para S3. Saiba mais.
- Para o Azure, você não precisará fazer nada, desde que o Cloud Manager tenha as permissões necessárias. Saiba mais.
- Para o GCP, você precisa configurar a sub-rede para o Acesso Privado do Google e configurar uma conta de serviço. Saiba mais.

Escolha uma política de disposição em categorias ao criar, modificar ou replicar um volume

O Cloud Manager solicita que você escolha uma política de disposição em categorias ao criar, modificar ou replicar um volume.

- "Disposição em camadas dos dados em volumes de leitura-gravação"
- "Disposição de dados em camadas em volumes de proteção de dados"

O que não é necessário para a disposição em camadas de dados. 8217

- Não é necessário instalar uma licença de recurso para habilitar a disposição em camadas de dados.
- Não é necessário criar a categoria de capacidade (um bucket do S3, contêiner do Blob do Azure ou bucket do GCP). O Cloud Manager faz isso por você.

Configurações compatíveis com categorização de dados

Você pode habilitar a disposição de dados em categorias usando configurações e recursos específicos:

- A disposição de dados em categorias é compatível com o padrão Cloud Volumes ONTAP, Premium e BYOL, começando com as seguintes versões:
  - Versão 9,2 na AWS
  - Versão 9,4 no Azure com sistemas de nó único

- Versão 9,6 no Azure com pares de HA
- Versão 9,6 no GCP

> A disposição de dados em categorias não é suportada no Azure com o tipo de máquina virtual DS3_v2.

- Na AWS, o nível de performance pode ser SSDs de uso geral, SSDs IOPS provisionados ou HDDs otimizados para taxa de transferência.
- No Azure, o nível de desempenho pode ser discos gerenciados SSD Premium, discos gerenciados SSD padrão ou discos gerenciados HDD padrão.
- No GCP, o nível de performance pode ser SSDs ou HDDs (discos padrão).
- A disposição de dados em categorias é compatível com tecnologias de criptografia.
- O thin Provisioning deve estar ativado em volumes.

Requisitos para categorizar dados inativos no AWS S3

Certifique-se de que o Cloud Volumes ONTAP tem uma ligação ao S3. A melhor maneira de fornecer essa conexão é criando um endpoint VPC para o serviço S3. Para obter instruções, "Documentação da AWS: Criando um endpoint do Gateway" consulte .

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

Se tiver algum problema, "AWS Support Knowledge Center: Por que não consigo me conetar a um bucket do S3 usando um endpoint VPC de gateway?"consulte .

Requisitos para categorizar dados inativos no storage Azure Blob

Você não precisa configurar uma conexão entre o nível de performance e o nível de capacidade, desde que o Cloud Manager tenha as permissões necessárias. O Cloud Manager habilita um endpoint de serviço VNet para você se a política do Cloud Manager tiver estas permissões:

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

As permissões estão incluídas no último "Política do Cloud Manager".

Requisitos para categorizar dados inativos em um bucket do Google Cloud Storage

- A sub-rede em que o Cloud Volumes ONTAP reside deve ser configurada para o acesso privado do Google. Para obter instruções, "Documentação do Google Cloud: Configurando o acesso privado do Google" consulte .
- Você precisa de uma conta de serviço que tenha a função de administrador de storage predefinida. Você precisará selecionar essa conta de serviço ao criar um ambiente de trabalho do Cloud Volumes ONTAP.

  "Configure essa conta de serviço em categorias da seguinte forma":

a. Atribua a função predefinida *Storage Admin* à conta de serviço de disposição em camadas.

b. Adicione a conta de serviço do conetor como um *Usuário da conta de serviço* à conta de serviço em camadas.

   Você pode fornecer a função de usuário "na etapa 3 do assistente quando você cria a conta de serviço de disposição em camadas" , ou "conceda a função após a criação da conta de serviço".

   Você precisará selecionar a conta de serviço de disposição em camadas mais tarde ao criar um ambiente de trabalho do Cloud Volumes ONTAP.

Se você não habilitar a disposição de dados em categorias e selecionar uma conta de serviço ao criar o sistema Cloud Volumes ONTAP, será necessário desativar o sistema e adicionar a conta de serviço ao Cloud Volumes ONTAP a partir do console do GCP.

Disposição em camadas dos dados de volumes de leitura-gravação

O Cloud Volumes ONTAP pode categorizar dados inativos em volumes de leitura-gravação para storage de objetos econômico, liberando a categoria de performance para dados ativos.

Passos

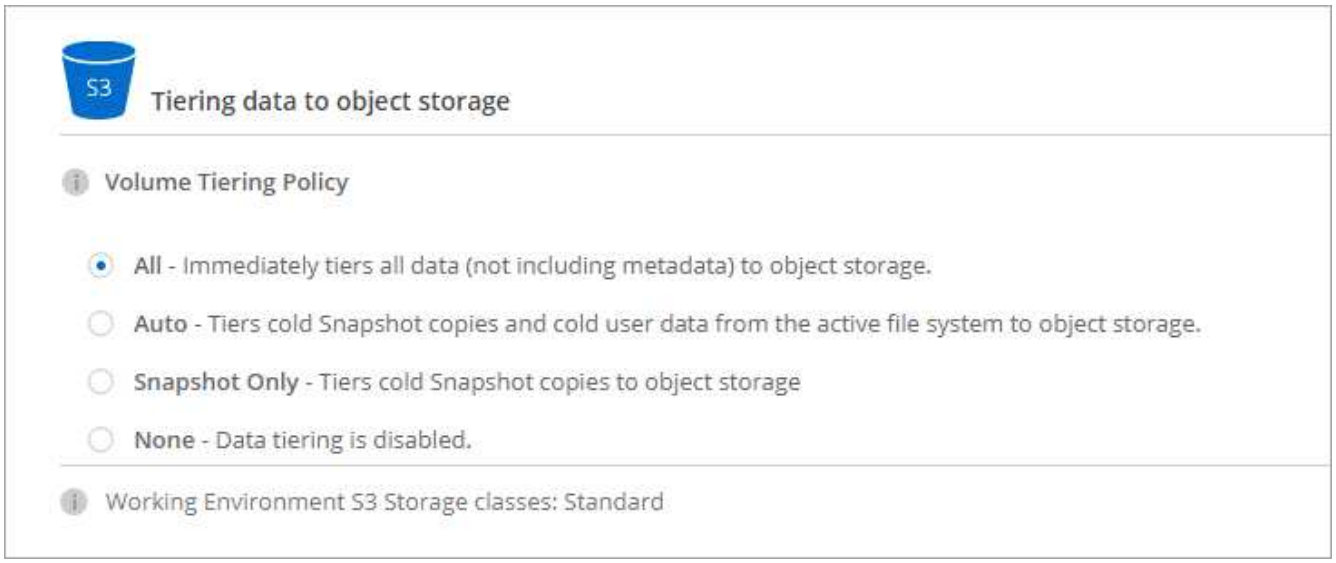
1. No ambiente de trabalho, crie um novo volume ou altere o nível de um volume existente:

Tarefa	Ação
Crie um novo volume	Clique em **Adicionar novo volume**.
Modificar um volume existente	Selecione o volume e clique em **alterar tipo de disco e Política de disposição em categorias**.

2. Selecione uma política de disposição em camadas.

   Para obter uma descrição dessas políticas, "Visão geral de categorização de dados"consulte .

   Exemplo



   O Cloud Manager cria um novo agregado para o volume se um agregado habilitado para categorização de dados ainda não existir.

Se você preferir criar agregados, habilite a disposição em categorias de dados em agregados ao criá-los.

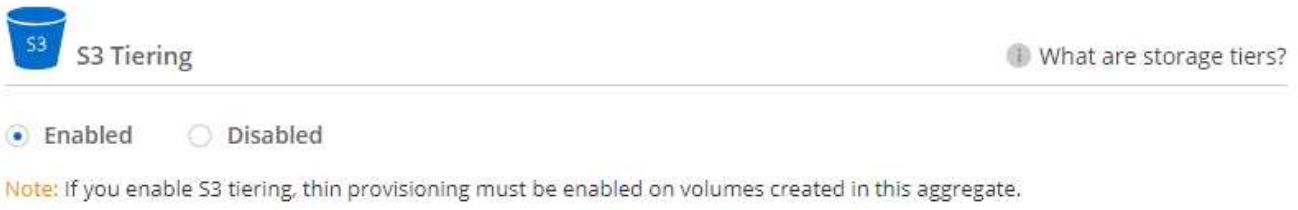
Disposição de dados em camadas em volumes de proteção de dados

O Cloud Volumes ONTAP pode categorizar dados de um volume de proteção de dados em uma categoria de capacidade. Se você ativar o volume de destino, os dados serão movidos gradualmente para o nível de performance à medida que forem lidos.

Passos

1. Na página ambientes de trabalho, selecione o ambiente de trabalho que contém o volume de origem e, em seguida, arraste-o para o ambiente de trabalho para o qual pretende replicar o volume.
2. Siga as instruções até chegar à página de disposição em categorias e habilitar a disposição de dados em categorias no storage de objetos.

   Exemplo



   Para obter ajuda com a replicação de dados, "Replicação de dados de e para a nuvem"consulte .

Alteração da classe de armazenamento para dados em camadas

Depois de implantar o Cloud Volumes ONTAP, você poderá reduzir os custos de storage alterando a classe de storage para dados inativos que não foram acessados por 30 dias. Os custos de acesso são maiores se você acessar os dados, então você deve levar isso em consideração antes de alterar a classe de storage.

A classe de armazenamento para dados em camadas é de todo o sistema, it não por volume.

Para obter informações sobre classes de armazenamento suportadas, "Visão geral de categorização de dados"consulte .

Passos

1. No ambiente de trabalho, clique no ícone de menu e, em seguida, clique em **classes de armazenamento** ou **disposição em camadas de armazenamento Blob**.
2. Escolha uma classe de armazenamento e clique em **Salvar**.

Posso habilitar a categorização de dados em um agregado existente?

Não, você não pode habilitar a disposição em categorias de dados em um agregado existente. Só é possível habilitar a disposição de dados em categorias em novos agregados.

Você pode habilitar a disposição de dados em categorias em um novo agregado, "criando um agregado você mesmo" ou ao criar um novo volume com a disposição de dados em categorias ativada. O Cloud Manager criaria um novo agregado para o volume se um agregado habilitado para disposição em camadas de dados

ainda não existir.

Gerenciamento de VMs de storage

Uma VM de armazenamento é uma máquina virtual em execução no ONTAP que fornece serviços de armazenamento e dados aos seus clientes. Você pode saber isso como um *SVM* ou um *vserver*. O Cloud Volumes ONTAP é configurado com uma VM de storage por padrão, mas algumas configurações oferecem suporte a VMs de storage adicionais.

Número suportado de VMs de storage

O Cloud Volumes ONTAP 9,7 dá suporte a várias VMs de storage na AWS com certas configurações e uma licença complementar. "Veja o número de VMs de storage compatíveis na AWS". Entre em Contato com sua equipe de conta para obter uma licença complementar da SVM.

Todas as outras configurações do Cloud Volumes ONTAP oferecem suporte a uma VM de storage de fornecimento de dados e a uma VM de storage de destino usada para recuperação de desastres. Você pode ativar a VM de storage de destino para acesso aos dados se houver uma interrupção na VM de storage de origem.

Uma VM de storage abrange todo o sistema Cloud Volumes ONTAP (par de HA ou nó único).

Criação de VMs de storage adicionais

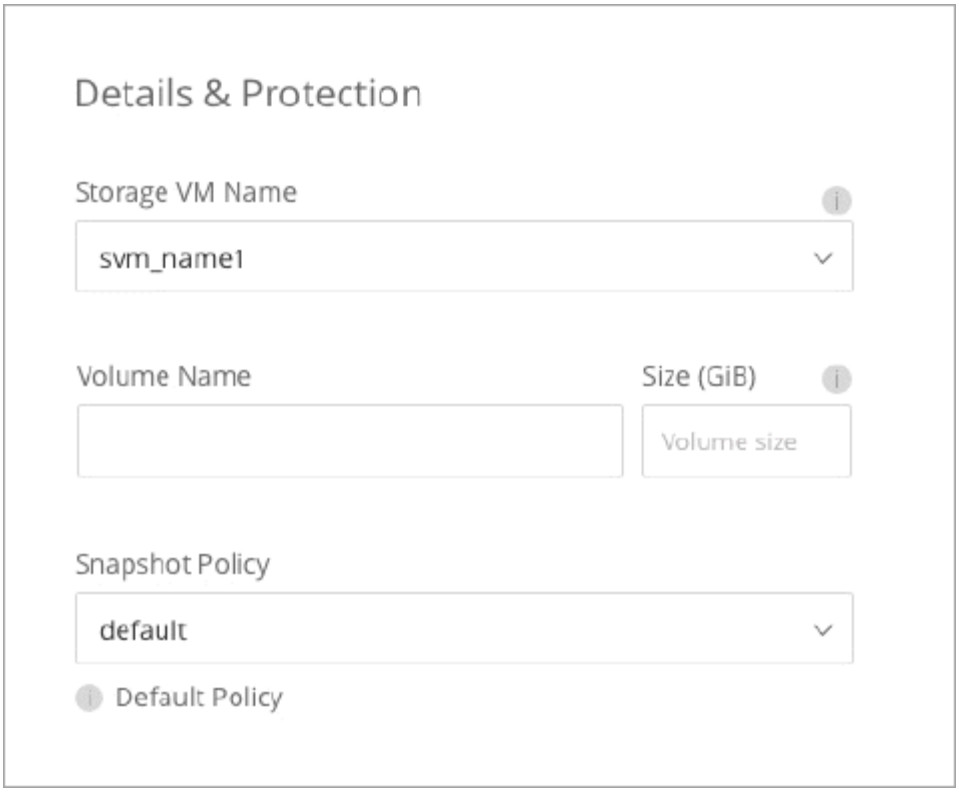
Se houver suporte na configuração, você poderá criar VMs de storage adicionais usando "System Manager ou CLI"o .

- "Criação de um SVM para acesso SMB"
- "Criação de um SVM para acesso ao NFS"
- "Criação de um SVM para acesso iSCSI"
- "Criação de um SVM de destino para recuperação de desastres"

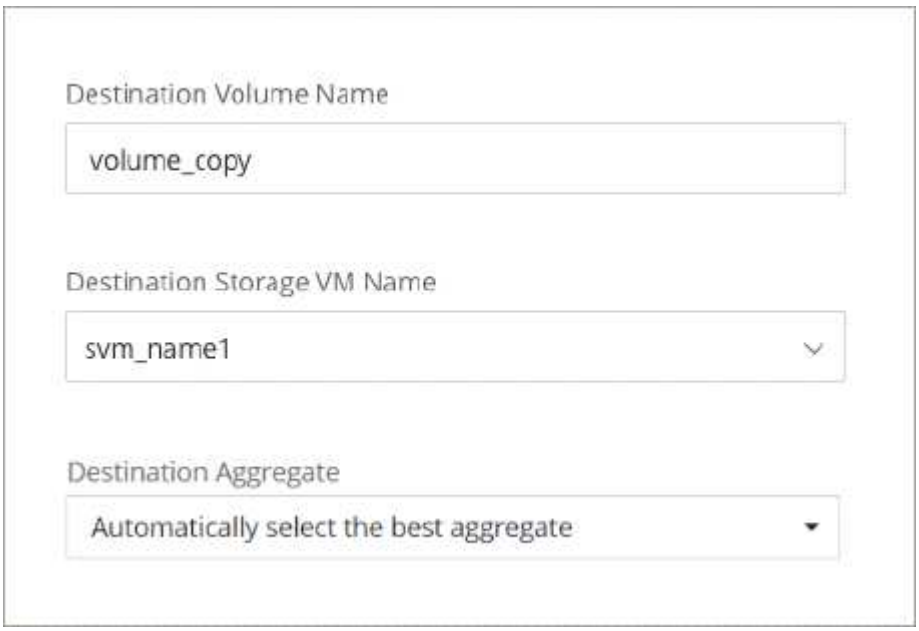
Trabalhando com várias VMs de storage no Cloud Manager

O Cloud Manager é compatível com quaisquer VMs de storage adicionais que você criar a partir do System Manager ou da CLI.

Por exemplo, a imagem a seguir mostra como você pode escolher uma VM de armazenamento ao criar um volume.



E a imagem a seguir mostra como você pode escolher uma VM de storage ao replicar um volume para outro sistema.



Gerenciamento da recuperação de desastres da VM de storage

O Cloud Manager não oferece suporte de configuração ou orquestração para recuperação de desastres de VM de storage. Você deve usar o System Manager ou a CLI.

- "Guia expresso de preparação para recuperação de desastres da SVM"
- "Guia do SVM Disaster Recovery Express"

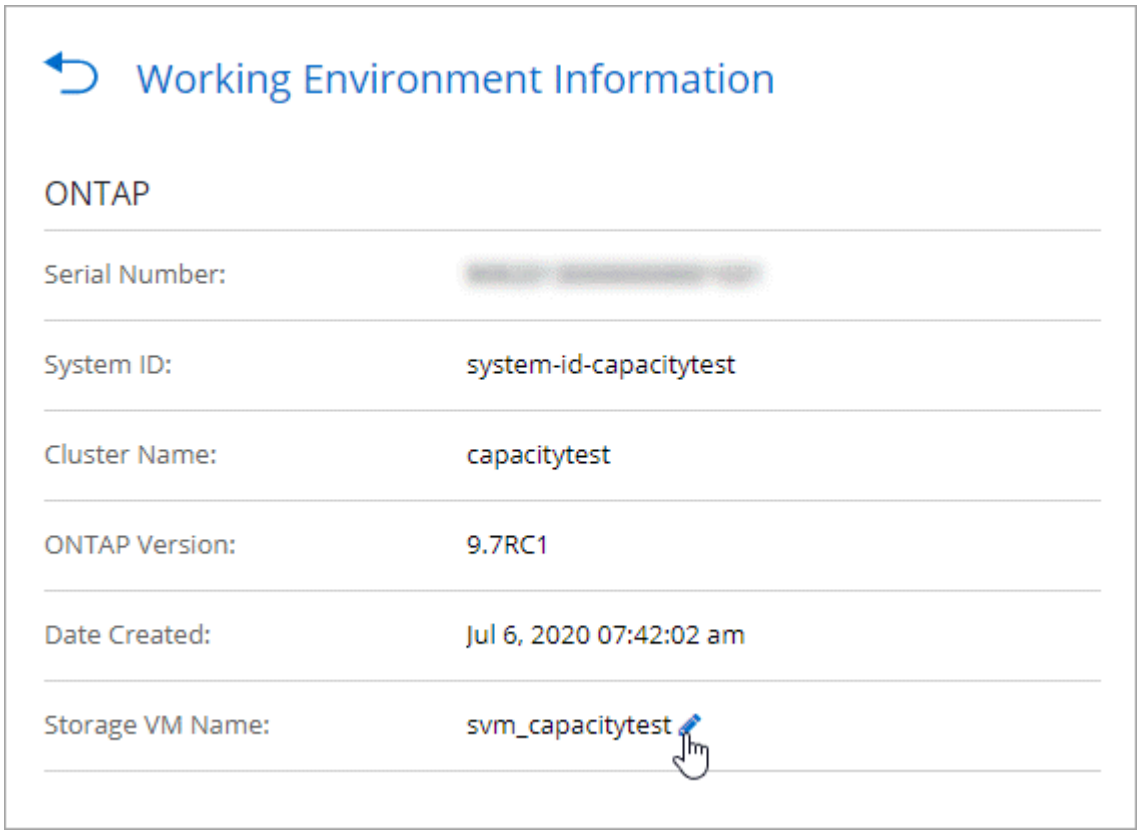
Modificação do nome da VM de armazenamento

O Cloud Manager nomeia automaticamente a única VM de storage que cria para o Cloud Volumes ONTAP. Você pode modificar o nome da VM de armazenamento se tiver padrões de nomenclatura rigorosos. Por exemplo, talvez você queira que o nome corresponda ao nome das VMs de storage dos clusters do ONTAP.

Se você criou quaisquer VMs de armazenamento adicionais para o Cloud Volumes ONTAP, não será possível renomear as VMs de armazenamento a partir do Cloud Manager. Você precisará fazer isso diretamente do Cloud Volumes ONTAP usando o Gerenciador de sistema ou a CLI.

Passos

1. No ambiente de trabalho, clique no ícone do menu e, em seguida, clique em **Informação**.
2. Clique no ícone de edição à direita do nome da VM de armazenamento.



3. Na caixa de diálogo Modificar Nome do SVM, altere o nome e clique em **Salvar**.

Usando o Cloud Volumes ONTAP como storage persistente para Kubernetes

O Cloud Manager pode automatizar a implantação do NetApp Trident nos clusters do Kubernetes. Assim, você pode usar o Cloud Volumes ONTAP como storage persistente para contêineres.

O Trident é um projeto de código aberto totalmente suportado mantido pela NetApp. O Trident é integrado nativamente ao Kubernetes e à estrutura de volume persistente para você provisionar e gerenciar volumes de sistemas que executam qualquer combinação de plataformas de storage do NetApp. "Saiba mais sobre o Trident".

O recurso Kubernetes não é compatível com clusters do ONTAP no local. É suportado apenas com Cloud Volumes ONTAP.

Início rápido

Comece rapidamente seguindo estas etapas ou role para baixo até as seções restantes para obter detalhes completos.

Reveja os pré-requisitos

Garanta que seu ambiente atenda aos pré-requisitos, o que inclui conectividade entre clusters do Kubernetes e o Cloud Volumes ONTAP, conectividade entre clusters do Kubernetes e um conetor, uma versão mínima do Kubernetes do 1,14, pelo menos um nó de trabalho em um cluster e muito mais. Veja a lista completa.

Adicione clusters de Kubernetes ao Cloud Manager

No Cloud Manager, clique em **Kubernetes** e descubra clusters diretamente do serviço gerenciado do seu provedor de nuvem ou importe um cluster fornecendo um arquivo kubeconfig.

Conecte os clusters ao Cloud Volumes ONTAP

Depois de adicionar um cluster Kubernetes, clique em **conetar ao ambiente de trabalho** para conetar o cluster a um ou mais sistemas Cloud Volumes ONTAP.

Inicie o provisionamento de volumes persistentes

Solicite e gerencie volumes persistentes usando interfaces e construções nativas do Kubernetes. O Cloud Manager cria classes de storage NFS e iSCSI que você pode usar ao provisionar volumes persistentes.

"Saiba mais sobre como provisionar seu primeiro volume com o Trident para Kubernetes".

Rever pré-requisitos

Antes de começar, verifique se os clusters e o conector Kubernetes atendem a requisitos específicos.

Requisitos de cluster do Kubernetes

- A conectividade de rede é necessária entre um cluster Kubernetes e o conector e entre um cluster Kubernetes e o Cloud Volumes ONTAP.

  O conetor e o Cloud Volumes ONTAP precisam de uma conexão com o ponto de extremidade da API do Kubernetes:

  - Para clusters gerenciados, configure uma rota entre a VPC de um cluster e a VPC onde o conetor e o Cloud Volumes ONTAP residem.
  - Para outros clusters, o endereço IP do nó principal ou do balanceador de carga (conforme listado no arquivo kubeconfig) deve ser acessível pelo conetor e pelo Cloud Volumes ONTAP, e deve apresentar

um certificado TLS válido.

- Um cluster do Kubernetes pode estar em qualquer local que tenha a conectividade de rede listada acima.
- Um cluster do Kubernetes deve estar executando a versão 1,14 no mínimo.

  A versão máxima suportada é definida pelo Trident. "Clique aqui para ver a versão do Kubernetes com suporte máximo".

- Um cluster do Kubernetes precisa ter pelo menos um nó de trabalho.
- Para clusters executados no Amazon Elastic Kubernetes Service (Amazon EKS), cada cluster precisa de uma função IAM adicionada para resolver um erro de permissões. Depois de adicionar o cluster, o Cloud Manager solicitará o comando eksctl exato que resolve o erro.

  "Saiba mais sobre os limites de permissões do IAM".

- Para clusters executados no Azure Kubernetes Service (AKS), esses clusters devem receber a função *Azure Kubernetes Service RBAC Cluster Admin*. Isso é necessário para que o Cloud Manager possa instalar o Trident e configurar classes de armazenamento no cluster.
- Para clusters executados no Google Kubernetes Engine (GKE), esses clusters não devem usar o sistema operacional otimizado por contêiner padrão. Você deve trocá-los para usar o Ubuntu.

  O GKE usa o Google por padrão "imagem otimizada para contentor", que não tem os utilitários que o Trident precisa para montar volumes.

Requisitos do conetor

Certifique-se de que a rede e as permissões a seguir estão em vigor para o conetor.

Rede

- O conetor precisa de uma conexão de saída à Internet para acessar os seguintes pontos finais ao instalar o Trident:

  https://packages.cloud.google.com/yum https://github.com/NetApp/Trident/Releases/download/

  O Cloud Manager instala o Trident em um cluster do Kubernetes quando você conecta um ambiente de trabalho ao cluster.

Permissões necessárias para descobrir e gerenciar clusters do EKS

O conetor precisa de permissões de administrador para descobrir e gerenciar clusters do Kubernetes executados no Amazon Elastic Kubernetes Service (EKS):

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "eks:*",
            "Resource": "*"
        }
    ]
}
```

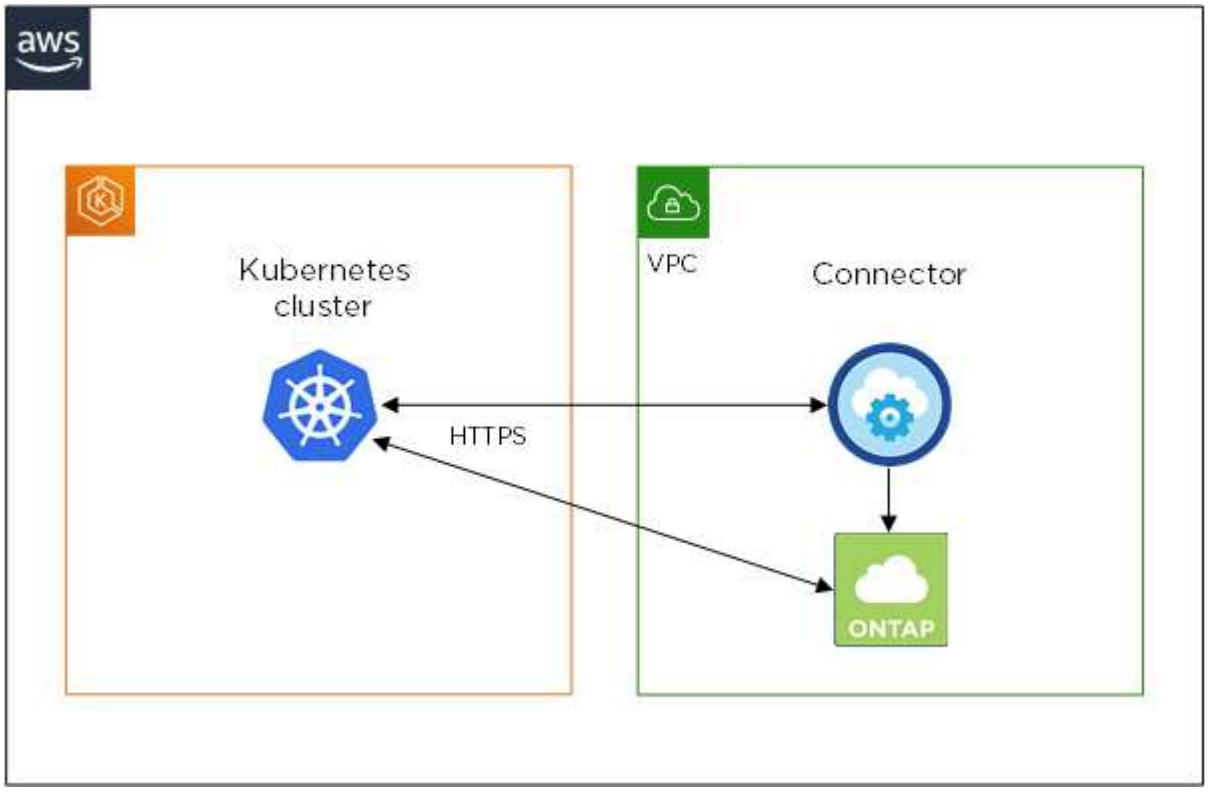
Permissões necessárias para descobrir e gerenciar clusters GKE

O conetor precisa das permissões a seguir para descobrir e gerenciar clusters do Kubernetes executados no Google Kubernetes Engine (GKE):

```
container.*
```

Exemplo de configuração

A imagem a seguir mostra um exemplo de um cluster do Kubernetes em execução no Amazon Elastic Kubernetes Service (Amazon EKS) e suas conexões ao Connector e ao Cloud Volumes ONTAP.



Adição de clusters de Kubernetes

Adicione clusters do Kubernetes ao Cloud Manager descobrindo os clusters executados no serviço Kubernetes gerenciado do seu provedor de nuvem ou importando o arquivo kubeconfig de um cluster.

Passos

1. Na parte superior do Cloud Manager, clique em **Kubernetes**.
2. Clique em **Add Cluster**.
3. Escolha uma das opções disponíveis:
   - Clique em **Discover clusters** para descobrir os clusters gerenciados aos quais o Cloud Manager tem acesso com base nas permissões fornecidas ao conetor.

     Por exemplo, se o conetor estiver em execução no Google Cloud, o Cloud Manager usará as permissões da conta de serviço do conetor para descobrir clusters executados no Google Kubernetes Engine (GKE).

   - Clique em **Import Cluster** para importar um cluster usando um arquivo kubeconfig.

     Depois de fazer o upload do arquivo, o Cloud Manager verifica a conetividade ao cluster e salva uma cópia criptografada do arquivo kubeconfig.

Resultado

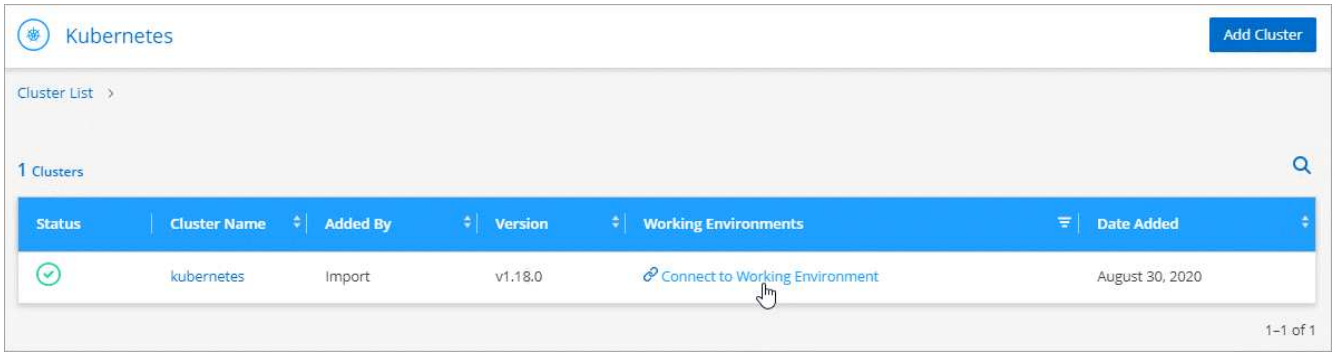
O Cloud Manager adiciona o cluster do Kubernetes. Agora você pode conetar o cluster ao Cloud Volumes ONTAP.

Conetando um cluster ao Cloud Volumes ONTAP

Conecte um cluster do Kubernetes ao Cloud Volumes ONTAP para que você possa usar o Cloud Volumes ONTAP como storage persistente para contêineres.

Passos

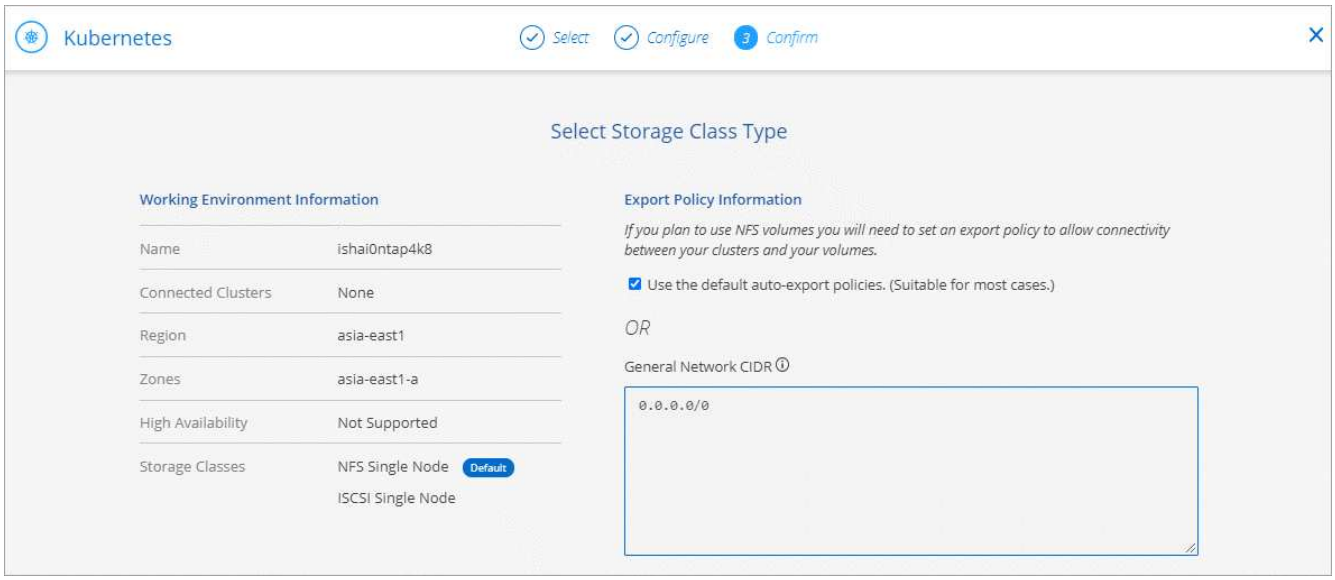
1. Na parte superior do Cloud Manager, clique em **Kubernetes**.
2. Clique em **conetar ao ambiente de trabalho** para o cluster que você acabou de adicionar.



3. Selecione um ambiente de trabalho e clique em **continuar**.
4. Escolha a classe de armazenamento NetApp a ser usada como a classe de armazenamento padrão para o cluster Kubernetes e clique em **continuar**.

   Quando um usuário cria um volume persistente, o cluster do Kubernetes pode usar essa classe de storage como storage de back-end por padrão.

5. Escolha se deseja usar políticas de exportação automática padrão ou se deseja adicionar um bloco CIDR personalizado.



6. Clique em **Adicionar ambiente de trabalho**.

Resultado

O Cloud Manager conecta o ambiente de trabalho ao cluster, o que pode levar até 15 minutos.

Gerenciamento dos clusters

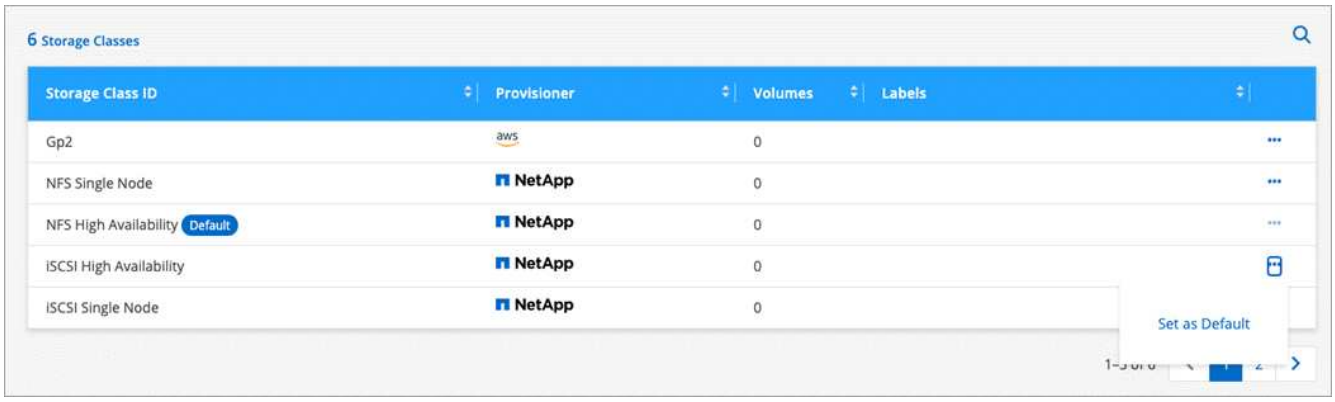
O Cloud Manager permite gerenciar clusters do Kubernetes alterando a classe de storage padrão, atualizando o Trident e muito mais.

Alterar a classe de armazenamento padrão

Certifique-se de definir uma classe de storage do Cloud Volumes ONTAP como a classe de storage padrão para que os clusters usem o Cloud Volumes ONTAP como o storage de back-end.

Passos

1. Na parte superior do Cloud Manager, clique em **Kubernetes**.
2. Clique no nome do cluster do Kubernetes.
3. Na tabela **Storage classes**, clique no menu ações na extrema direita da classe de armazenamento que você deseja definir como padrão.



4. Clique em **Definir como padrão**.

Atualizando o Trident

Você pode atualizar o Trident do Cloud Manager quando uma nova versão do Trident estiver disponível.

Passos

1. Na parte superior do Cloud Manager, clique em **Kubernetes**.
2. Clique no nome do cluster do Kubernetes.
3. Se uma nova versão estiver disponível, clique em **Atualizar** ao lado da versão Trident.

Atualizando o arquivo kubeconfig

Se você tiver adicionado seu cluster ao Cloud Manager importando o arquivo kubeconfig, poderá fazer o upload do arquivo kubeconfig mais recente para o Cloud Manager a qualquer momento. Você pode fazer isso se tiver atualizado as credenciais, se tiver alterado usuários ou funções ou se algo alterado que afete o cluster, usuário, namespaces ou autenticação.

Passos

1. Na parte superior do Cloud Manager, clique em **Kubernetes**.
2. Clique no nome do cluster do Kubernetes.
3. Clique em **Atualizar Kubeconfig**.
4. Quando solicitado através do navegador da Web, selecione o arquivo kubeconfig atualizado e clique em **Open**.

Resultado

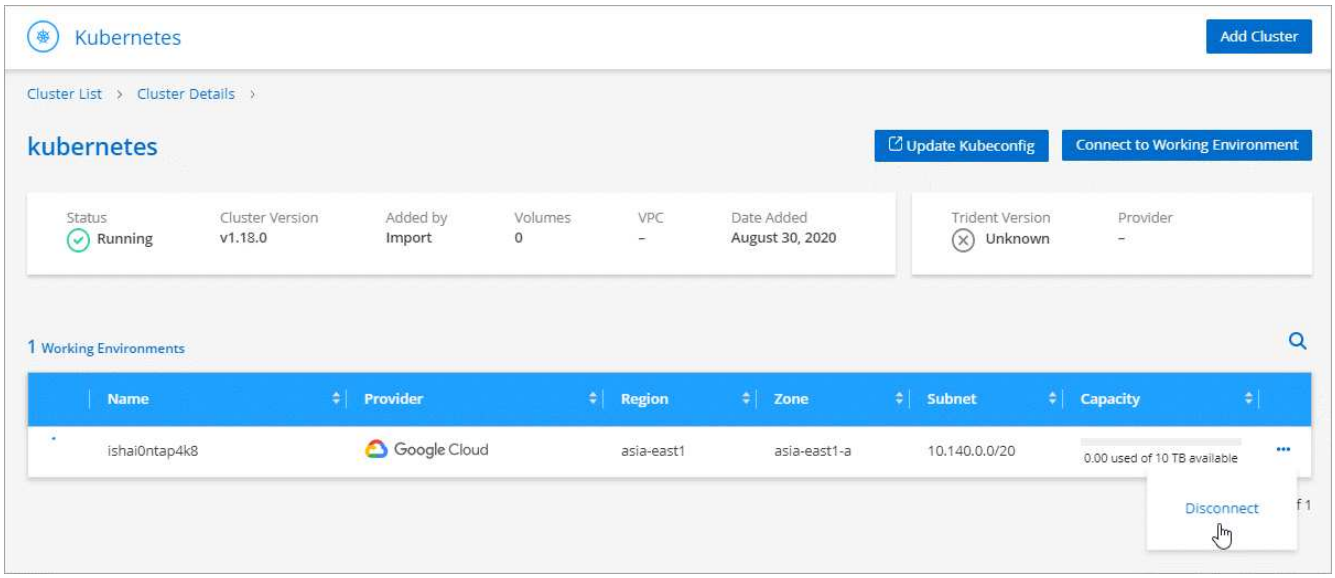
O Cloud Manager atualiza informações sobre o cluster do Kubernetes com base no arquivo kubeconfig mais recente.

Desligar um painel de instrumentos

Quando você desconeta um cluster do Cloud Volumes ONTAP, não pode mais usar esse sistema Cloud Volumes ONTAP como storage persistente para contêineres. Os volumes persistentes existentes não são excluídos.

Passos

1. Na parte superior do Cloud Manager, clique em **Kubernetes**.
2. Clique no nome do cluster do Kubernetes.
3. Na tabela **ambientes de trabalho**, clique no menu ações na extrema direita do ambiente de trabalho que você deseja desconetar.



4. Clique em **Disconnect**.

Resultado

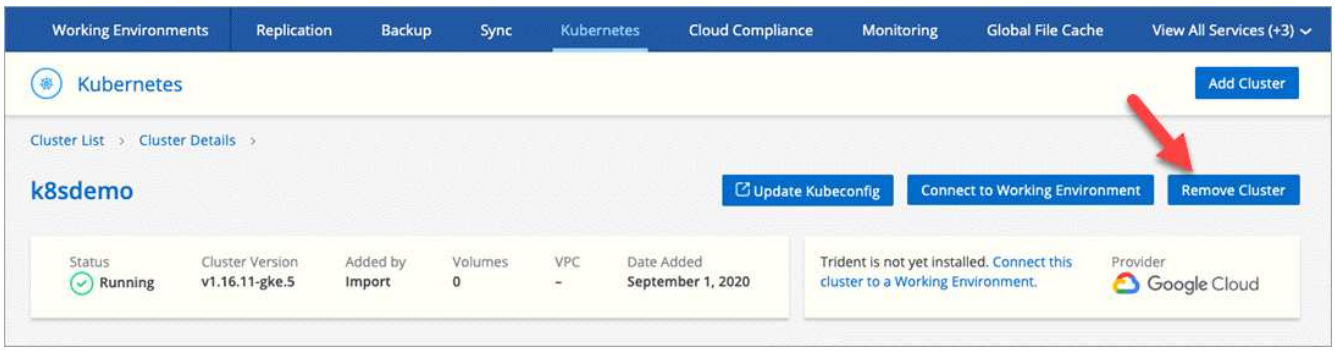
O Cloud Manager desconeta o cluster do sistema Cloud Volumes ONTAP.

Remover um cluster

Remova clusters desativados do Cloud Manager depois de desconetar todos os ambientes de trabalho do cluster.

Passos

1. Na parte superior do Cloud Manager, clique em **Kubernetes**.
2. Clique no nome do cluster do Kubernetes.
3. Clique em **Remove Cluster**.



Criptografando volumes com soluções de criptografia NetApp

O Cloud Volumes ONTAP é compatível com criptografia de volume NetApp (NVE) e criptografia agregada NetApp (NAE) com um gerenciador de chaves externo. NVE e NAE são soluções baseadas em software que permitem a criptografia de volumes em repouso compatível com FIPS (140-2) em conformidade com dados em repouso de volumes. "Saiba mais sobre essas soluções de criptografia".

A partir do Cloud Volumes ONTAP 9,7, novos agregados terão NAE ativado por padrão depois de configurar um gerenciador de chaves externo. Novos volumes que não fazem parte de um agregado NAE terão o NVE ativado por padrão (por exemplo, se você tiver agregados existentes que foram criados antes de configurar um gerenciador de chaves externo).

O Cloud Volumes ONTAP não é compatível com o gerenciamento de chaves integrado.

O que você vai precisar

Seu sistema Cloud Volumes ONTAP deve ser registrado com o suporte da NetApp. A partir do Cloud Manager 3,7.1, uma licença de criptografia de volume do NetApp é instalada automaticamente em cada sistema Cloud Volumes ONTAP registrado no suporte do NetApp.

- "Adicionar contas do site de suporte da NetApp ao Cloud Manager"
- "Registar sistemas de pagamento conforme o uso"

O Cloud Manager não instala a licença NVE em sistemas que residem na região da China.

Passos

1. Reveja a lista de gestores-chave suportados no "Ferramenta de Matriz de interoperabilidade do NetApp".

   Procure a solução **Key Managers**.

2. "Conete-se à CLI do Cloud Volumes ONTAP".
3. Instale certificados SSL e conete-se aos servidores externos de gerenciamento de chaves.

   "Guia de alimentação de criptografia ONTAP 9 NetApp: Configuração do gerenciamento de chaves externas"

Replicação de dados entre sistemas

É possível replicar dados entre ambientes de trabalho escolhendo uma replicação de dados única para transferência de dados ou uma programação recorrente para recuperação de desastres ou retenção de longo prazo. Por exemplo, você pode configurar a replicação de dados de um sistema ONTAP local para o Cloud Volumes ONTAP para recuperação de desastres.

O Cloud Manager simplifica a replicação de dados entre volumes em sistemas separados, usando as tecnologias SnapMirror e SnapVault. Basta identificar o volume de origem e o volume de destino e escolher uma política de replicação e uma programação. O Cloud Manager compra os discos necessários, configura relacionamentos, aplica a política de replicação e, em seguida, inicia a transferência de linha de base entre volumes.

A transferência da linha de base inclui uma cópia completa dos dados de origem. As transferências subsequentes contêm cópias diferenciais dos dados de origem.

O Cloud Manager permite a replicação de dados entre os seguintes tipos de ambientes de trabalho:

- De um sistema Cloud Volumes ONTAP para outro sistema Cloud Volumes ONTAP
- Entre um sistema Cloud Volumes ONTAP e um cluster ONTAP no local

- Desde um cluster ONTAP no local até outro cluster ONTAP no local

Requisitos de replicação de dados

Antes de replicar dados, confirme se os requisitos específicos são atendidos nos sistemas Cloud Volumes ONTAP e nos clusters do ONTAP.

Requisitos de versão

Você deve verificar se os volumes de origem e destino estão executando versões compatíveis do ONTAP antes de replicar dados. Para obter detalhes, consulte "Guia de alimentação de proteção de dados" .

Requisitos específicos do Cloud Volumes ONTAP

- O grupo de segurança da instância deve incluir as regras de entrada e saída necessárias: Especificamente, regras para ICMP e portas 11104 e 11105.

  Essas regras estão incluídas no grupo de segurança predefinido.

- Para replicar dados entre dois sistemas Cloud Volumes ONTAP em sub-redes diferentes, as sub-redes devem ser roteadas juntas (essa é a configuração padrão).
- Para replicar dados entre um sistema Cloud Volumes ONTAP na AWS e um sistema no Azure, você precisa ter uma conexão VPN entre a VPC AWS e o VNet do Azure.

Requisitos específicos dos clusters do ONTAP

- Uma licença SnapMirror ativa deve ser instalada.
- Se o cluster estiver em suas instalações, você deve ter uma conexão da rede corporativa para a AWS ou Azure, que normalmente é uma conexão VPN.
- Os clusters do ONTAP devem atender a requisitos adicionais de sub-rede, porta, firewall e cluster.

  Para obter detalhes, consulte o Guia expresso de peering de cluster e SVM para sua versão do ONTAP.

Configurando a replicação de dados entre sistemas

É possível replicar dados entre sistemas Cloud Volumes ONTAP e clusters do ONTAP escolhendo uma replicação de dados única, que pode ajudar você a migrar dados de e para a nuvem, ou uma programação recorrente que pode ajudar na recuperação de desastres ou retenção de longo prazo.

Sobre esta tarefa

O Cloud Manager é compatível com configurações de proteção de dados simples, de fanout e em cascata:

- Em uma configuração simples, a replicação ocorre do volume A ao volume B..
- Em uma configuração de fanout, a replicação ocorre do Volume A para vários destinos.
- Em uma configuração em cascata, a replicação ocorre do volume A para o volume B e do volume B para o volume C.

Você pode configurar configurações de fanout e cascata no Cloud Manager configurando várias replicações de dados entre sistemas. Por exemplo, replicando um volume do sistema A para o sistema B e replicando o mesmo volume do sistema B para o sistema C.

Passos

1. Na página ambientes de trabalho, selecione o ambiente de trabalho que contém o volume de origem e, em seguida, arraste-o para o ambiente de trabalho para o qual pretende replicar o volume:

2. Se as páginas de Configuração de peering de origem e destino forem exibidas, selecione todas as LIFs entre clusters para o relacionamento de pares de cluster.

   A rede entre clusters deve ser configurada de modo que os pares de cluster tenham *pair-wise full-mesh connectivity*, o que significa que cada par de clusters em um relacionamento de cluster peer tem conetividade entre todas as suas LIFs entre clusters.

   Essas páginas aparecem se um cluster ONTAP que tem várias LIFs for a origem ou o destino.

3. Na página seleção de volume de origem, selecione o volume que deseja replicar.
4. Na página Nome do volume de destino e disposição em categorias, especifique o nome do volume de destino, escolha um tipo de disco subjacente, altere qualquer uma das opções avançadas e clique em **continuar**.

   Se o destino for um cluster do ONTAP, você também deverá especificar o SVM de destino e o agregado.

5. Na página taxa máxima de transferência, especifique a taxa máxima (em megabytes por segundo) na qual os dados podem ser transferidos.
6. Na página Política de replicação, escolha uma das políticas padrão ou clique em **políticas adicionais** e selecione uma das políticas avançadas.

   Para obter ajuda, "Escolhendo uma política de replicação"consulte .

   Se você escolher uma política de backup personalizado (SnapVault), os rótulos associados à política deverão corresponder aos rótulos das cópias Snapshot no volume de origem. Para obter mais informações, "Como funcionam as políticas de backup"consulte .

7. Na página Agendar, escolha uma cópia única ou uma programação recorrente.

   Várias programações padrão estão disponíveis. Se você quiser uma programação diferente, você deve criar uma nova programação no cluster *destination* usando o System Manager.

8. Na página Revisão, revise suas seleções e clique em **ir**.

Resultado

O Cloud Manager inicia o processo de replicação de dados. Você pode exibir detalhes sobre a replicação na página Status da replicação.

Gerenciamento de cronogramas e relacionamentos de replicação de dados

Depois de configurar a replicação de dados entre dois sistemas, você poderá gerenciar o cronograma e o relacionamento de replicação de dados no Cloud Manager.

Passos

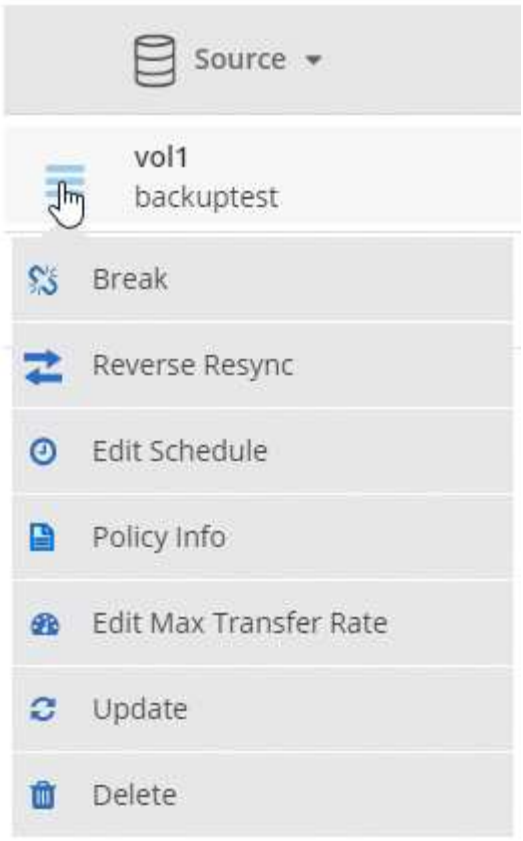
1. Na página ambientes de trabalho, exiba o status da replicação para todos os ambientes de trabalho no espaço de trabalho ou para um ambiente de trabalho específico:

Opção	Ação
Todos os ambientes de trabalho no espaço de trabalho	Na parte superior do Cloud Manager, clique em **replicação**.
Um ambiente de trabalho específico	Abra o ambiente de trabalho e clique em **replicações**.

2. Revise o status das relações de replicação de dados para verificar se elas estão íntegras.

> Se o Status de uma relação estiver ocioso e o Mirror State não for inicializado, você deverá inicializar a relação do sistema de destino para que a replicação de dados ocorra de acordo com a programação definida. Você pode inicializar o relacionamento usando o System Manager ou a interface de linha de comando (CLI). Esses estados podem aparecer quando o sistema de destino falha e, em seguida, volta online.

3. Selecione o ícone de menu ao lado do volume de origem e escolha uma das ações disponíveis.



A tabela a seguir descreve as ações disponíveis:

Ação	Descrição
Pausa	Quebra a relação entre os volumes de origem e destino e ativa o volume de destino para acesso aos dados. Essa opção é normalmente usada quando o volume de origem não pode servir dados devido a eventos como corrupção de dados, exclusão acidental ou um estado off-line. Para obter informações sobre como configurar um volume de destino para acesso a dados e reativar um volume de origem, consulte o Guia expresso de recuperação de desastres de volume do ONTAP 9.
Ressincronizar	Restabelece uma relação quebrada entre volumes e retoma a replicação de dados de acordo com a programação definida. Quando você ressincroniza os volumes, o conteúdo no volume de destino é substituído pelo conteúdo no volume de origem. Para executar uma ressincronização reversa, que ressincroniza os dados do volume de destino para o volume de origem, consulte o "Guia expresso de recuperação de desastres em volume do ONTAP 9".
Ressincronização reversa	Inverte as funções dos volumes de origem e destino. O conteúdo do volume de origem original é substituído pelo conteúdo do volume de destino. Isso é útil quando você deseja reativar um volume de origem que ficou offline. Quaisquer dados gravados no volume de origem original entre a última replicação de dados e a hora em que o volume de origem foi desativado não são preservados.

Ação	Descrição
Editar Agendamento	Permite escolher um agendamento diferente para replicação de dados.
Informações da política	Mostra a política de proteção atribuída à relação de replicação de dados.
Editar taxa de transferência máxima	Permite editar a taxa máxima (em kilobytes por segundo) na qual os dados podem ser transferidos.
Atualização	Inicia uma transferência incremental para atualizar o volume de destino.
Eliminar	Exclui a relação de proteção de dados entre os volumes de origem e destino, o que significa que a replicação de dados não ocorre mais entre os volumes. Esta ação não ativa o volume de destino para acesso aos dados. Essa ação também excluirá o relacionamento entre pares de cluster e o relacionamento entre pares de máquina virtual de armazenamento (SVM), se não houver outros relacionamentos de proteção de dados entre os sistemas.

Resultado

Depois de selecionar uma ação, o Cloud Manager atualiza a relação ou a programação.

Escolhendo uma política de replicação

Talvez você precise de ajuda para escolher uma política de replicação ao configurar a replicação de dados no Cloud Manager. Uma política de replicação define como o sistema de storage replica dados de um volume de origem para um volume de destino.

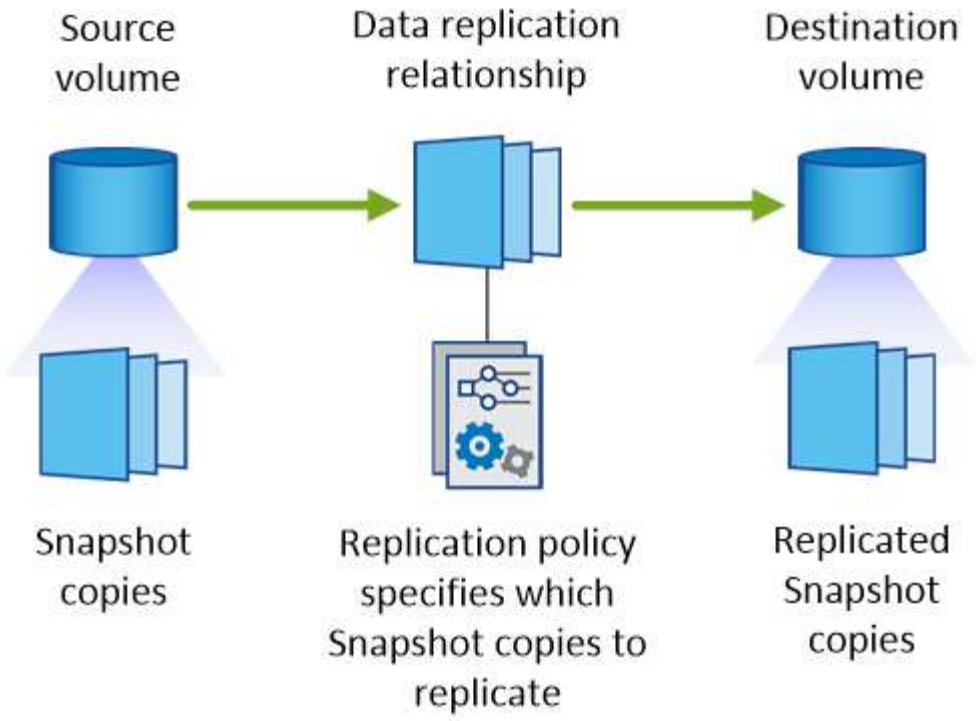
O que as políticas de replicação fazem

O sistema operacional ONTAP cria automaticamente backups chamados cópias Snapshot. Uma cópia Snapshot é uma imagem somente leitura de um volume que captura o estado do sistema de arquivos em um ponto no tempo.

Ao replicar dados entre sistemas, replica cópias Snapshot de um volume de origem para um volume de destino. Uma política de replicação especifica quais cópias Snapshot devem ser replicadas do volume de origem para o volume de destino.

As políticas de replicação também são chamadas de políticas *protection* porque são baseadas nas tecnologias SnapMirror e SnapVault, que fornecem proteção para recuperação de desastres e backup e recuperação de disco a disco.

A imagem a seguir mostra a relação entre cópias Snapshot e políticas de replicação:



Tipos de políticas de replicação

Existem três tipos de políticas de replicação:

- Uma política *Mirror* replica cópias Snapshot recém-criadas para um volume de destino.

  Use essas cópias Snapshot para proteger o volume de origem em preparação para a recuperação de desastres ou para replicação de dados única. Pode ativar o volume de destino para acesso aos dados a qualquer momento.

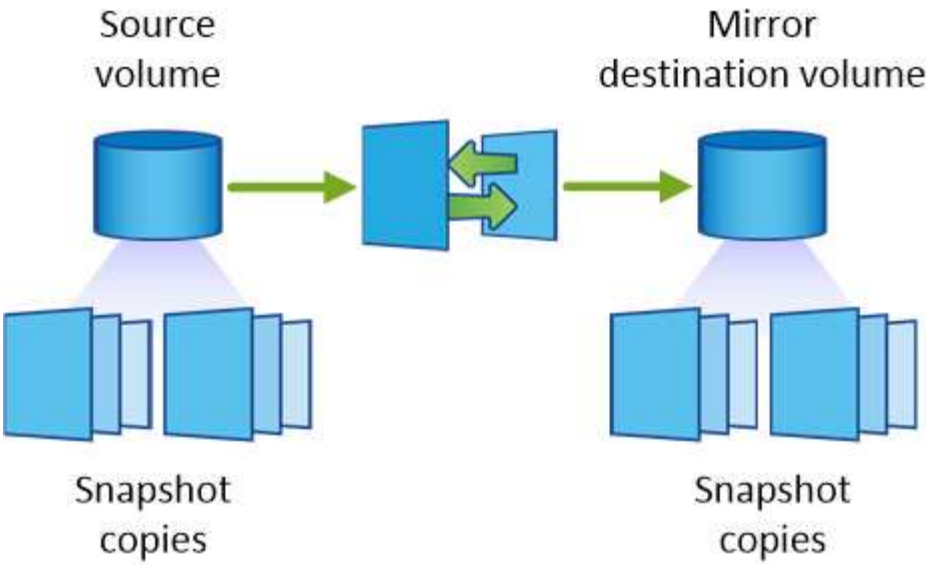
- Uma política de *Backup* replica cópias Snapshot específicas para um volume de destino e normalmente as retém por um período de tempo maior do que no volume de origem.

  Você pode restaurar os dados dessas cópias Snapshot quando os dados forem corrompidos ou perdidos e mantê-los para conformidade com os padrões e outros fins relacionados à governança.

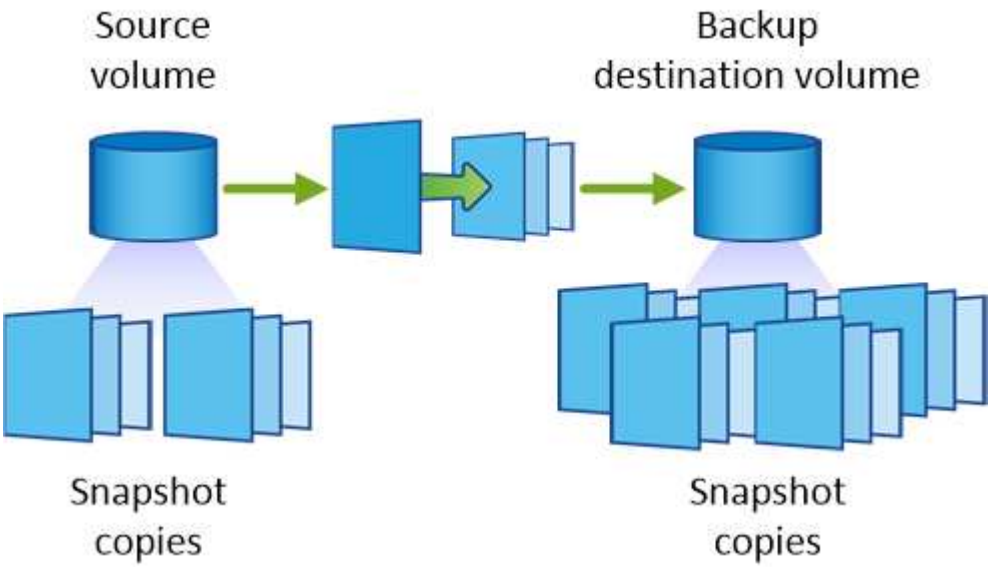
- Uma política *Mirror and Backup* fornece recuperação de desastres e retenção de longo prazo.

  Cada sistema inclui uma política de espelhamento e backup padrão, que funciona bem em muitas situações. Se você achar que precisa de políticas personalizadas, você pode criar suas próprias usando o System Manager.

As imagens a seguir mostram a diferença entre as políticas Mirror (espelho) e Backup (cópia de segurança). Uma política de espelhamento espelha as cópias Snapshot disponíveis no volume de origem.



Em geral, uma política de backup retém as cópias Snapshot por mais tempo do que as retidas no volume de origem:



Como as políticas de backup funcionam

Diferentemente das políticas de espelhamento, as políticas de backup (SnapVault) replicam cópias Snapshot específicas para um volume de destino. É importante entender como as políticas de backup funcionam se você quiser usar suas próprias políticas em vez das políticas padrão.

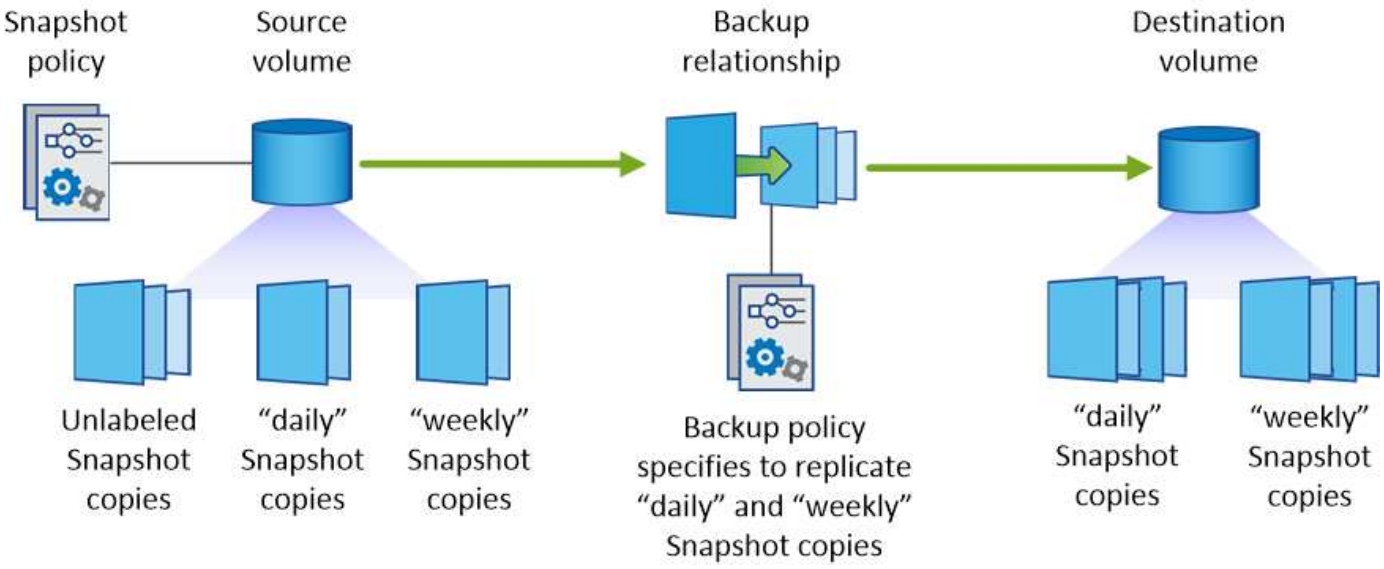
Entendendo a relação entre rótulos de cópia Snapshot e políticas de backup

Uma política do Snapshot define como o sistema cria cópias Snapshot de volumes. A política especifica quando criar as cópias Snapshot, quantas cópias devem ser mantidas e como rotulá-las. Por exemplo, um sistema pode criar uma cópia Snapshot todos os dias às 12:10 da manhã, manter as duas cópias mais recentes e rotulá-las "diariamente".

Uma política de backup inclui regras que especificam quais cópias Snapshot rotuladas para replicação em um volume de destino e quantas cópias devem reter. Os rótulos definidos em uma política de backup devem corresponder a um ou mais rótulos definidos em uma política de snapshot. Caso contrário, o sistema não

poderá replicar cópias Snapshot.

Por exemplo, uma política de backup que inclui os rótulos "diário" e "semanal" resulta na replicação de cópias Snapshot que incluem apenas esses rótulos. Nenhuma outra cópia Snapshot é replicada, como mostrado na imagem a seguir:



Políticas padrão e políticas personalizadas

A política padrão do Snapshot cria cópias Snapshot por hora, diárias e semanais, mantendo seis cópias por hora, duas por dia e duas por semana.

Você pode usar facilmente uma política de backup padrão com a política Snapshot padrão. As políticas de backup padrão replicam cópias Snapshot diárias e semanais, retendo sete cópias Snapshot diárias e 52 cópias Snapshot semanais.

Se você criar políticas personalizadas, os rótulos definidos por essas políticas devem corresponder. Você pode criar políticas personalizadas usando o System Manager.

Replicação de dados do NetApp HCI para o Cloud Volumes ONTAP

Se você estiver tentando replicar dados do NetApp HCI para o Cloud Volumes ONTAP, pode fazê-lo em um sistema NetApp HCI executando o software NetApp Element usando o SnapMirror. Como alternativa, você pode replicar dados em volumes criados em um sistema ONTAP Select executado como convidado virtual em uma solução da NetApp HCI para o Cloud Volumes ONTAP.

Consulte os seguintes relatórios técnicos para obter detalhes:

- "Relatório Técnico 4641: Proteção de dados NetApp HCI"
- "Relatório Técnico 4651: Arquitetura e Configuração do NetApp SolidFire SnapMirror"

Monitorar o desempenho

Saiba mais sobre o serviço de monitoramento

Ao utilizar o "Serviço NetApp Cloud Insights", o Cloud Manager fornece insights sobre a

integridade e o desempenho das instâncias do Cloud Volumes ONTAP e ajuda você a solucionar problemas e otimizar o desempenho do seu ambiente de storage de nuvem.

Caraterísticas

- Monitorar automaticamente todos os volumes
- Visualize os dados de performance de volume em termos de IOPS, taxa de transferência e latência
- Identifique problemas de desempenho para minimizar o impactos em seus usuários e aplicativos

Fornecedores de nuvem compatíveis

O serviço de monitoramento é compatível com o Cloud Volumes ONTAP para AWS.

Custo

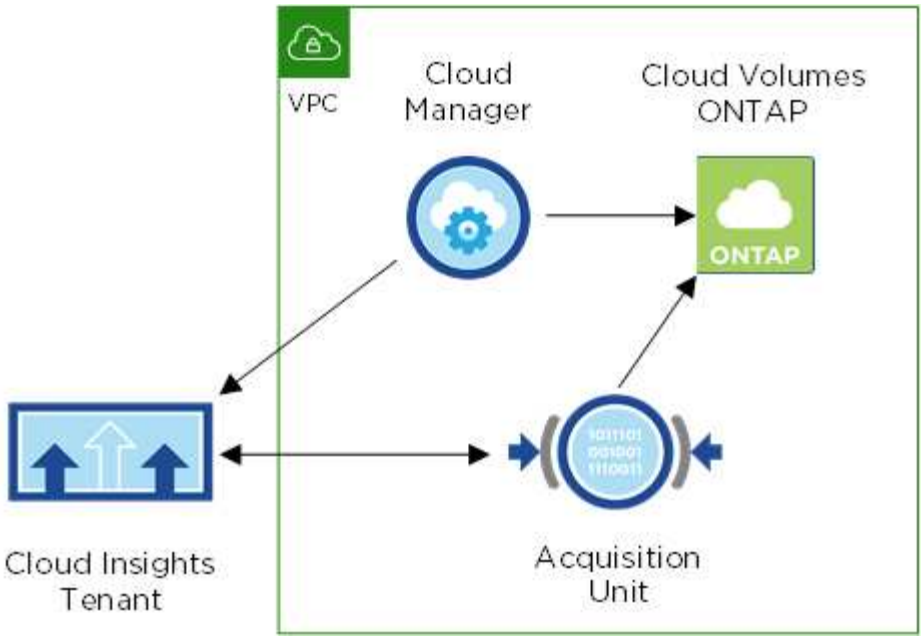
O monitoramento está disponível atualmente como uma visualização. A ativação é gratuita, mas o Cloud Manager inicia uma máquina virtual na VPC para facilitar o monitoramento. Essa VM resulta em cobranças do seu provedor de nuvem.

Como o Cloud Insights funciona com o Cloud Manager

Em um alto nível, a integração do Cloud Insights com o Cloud Manager funciona assim:

1. Você ativa o serviço de monitoramento no Cloud Volumes ONTAP.
2. O Cloud Manager configura seu ambiente. Ele faz o seguinte:
    a. Cria um locatário do Cloud Insights (também chamado de *ambiente*) e associa todos os usuários da sua conta do Cloud Central ao locatário.
    b. Permite uma avaliação gratuita de 30 dias do Cloud Insights.
    c. Implanta uma máquina virtual na VPC chamada Unidade de aquisição, o que facilita o monitoramento de volumes (essa é a VM mencionada na seção custo acima).
    d. Liga a unidade de aquisição ao Cloud Volumes ONTAP e ao locatário do Cloud Insights.
3. No Cloud Manager, você clica em Monitoramento e usa os dados de performance para solucionar problemas e otimizar a performance.

A imagem seguinte mostra a relação entre estes componentes:



A Unidade de aquisição

Quando você ativa o Monitoramento, o Cloud Manager implanta uma Unidade de aquisição na mesma sub-rede que o conetor.

Uma *Unidade de aquisição* coleta dados de desempenho do Cloud Volumes ONTAP e os envia ao locatário do Cloud Insights. Em seguida, o Cloud Manager consulta esses dados e os apresenta a você.

Observe o seguinte sobre a instância da Unidade de aquisição:

- A Unidade de aquisição é executada em uma instância T3.xlarge com um volume GP2 de 100 GB.
- A instância é chamada *AcquisitionUnit* com um hash gerado (UUID) concatenado a ela. Por exemplo: *AcquisitionUnit-FAN7FqeH*
- Apenas uma unidade de aquisição é ativada por conetor.
- A instância deve estar em execução para acessar informações de desempenho na guia Monitoramento.

Locatário da Cloud Insights

O Cloud Manager configura um *locatário* para você quando você ativa o monitoramento. Um locatário do Cloud Insights permite-lhe aceder aos dados de desempenho que a Unidade de aquisição recolhe. O locatário é uma partição de dados segura dentro do serviço NetApp Cloud Insights.

Interface Web do Cloud Insights

A guia Monitoramento do Cloud Manager fornece dados básicos de performance para seus volumes. Você pode ir para a interface da Web do Cloud Insights a partir do seu navegador para executar um monitoramento mais detalhado e configurar alertas para seus sistemas Cloud Volumes ONTAP.

Avaliação gratuita e assinatura

O Cloud Manager permite uma avaliação gratuita de 30 dias do Cloud Insights para fornecer dados de desempenho no Cloud Manager e para você explorar os recursos que o Cloud Insights Standard Edition tem a oferecer.

Você precisa se inscrever até o final da avaliação gratuita ou seu locatário do Cloud Insights será excluído. Você pode se inscrever na edição básica, padrão ou Premium para continuar usando o recurso de monitoramento no Cloud Manager.

"Saiba como se inscrever no Cloud Insights".

Monitorando o Cloud Volumes ONTAP na AWS

Execute algumas etapas para começar a monitorar o desempenho do Cloud Volumes ONTAP.

Início rápido

Comece rapidamente seguindo estas etapas ou role para baixo até as seções restantes para obter detalhes completos.

Verifique o suporte para sua configuração

Você precisa de uma nova instalação do Cloud Manager 3.8.4 ou posterior na AWS, Cloud Volumes ONTAP na AWS, e você precisa ser um novo cliente do Cloud Insights.

Ative a monitorização no seu sistema novo ou existente

- Novos ambientes de trabalho: Certifique-se de manter o Monitoramento ativado quando você cria o ambiente de trabalho (ele está habilitado por padrão).
- Ambientes de trabalho existentes: Selecione um ambiente de trabalho e clique em **Start Monitoring**.

Visualizar dados de desempenho

Clique em **Monitoramento** e veja os dados de desempenho dos seus volumes.

Inscreva-se no Cloud Insights

Inscreva-se antes que sua avaliação gratuita de 30 dias termine para continuar vendo dados de desempenho no Cloud Manager e no Cloud Insights. "Saiba como se inscrever".

Requisitos

Leia os seguintes requisitos para se certificar de que tem uma configuração suportada.

Versões compatíveis do Cloud Manager

Você precisa de uma nova instalação do Cloud Manager 3.8.4 ou posterior. Uma nova instalação é necessária porque uma nova infraestrutura é necessária para habilitar o serviço de monitoramento. Essa infraestrutura está disponível a partir de novas instalações do Cloud Manager 3,8.4.

Versões suportadas do Cloud Volumes ONTAP

Qualquer versão do Cloud Volumes ONTAP na AWS.

Requisito Cloud Insights

Você deve ser um novo cliente da Cloud Insights. O monitoramento não é suportado se você já tiver um locatário do Cloud Insights.

Endereço de e-mail do Cloud Central

O endereço de e-mail da sua conta de usuário do Cloud Central deve ser o endereço de e-mail da sua empresa. Domínios de e-mail gratuitos como gmail e hotmail não são suportados ao criar um locatário do Cloud Insights.

Rede para a unidade de aquisição

A Unidade de aquisição usa autenticação de 2 vias/mútua para se conetar ao servidor Cloud Insights. O certificado de cliente deve ser passado para o servidor Cloud Insights para ser autenticado. Para fazer isso, o proxy deve ser configurado para encaminhar a solicitação http para o servidor Cloud Insights sem descriptografar os dados.

A Unidade de aquisição usa os dois pontos finais a seguir para se comunicar com o Cloud Insights. Se você tiver um firewall entre o servidor da Unidade de aquisição e o Cloud Insights, precisará desses endpoints ao configurar regras de firewall:

```
https://aulogin.<Cloud Insights Domain>
https://<your-tenant-ID>.<Cloud Insights Domain>
```

Por exemplo:

```
https://aulogin.c01.cloudinsights.netapp.com
https://cg0c586a-ee05-45rb-a5ac-
333b5ae7718d7.c01.cloudinsights.netapp.com
```

Entre em Contato conosco através do chat no produto se precisar de ajuda para identificar seu domínio Cloud Insights e ID do locatário.

Rede para o conetor

Semelhante à Unidade de aquisição, o conetor deve ter conetividade de saída ao locatário do Cloud Insights. Mas o ponto final que o conetor entra em Contato é um pouco diferente. Ele entra em Contato com o URL do host do locatário usando o ID do locatário encurtado:

```
 https://<your-short-tenant-ID>.<Cloud Insights Domain>
Por exemplo:
```

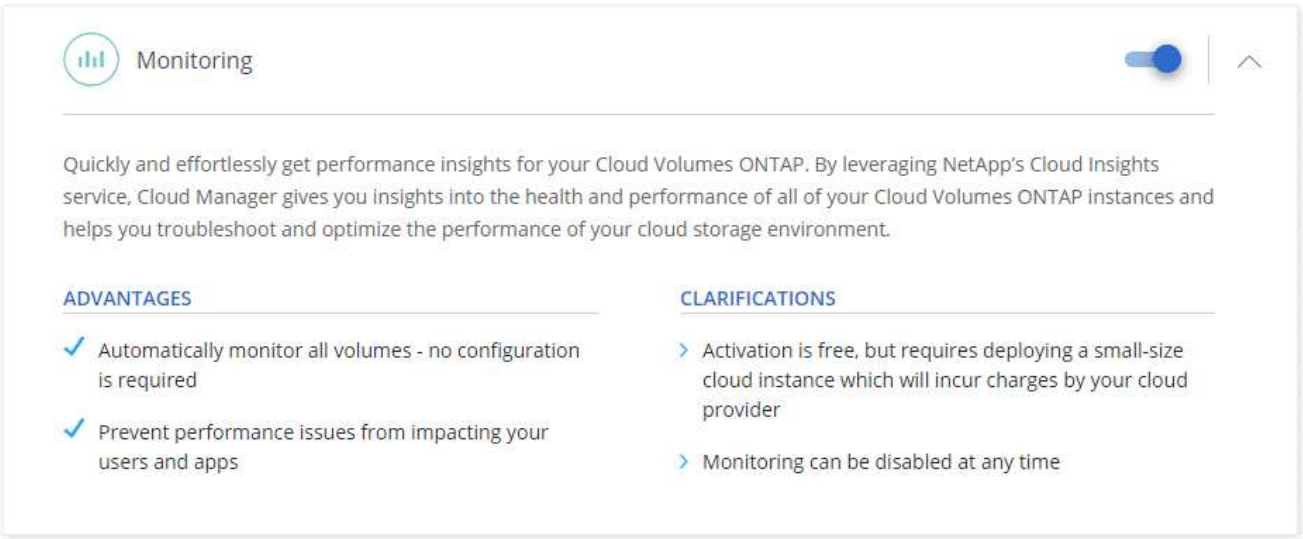
```
 https://abcd12345.c01.cloudinsights.netapp.com
Novamente, você pode entrar em Contato conosco através do chat no
produto se precisar de ajuda para identificar o URL do host do
locatário.
```

Ativar a monitorização num novo sistema

O serviço de monitorização é ativado por predefinição no assistente do ambiente de trabalho. Certifique-se de que mantém a opção ativada.

Passos

1. Clique em **Create Cloud Volumes ONTAP**.
2. Selecione Amazon Web Services como provedor de nuvem e escolha um único nó ou sistema de HA.
3. Preencha a página Detalhes e credenciais.
4. Na página Serviços, deixe o serviço ativado e clique em **continuar**.

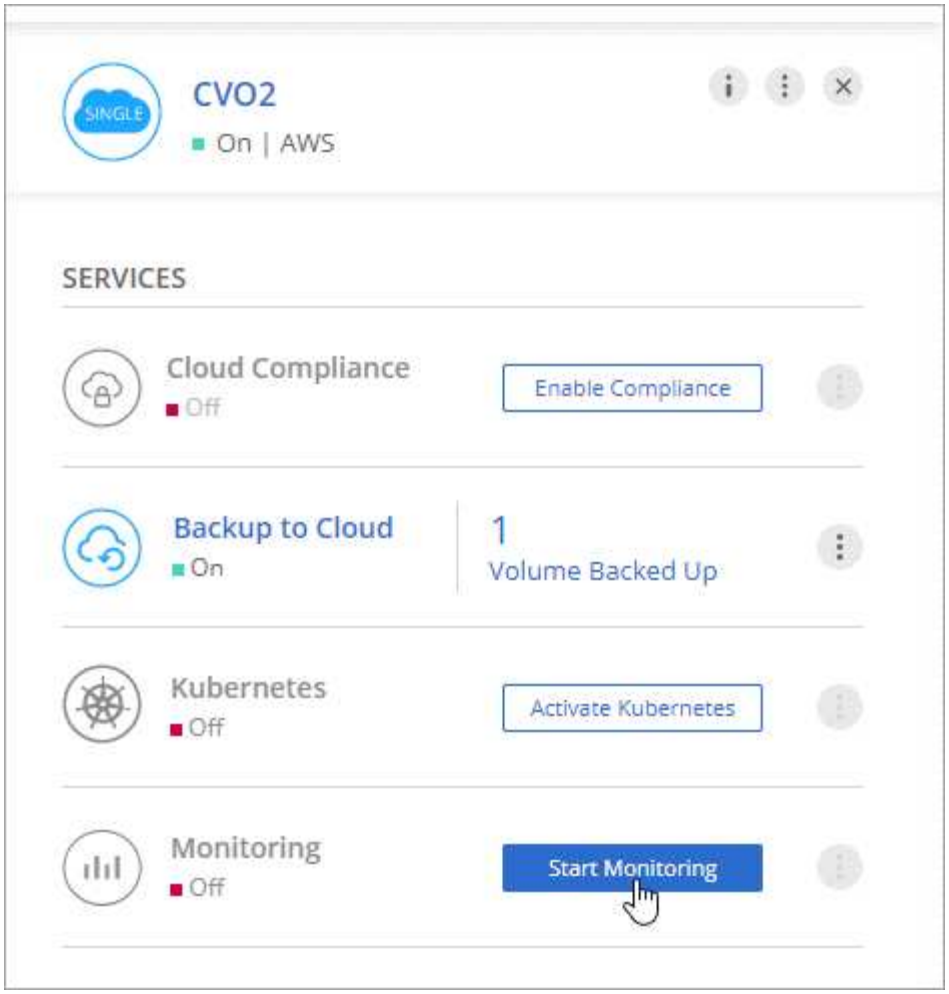


Ativar a monitorização num sistema existente

Ativar a monitorização a qualquer momento a partir do ambiente de trabalho.

Passos

1. Na parte superior do Cloud Manager, clique em **ambientes de trabalho**.
2. Selecione um ambiente de trabalho.
3. No painel à direita, clique em **Iniciar monitoramento**.



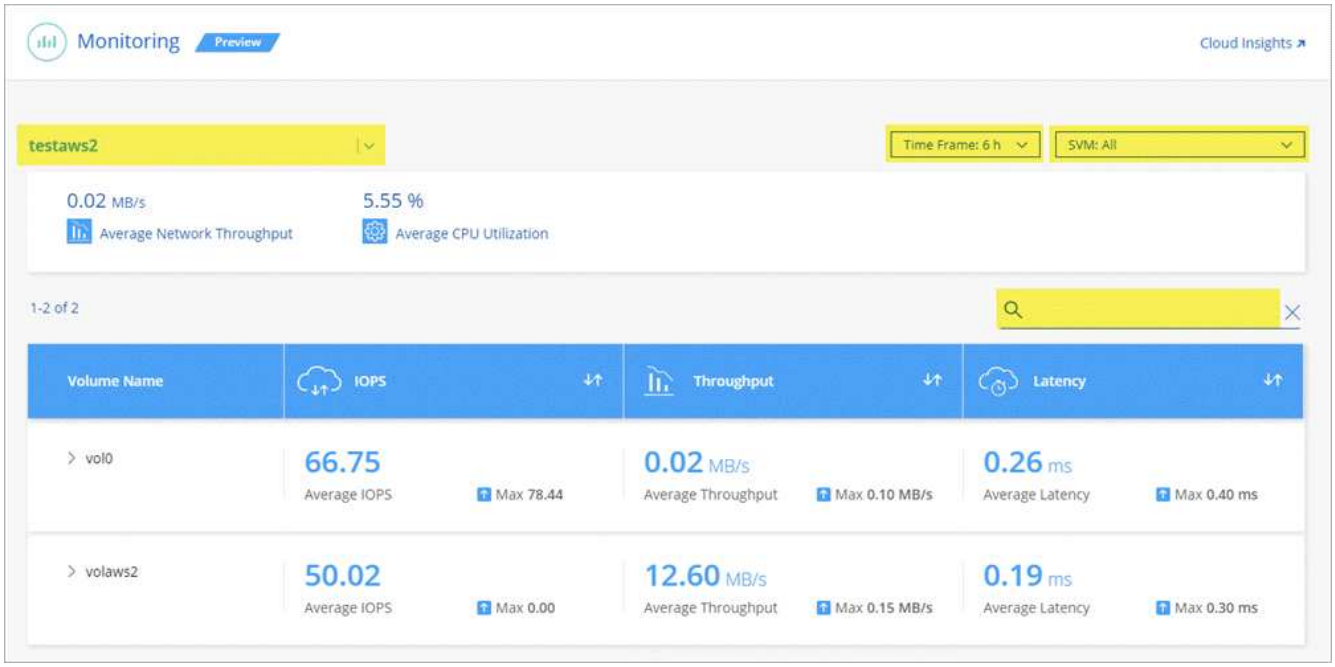
Monitorando seus volumes

Monitore a performance visualizando IOPS, taxa de transferência e latência de cada um dos volumes.

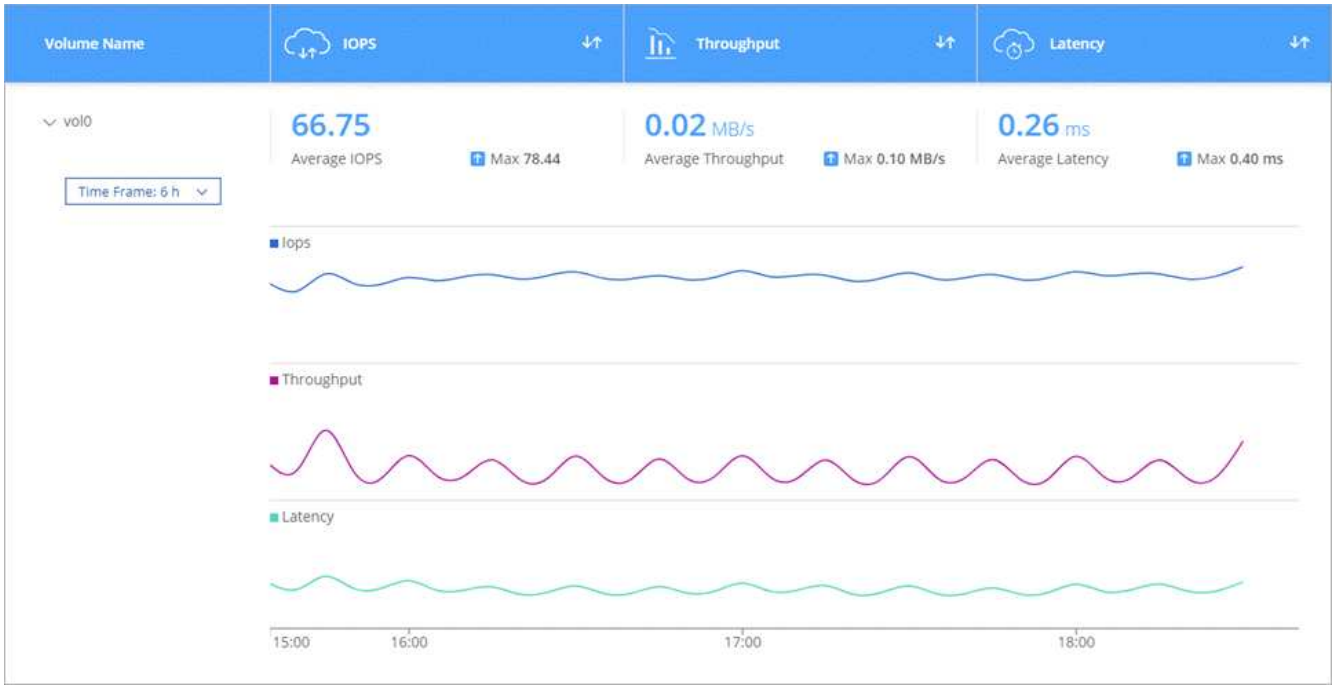
Passos

1. Na parte superior do Cloud Manager, clique em **Monitoramento**.
2. Filtre o conteúdo do painel para obter as informações de que você precisa.
   - Selecione um ambiente de trabalho específico.
   - Selecione um período de tempo diferente.
   - Selecione uma SVM específica.
   - Procure um volume específico.

   A imagem a seguir destaca cada uma destas opções:



3. Clique em um volume na tabela para expandir a linha e exibir uma linha do tempo para IOPS, taxa de transferência e latência.



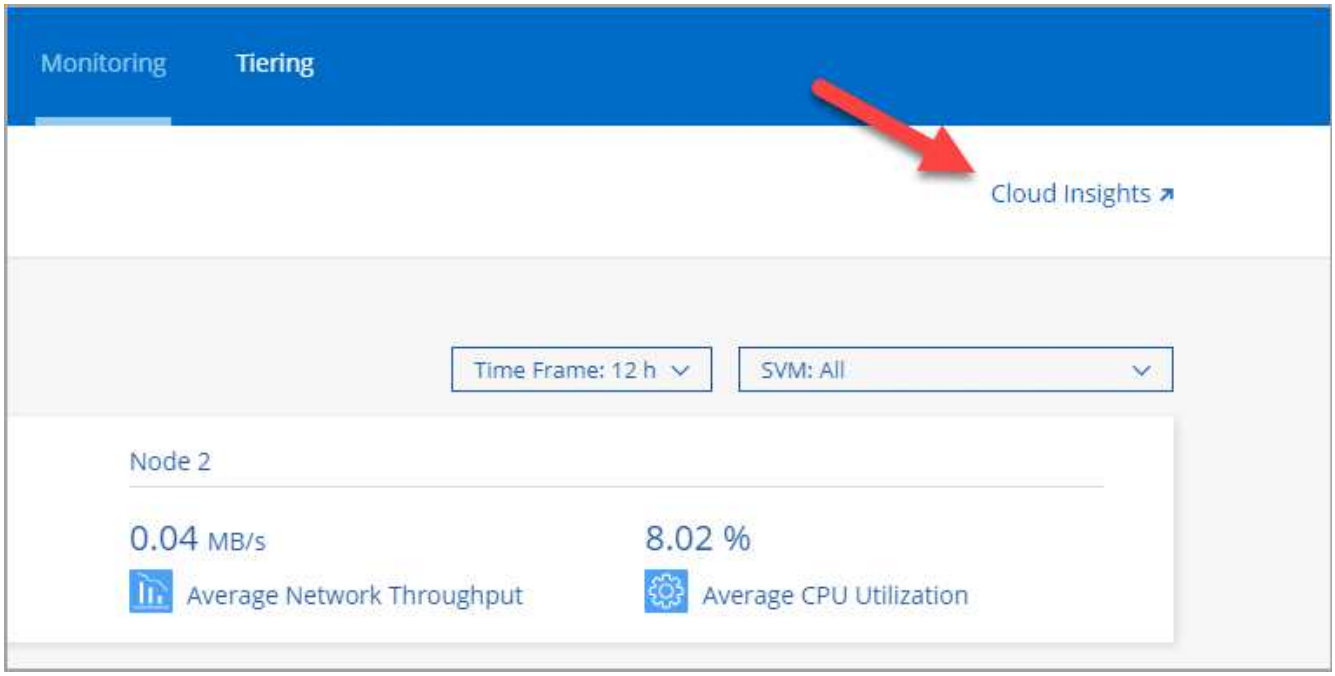
4. Use os dados para identificar problemas de desempenho para minimizar o impactos nos usuários e aplicativos.

Obter mais informações do Cloud Insights

A guia Monitoramento do Cloud Manager fornece dados básicos de performance para seus volumes. Você pode ir para a interface da Web do Cloud Insights a partir do seu navegador para executar um monitoramento mais detalhado e configurar alertas para seus sistemas Cloud Volumes ONTAP.

Passos

1. Na parte superior do Cloud Manager, clique em **Monitoramento**.
2. Clique no link **Cloud Insights**.



Resultado

Cloud Insights abrir em uma nova guia do navegador. Se precisar de ajuda, consulte o "Documentação do Cloud Insights".

Desativação da monitorização

Se você não quiser mais monitorar o Cloud Volumes ONTAP, você pode desativar o serviço a qualquer momento.

Se você desativar o monitoramento de cada um de seus ambientes de trabalho, precisará excluir a instância do EC2 sozinho. A instância é chamada *AcquisitionUnit* com um hash gerado (UUID) concatenado a ela. Por exemplo: *AcquisitionUnit-FAN7FqeH*

Passos

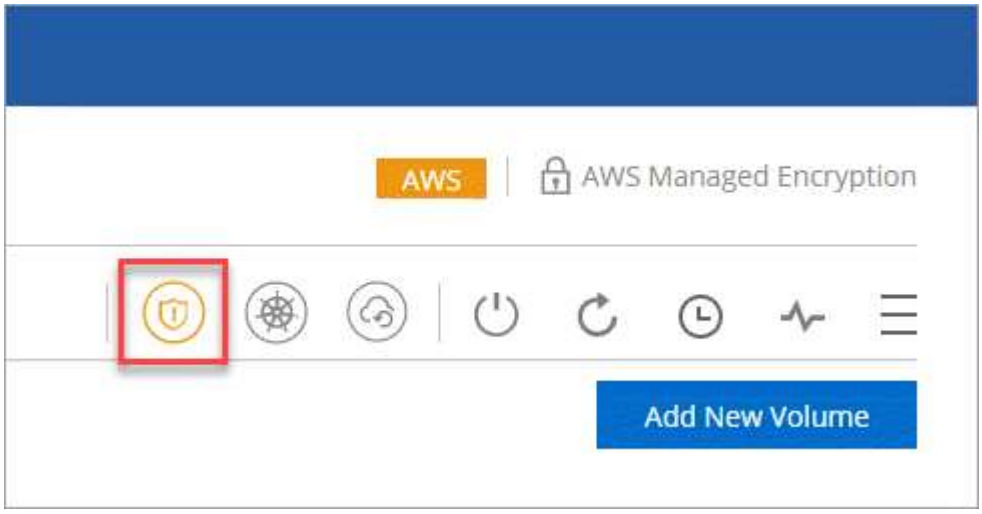
1. Na parte superior do Cloud Manager, clique em **ambientes de trabalho**.
2. Selecione um ambiente de trabalho.
3. No painel à direita, clique no ícone e selecione **Desativar digitalização**.

Aumento da proteção contra ransomware

Os ataques de ransomware podem custar tempo, recursos e reputação aos negócios. Com o Cloud Manager, você implementa a solução NetApp para ransomware, que fornece ferramentas eficazes de visibilidade, detecção e correção.

Passos

1. No ambiente de trabalho, clique no ícone **ransomware**.

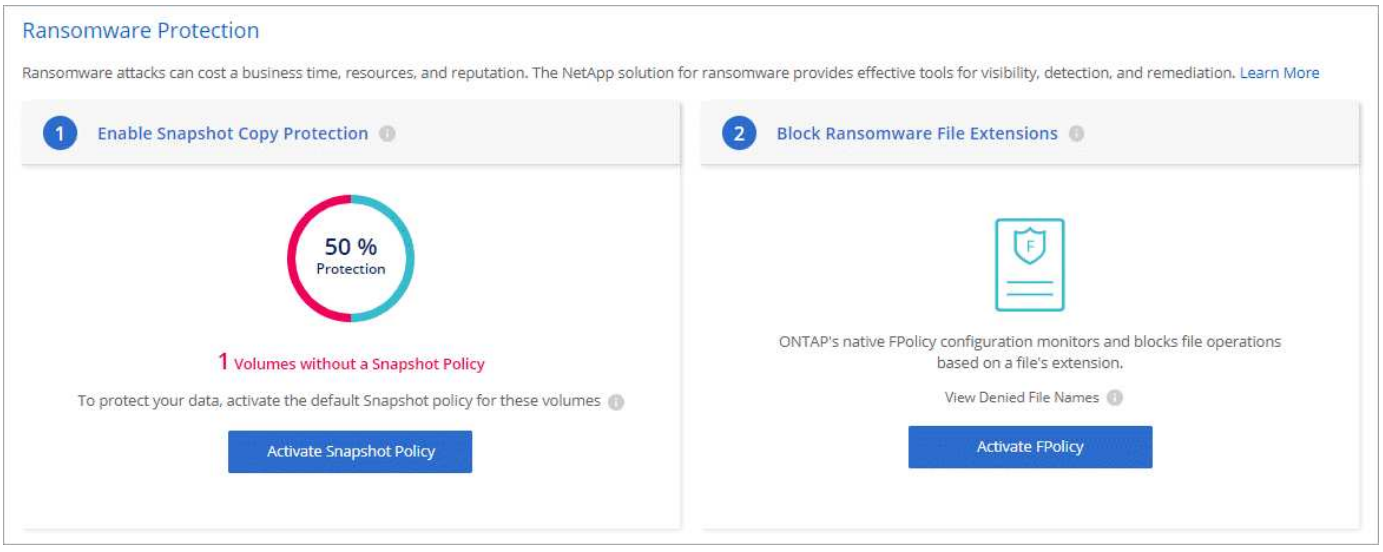


2. Implemente a solução NetApp para ransomware:
   a. Clique em **Ativar política de instantâneo**, se tiver volumes que não tenham uma política de instantâneo ativada.

      A tecnologia NetApp Snapshot oferece a melhor solução do setor para correção de ransomware. A chave para uma recuperação bem-sucedida é restaurar a partir de backups não infetados. As cópias snapshot são somente leitura, o que impede a corrupção de ransomware. Eles também podem fornecer a granularidade para criar imagens de uma única cópia de arquivo ou uma solução completa de recuperação de desastres.

   b. Clique em **Ativar FPolicy** para ativar a solução FPolicy do ONTAP, que pode bloquear operações de arquivo com base na extensão de um arquivo.

      Essa solução preventiva melhora a proteção contra ataques de ransomware bloqueando tipos comuns de arquivos de ransomware.



Administrar

Registar sistemas de pagamento conforme o uso

O suporte do NetApp está incluído nos sistemas Cloud Volumes ONTAP Explore, Standard e Premium, mas você deve primeiro ativar o suporte registrando os sistemas no NetApp.

Passos

1. Se você ainda não adicionou sua conta do site de suporte da NetApp ao Gerenciador de nuvem, acesse **Configurações da conta** e adicione-a agora.

   "Saiba como adicionar contas do site de suporte da NetApp".

2. Na página ambientes de trabalho, clique duas vezes no nome do sistema que deseja Registrar.
3. Clique no ícone do menu e, em seguida, clique em **Registro de suporte**:

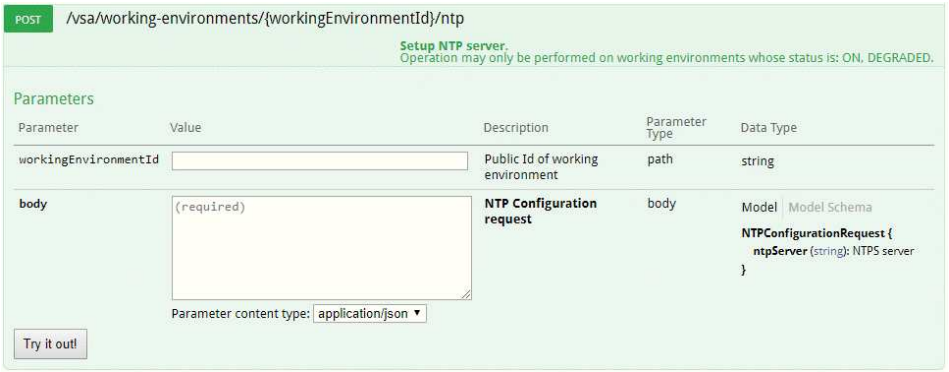
4. Selecione uma conta do site de suporte da NetApp e clique em **Register**.

Resultado

O Cloud Manager Registra o sistema com o NetApp.

Configurar o Cloud Volumes ONTAP

Depois de implantar o Cloud Volumes ONTAP, você pode configurá-lo sincronizando a hora do sistema usando o NTP e executando algumas tarefas opcionais do Gerenciador do sistema ou da CLI.

Tarefa	Descrição
Sincronize a hora do sistema usando NTP	Especificar um servidor NTP sincroniza o tempo entre os sistemas da rede, o que pode ajudar a evitar problemas devido a diferenças de tempo. Especifique um servidor NTP usando a API do Cloud Manager ou a partir da interface do usuário quando você configura um servidor CIFS. • "Modificação do servidor CIFS" • "Guia do desenvolvedor de API do Cloud Manager" Por exemplo, aqui está a API para um sistema de nó único na AWS: 
Opcional: Configurar o AutoSupport	O AutoSupport monitora proativamente a integridade do sistema e envia mensagens automaticamente para o suporte técnico da NetApp por padrão. Se o administrador da conta tiver adicionado um servidor proxy ao Cloud Manager antes de iniciar a instância, o Cloud Volumes ONTAP será configurado para usar esse servidor proxy para mensagens do AutoSupport. Você deve testar o AutoSupport para garantir que ele possa enviar mensagens. Para obter instruções, consulte a Ajuda do System Manager ou o "Referência de administração do sistema ONTAP 9".
Opcional: Configure o Cloud Manager como o proxy AutoSupport	Se o seu ambiente exigir um servidor proxy para enviar mensagens do AutoSupport, você pode configurar o Cloud Manager para agir como proxy. Nenhuma configuração para o Cloud Manager é necessária, além do acesso à Internet. Você simplesmente precisa ir para a CLI para Cloud Volumes ONTAP e executar o seguinte comando: `system node autosupport modify -proxy-url <cloud-manager-ip-address>`
Opcional: Configurar EMS	O sistema de Gestão de Eventos (EMS) recolhe e apresenta informações sobre eventos que ocorrem em sistemas Cloud Volumes ONTAP. Para receber notificações de eventos, você pode definir destinos de eventos (endereços de e-mail, hosts de intercetação SNMP ou servidores syslog) e rotas de eventos para uma determinada gravidade de evento. Você pode configurar o EMS usando a CLI. Para obter instruções, consulte "Guia expresso de configuração de EMS do ONTAP 9" .

Tarefa	Descrição
Opcional: Crie uma interface de rede de gerenciamento (LIF) SVM para sistemas de HA em várias zonas de disponibilidade da AWS	Uma interface de rede (LIF) de gerenciamento de máquina virtual de storage (SVM) é necessária se você quiser usar o SnapCenter ou o SnapDrive para Windows com um par de HA. O LIF de gerenciamento da SVM deve usar um endereço IP *flutuante* ao usar um par de HA em várias zonas de disponibilidade da AWS. O Cloud Manager solicita que você especifique o endereço IP flutuante ao iniciar o par de HA. Se você não tiver especificado o endereço IP, você poderá criar o SVM Management LIF a partir do System Manager ou da CLI. O exemplo a seguir mostra como criar o LIF a partir da CLI: `network interface create -vserver svm_cloud -lif svm_mgmt -role data -data-protocol none -home-node cloud-01 -home-port e0a -address 10.0.2.126 -netmask 255.255.255.0 -status-admin up -firewall -policy mgmt`
Opcional: Altere o local de backup dos arquivos de configuração	O Cloud Volumes ONTAP cria automaticamente arquivos de backup de configuração que contêm informações sobre as opções configuráveis que ele precisa para operar corretamente. Por padrão, o Cloud Volumes ONTAP faz backup dos arquivos para o host do conetor a cada oito horas. Se você quiser enviar os backups para um local alternativo, você pode alterar o local para um servidor FTP ou HTTP em seu data center ou na AWS. Por exemplo, talvez você já tenha um local de backup para seus sistemas de storage FAS. Você pode alterar o local de backup usando a CLI. Consulte "Referência de administração do sistema ONTAP 9" .

Gerenciamento de licenças BYOL para Cloud Volumes ONTAP

Adicione uma licença de sistema BYOL da Cloud Volumes ONTAP para adicionar capacidade adicional, atualizar uma licença de sistema existente e gerenciar licenças BYOL para backup na nuvem.

Gerenciamento de licenças de sistema

Você pode comprar várias licenças para um sistema BYOL da Cloud Volumes ONTAP para alocar mais de 368 TB de capacidade. Por exemplo, você pode comprar duas licenças para alocar até 736 TB de capacidade para o Cloud Volumes ONTAP. Ou você pode comprar quatro licenças para obter até 1,4 PB.

O número de licenças que você pode comprar para um único sistema de nó ou par de HA é ilimitado.

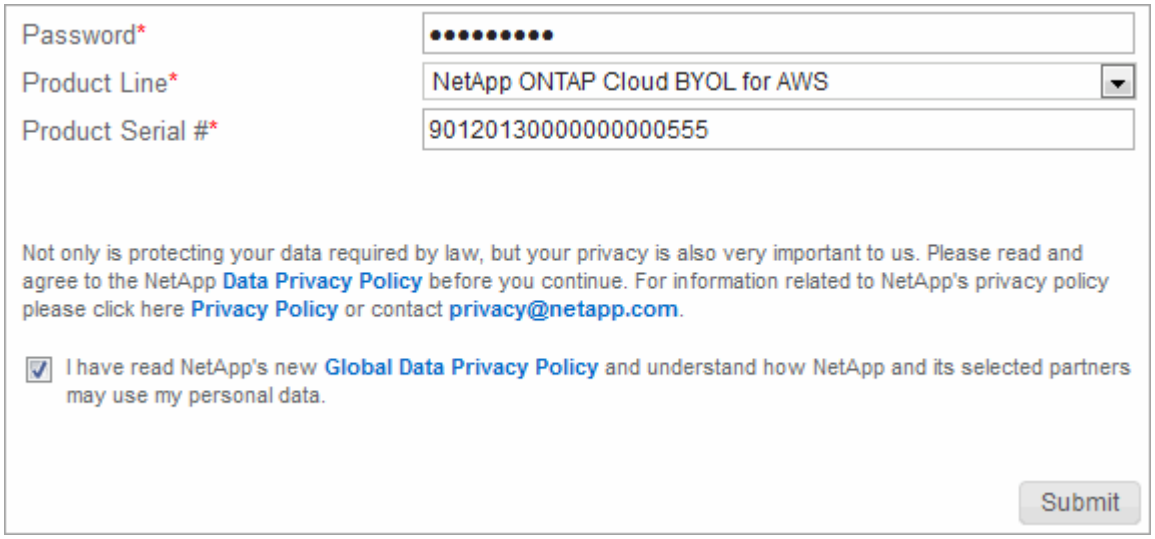
Obtenção de um ficheiro de licença do sistema

Na maioria dos casos, o Cloud Manager pode obter automaticamente seu arquivo de licença usando sua conta do site de suporte da NetApp. Mas se não puder, você precisará fazer o upload manual do arquivo de licença. Se não tiver o ficheiro de licença, pode obtê-lo a partir do NetApp.com.

Passos

1. Aceda ao "Gerador de arquivos de licença NetApp" e inicie sessão utilizando as suas credenciais do site de suporte da NetApp.
2. Introduza a sua palavra-passe, escolha o seu produto, introduza o número de série, confirme que leu e aceitou a política de privacidade e, em seguida, clique em **Enviar**.

   Exemplo



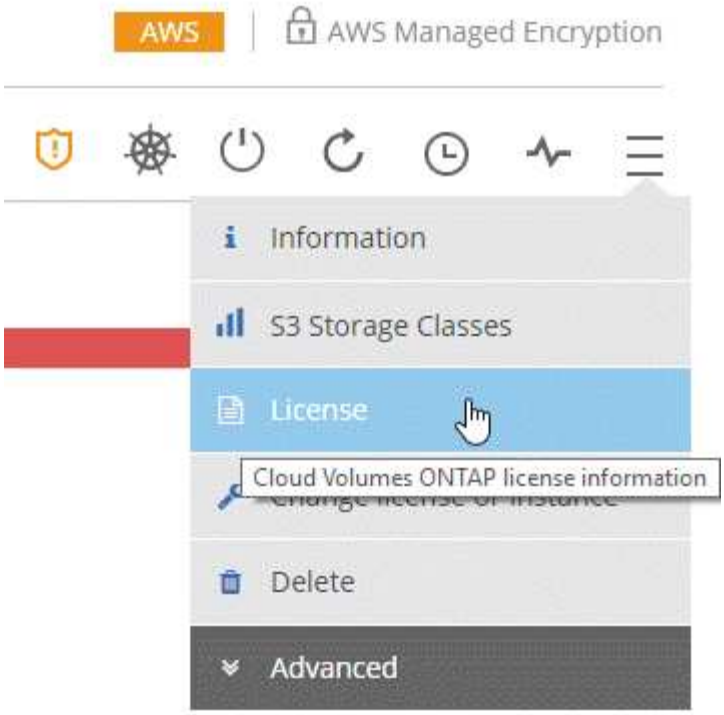
3. Escolha se você deseja receber o arquivo JSON serialnumber.NLF por e-mail ou download direto.

Adicionando uma nova licença de sistema

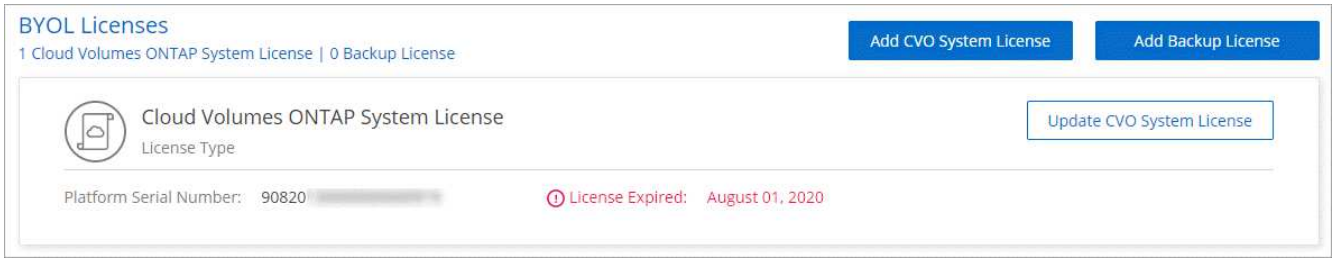
Adicione uma nova licença de sistema BYOL a qualquer momento para alocar 368 TB de capacidade adicional ao seu sistema BYOL da Cloud Volumes ONTAP.

Passos

1. No Cloud Manager, abra o ambiente de trabalho BYOL da Cloud Volumes ONTAP.
2. Clique no ícone do menu e, em seguida, clique em **Licença**.



3. Clique em **Add CVO System License**.



4. Escolha introduzir o número de série ou carregar o ficheiro de licença.
5. Clique em **Adicionar licença**.

Resultado

O Cloud Manager instala o novo arquivo de licença no sistema Cloud Volumes ONTAP.

Atualizar uma licença de sistema

Quando você renova uma assinatura BYOL entrando em Contato com um representante da NetApp, o Cloud Manager obtém automaticamente a nova licença do NetApp e a instala no sistema Cloud Volumes ONTAP.

Se o Cloud Manager não puder acessar o arquivo de licença pela conexão segura à Internet, você poderá obter o arquivo sozinho e, em seguida, fazer o upload manual do arquivo para o Cloud Manager.

Passos

1. No Cloud Manager, abra o ambiente de trabalho BYOL da Cloud Volumes ONTAP.
2. Clique no ícone do menu e, em seguida, clique em **Licença**.
3. Clique em **Atualizar licença do sistema CVO**.

4. Clique em **carregar ficheiro** e selecione o ficheiro de licença.
5. Clique em **Atualizar licença**.

Resultado

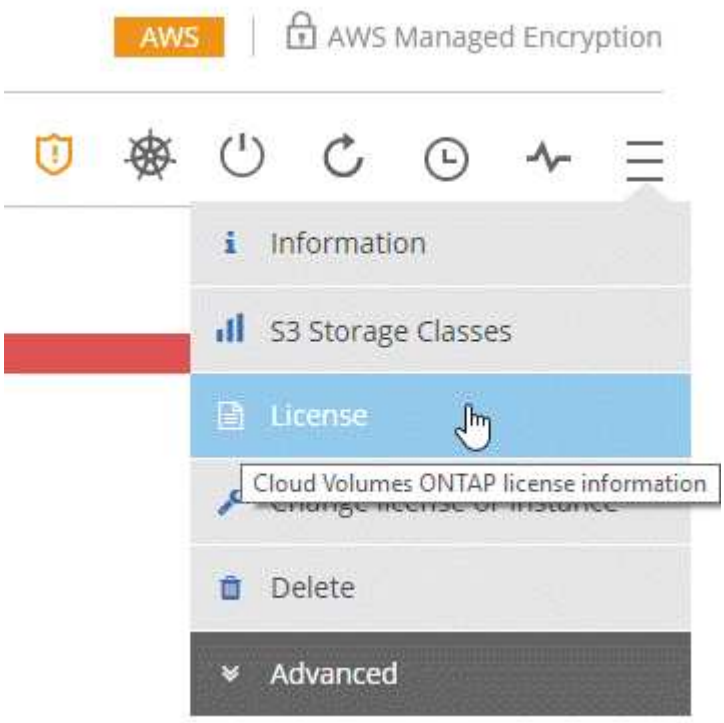
O Cloud Manager atualiza a licença no sistema Cloud Volumes ONTAP.

Adicionar e atualizar sua licença do Backup BYOL

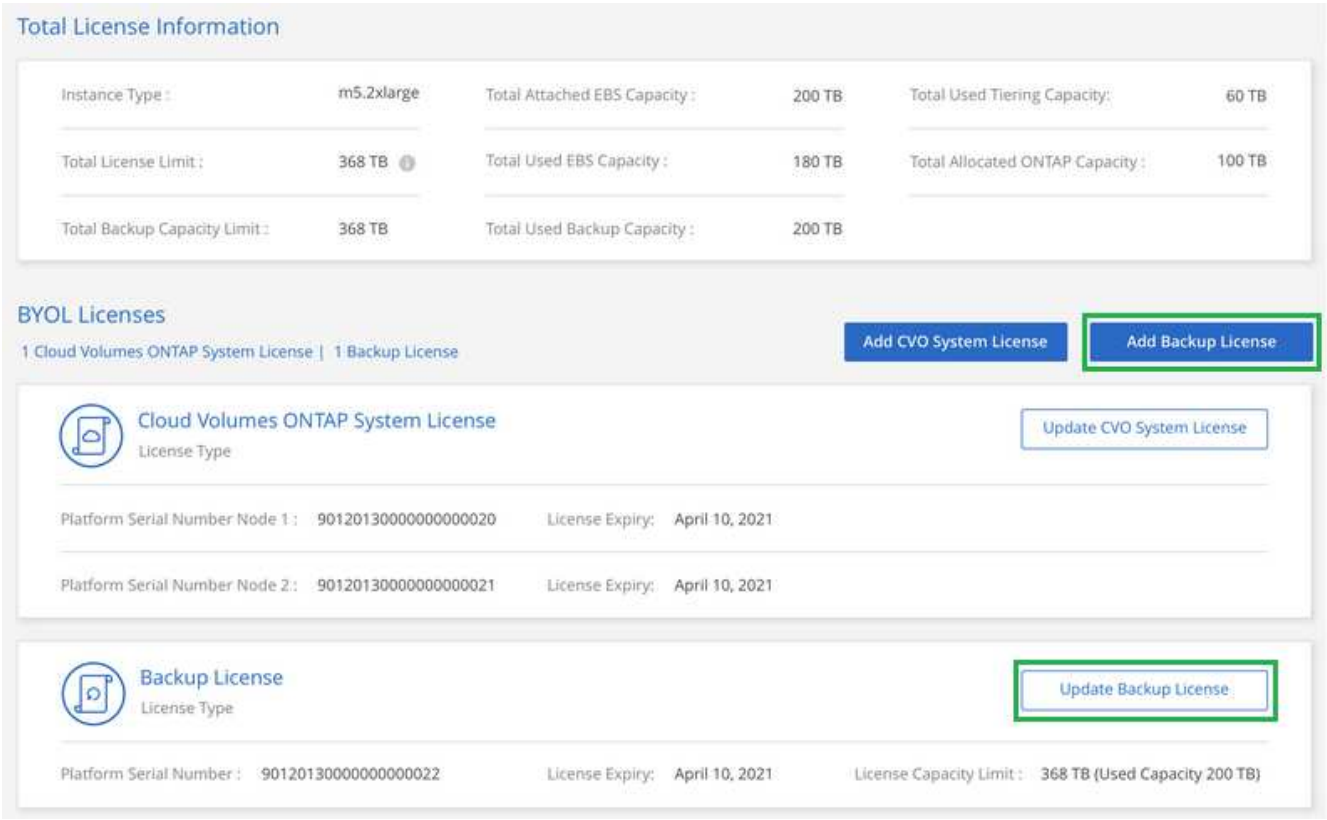
Você usa a página licenças BYOL para adicionar ou atualizar sua licença do Backup BYOL.

Passos

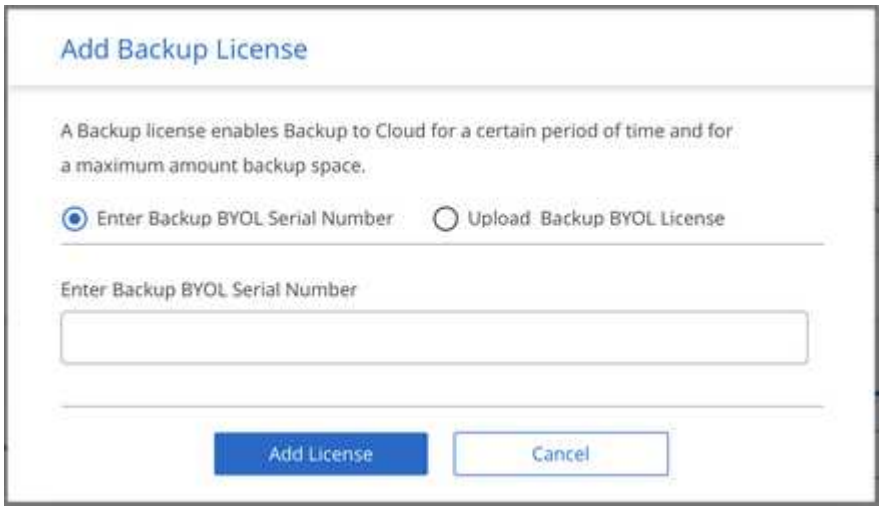
1. No Cloud Manager, abra o ambiente de trabalho BYOL da Cloud Volumes ONTAP.
2. Clique no ícone do menu e, em seguida, clique em **Licença**.



3. Clique em **Adicionar licença de backup** ou **Atualizar licença de backup** dependendo se você está adicionando uma nova licença ou atualizando uma licença existente.



4. Insira as informações da licença e clique em **Adicionar licença**:
   - Se você tiver o número de série, selecione a opção **Digite o número de série BYOL de backup** e digite o número de série.
   - Se você tiver o arquivo de licença de backup, selecione a opção **Upload Backup BYOL License** e siga as instruções para anexar o arquivo.



Resultado

O Cloud Manager adiciona ou atualiza a licença para que o serviço Backup to Cloud esteja ativo.

A atualizar o software Cloud Volumes ONTAP

O Cloud Manager inclui várias opções que você pode usar para atualizar para a versão

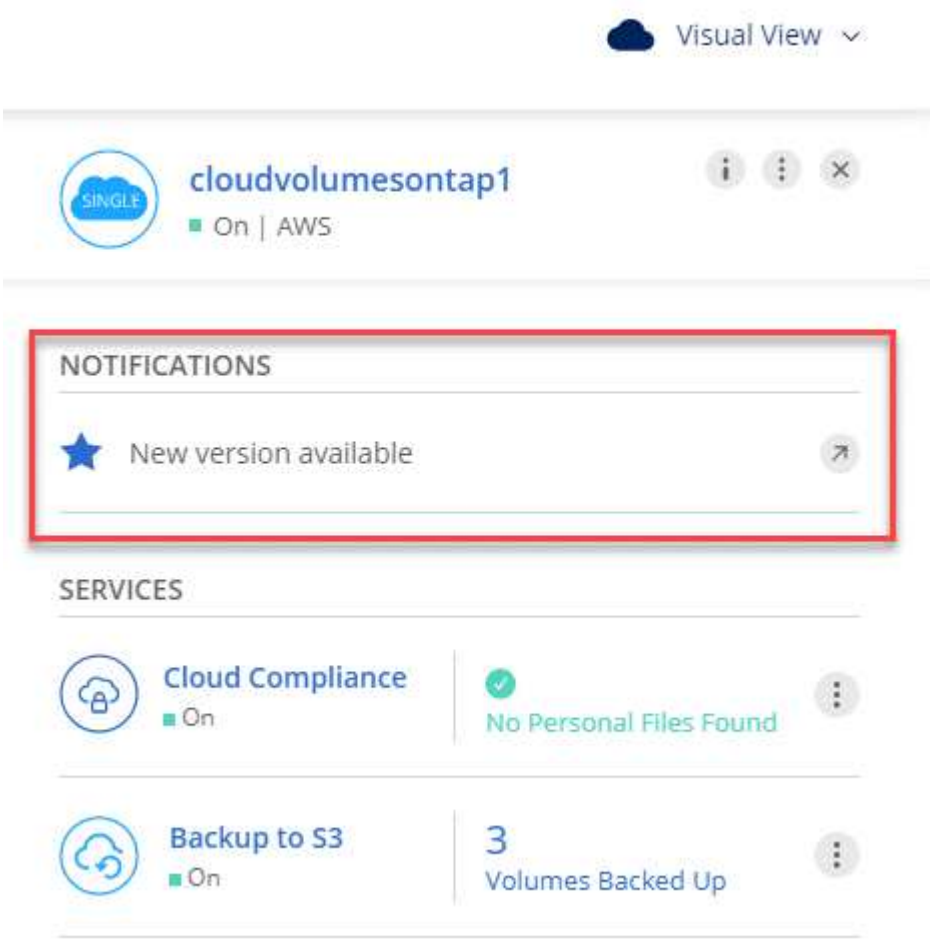
atual do Cloud Volumes ONTAP ou para fazer o downgrade do Cloud Volumes ONTAP para uma versão anterior. Você deve preparar os sistemas Cloud Volumes ONTAP antes de atualizar ou fazer o downgrade do software.

As atualizações de software devem ser concluídas pelo Cloud Manager

As atualizações do Cloud Volumes ONTAP devem ser concluídas a partir do Cloud Manager. Você não deve atualizar o Cloud Volumes ONTAP usando o Gerenciador de sistema ou a CLI. Isso pode afetar a estabilidade do sistema.

Maneiras de atualizar o Cloud Volumes ONTAP

O Cloud Manager exibe uma notificação em ambientes de trabalho do Cloud Volumes ONTAP quando uma nova versão do Cloud Volumes ONTAP está disponível:



Você pode iniciar o processo de atualização a partir desta notificação, que automatiza o processo, obtendo a imagem de software de um bucket do S3, instalando a imagem e reiniciando o sistema. Para obter detalhes, Atualizando o Cloud Volumes ONTAP a partir das notificações do Cloud Managerconsulte .

Para sistemas de HA na AWS, o Cloud Manager pode atualizar o mediador de HA como parte do processo de atualização.

Opções avançadas para atualizações de software

O Cloud Manager também oferece as seguintes opções avançadas para atualizar o software Cloud Volumes ONTAP:

- Atualizações de software usando uma imagem em um URL externo

  Essa opção é útil se o Cloud Manager não puder acessar o bucket do S3 para atualizar o software, se você tiver fornecido um patch ou se quiser fazer o downgrade do software para uma versão específica.

  Para obter detalhes, Atualizando ou baixando Cloud Volumes ONTAP usando um servidor HTTP ou FTPconsulte .

- Atualizações de software usando a imagem alternativa no sistema

  Você pode usar essa opção para fazer o downgrade para a versão anterior, tornando a imagem de software alternativa a imagem padrão. Essa opção não está disponível para pares de HA.

  Para obter detalhes, Downgrade Cloud Volumes ONTAP usando uma imagem localconsulte .

A preparar para atualizar o software Cloud Volumes ONTAP

Antes de executar uma atualização ou downgrade, você deve verificar se seus sistemas estão prontos e fazer as alterações necessárias na configuração.

- Planejamento para inatividade
- Rever os requisitos da versão
- Verificando se o giveback automático ainda está ativado
- Suspender transferências SnapMirror
- Verificar se os agregados estão online

Planejamento para inatividade

Quando você atualiza um sistema de nó único, o processo de atualização leva o sistema off-line por até 25 minutos, durante os quais a e/S é interrompida.

A atualização de um par de HA não causa interrupções e e/S é ininterrupta. Durante esse processo de atualização sem interrupções, cada nó é atualizado em conjunto para continuar fornecendo e/S aos clientes.

Rever os requisitos da versão

A versão do ONTAP para a qual você pode atualizar ou fazer o downgrade varia de acordo com a versão do ONTAP atualmente em execução no seu sistema.

Para compreender os requisitos da versão, "Documentação do ONTAP 9: Requisitos de atualização do cluster" consulte a .

Verificando se o giveback automático ainda está ativado

A giveback automática deve estar ativada num par de HA Cloud Volumes ONTAP (esta é a predefinição). Se não for, então a operação falhará.

"Documentação do ONTAP 9: Comandos para configurar o giveback automático"

Suspender transferências SnapMirror

Se um sistema Cloud Volumes ONTAP tiver relações SnapMirror ativas, é melhor suspender transferências antes de atualizar o software Cloud Volumes ONTAP. Suspender as transferências impede falhas no SnapMirror. Tem de suspender as transferências a partir do sistema de destino.

Sobre esta tarefa

Estas etapas descrevem como usar o System Manager para a versão 9,3 e posterior.

Passos

1. "Inicie sessão no System Manager" a partir do sistema de destino.
2. Clique em **proteção > relacionamentos**.
3. Selecione a relação e clique em **operações > quiesce**.

Verificar se os agregados estão online

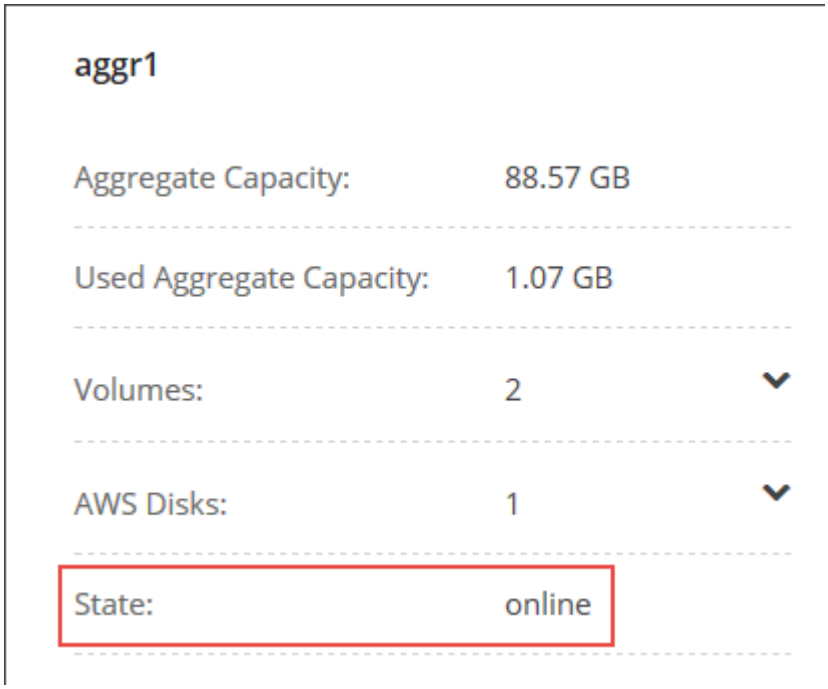
Os agregados para Cloud Volumes ONTAP devem estar online antes de atualizar o software. Os agregados devem estar online na maioria das configurações, mas se não estiverem, você deve colocá-los online.

Sobre esta tarefa

Estas etapas descrevem como usar o System Manager para a versão 9,3 e posterior.

Passos

1. No ambiente de trabalho, clique no ícone do menu e, em seguida, clique em **Avançado > Alocação avançada**.
2. Selecione um agregado, clique em **Info** e verifique se o estado está online.



3. Se o agregado estiver offline, use o System Manager para colocar o agregado on-line:
   a. "Inicie sessão no System Manager".
   b. Clique em **armazenamento > agregados e discos > agregados**.

c. Selecione o agregado e clique em **mais ações > Status > Online**.

Atualizando o Cloud Volumes ONTAP a partir das notificações do Cloud Manager

O Cloud Manager notifica você quando uma nova versão do Cloud Volumes ONTAP está disponível. Clique na notificação para iniciar o processo de atualização.

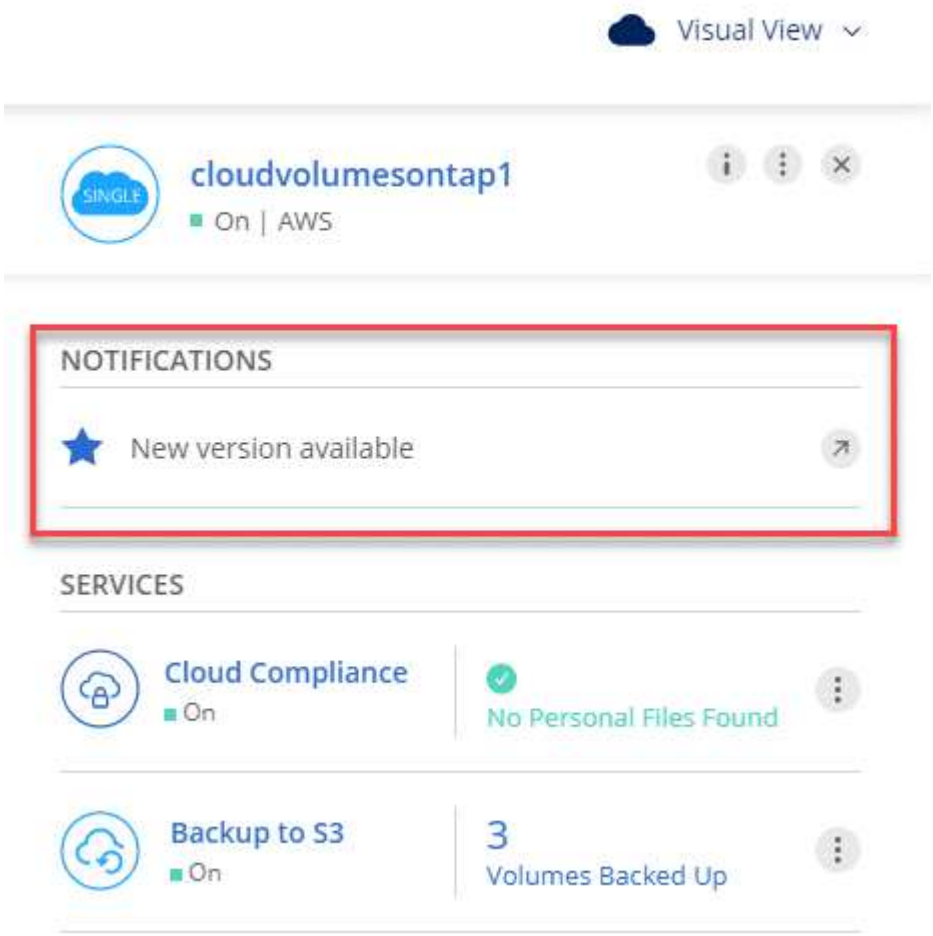
Antes de começar

As operações do Cloud Manager, como a criação de volume ou agregado, não devem estar em andamento para o sistema Cloud Volumes ONTAP.

Passos

1. Clique em **ambientes de trabalho**.
2. Selecione um ambiente de trabalho.

   Uma notificação será exibida no painel direito se uma nova versão estiver disponível:



3. Se uma nova versão estiver disponível, clique em **Upgrade**.
4. Na página informações da versão, clique no link para ler as Notas da versão especificada e marque a caixa de seleção **Eu li…**.
5. Na página Contrato de Licença de Usuário final (EULA), leia o EULA e selecione **Eu li e aprovo o EULA**.

6. Na página Revisão e aprovação, leia as notas importantes, selecione **Eu entendo…** e clique em **ir**.

Resultado

O Cloud Manager inicia a atualização de software. Você pode executar ações no ambiente de trabalho assim que a atualização de software estiver concluída.

Depois de terminar

Se você suspendeu as transferências do SnapMirror, use o Gerenciador do sistema para retomar as transferências.

Atualizando ou baixando Cloud Volumes ONTAP usando um servidor HTTP ou FTP

Você pode colocar a imagem do software Cloud Volumes ONTAP em um servidor HTTP ou FTP e, em seguida, iniciar a atualização do software a partir do Gerenciador de nuvem. Você pode usar essa opção se o Cloud Manager não puder acessar o bucket do S3 para atualizar o software ou se quiser fazer o downgrade do software.

Passos

1. Configure um servidor HTTP ou FTP que possa hospedar a imagem do software Cloud Volumes ONTAP.
2. Se você tiver uma conexão VPN com a rede virtual, poderá colocar a imagem do software Cloud Volumes ONTAP em um servidor HTTP ou FTP em sua própria rede. Caso contrário, você deve colocar o arquivo em um servidor HTTP ou servidor FTP na nuvem.
3. Se você usar seu próprio grupo de segurança para o Cloud Volumes ONTAP, verifique se as regras de saída permitem conexões HTTP ou FTP para que o Cloud Volumes ONTAP possa acessar a imagem do software.

   O grupo de segurança Cloud Volumes ONTAP predefinido permite ligações HTTP e FTP de saída por predefinição.

4. Obtenha a imagem do software em "O site de suporte da NetApp".
5. Copie a imagem do software para o diretório no servidor HTTP ou FTP a partir do qual o arquivo será servido.
6. No ambiente de trabalho do Cloud Manager, clique no ícone de menu e, em seguida, clique em **Avançado > Atualizar Cloud Volumes ONTAP**.
7. Na página de atualização do software, escolha **Selecione uma imagem disponível a partir de um URL**, insira o URL e clique em **alterar imagem**.
8. Clique em **Proceed** para confirmar.

Resultado

O Cloud Manager inicia a atualização de software. Você pode executar ações no ambiente de trabalho assim que a atualização de software estiver concluída.

Depois de terminar

Se você suspendeu as transferências do SnapMirror, use o Gerenciador do sistema para retomar as transferências.

Downgrade Cloud Volumes ONTAP usando uma imagem local

A transição do Cloud Volumes ONTAP para uma versão anterior na mesma família de versões (por exemplo, 9,5 para 9,4) é referida como downgrade. Você pode fazer o downgrade sem assistência ao fazer o

downgrade de clusters novos ou de teste, mas entre em Contato com o suporte técnico se quiser fazer o downgrade de um cluster de produção.

Cada sistema Cloud Volumes ONTAP pode conter duas imagens de software: A imagem atual que está sendo executada e uma imagem alternativa que você pode inicializar. O Cloud Manager pode alterar a imagem alternativa para ser a imagem padrão. Você pode usar essa opção para fazer o downgrade para a versão anterior do Cloud Volumes ONTAP, se estiver com problemas com a imagem atual.

Sobre esta tarefa

Este processo de downgrade está disponível apenas para sistemas Cloud Volumes ONTAP únicos. Ele não está disponível para pares de HA.

Passos

1. No ambiente de trabalho, clique no ícone de menu e, em seguida, clique em **Avançado > Atualizar Cloud Volumes ONTAP**.
2. Na página de atualização do software, selecione a imagem alternativa e clique em **alterar imagem**.
3. Clique em **Proceed** para confirmar.

Resultado

O Cloud Manager inicia a atualização de software. Você pode executar ações no ambiente de trabalho assim que a atualização de software estiver concluída.

Depois de terminar

Se você suspendeu as transferências do SnapMirror, use o Gerenciador do sistema para retomar as transferências.

Modificação de sistemas Cloud Volumes ONTAP

Talvez seja necessário alterar a configuração dos sistemas Cloud Volumes ONTAP à medida que suas necessidades de storage mudam. Por exemplo, você pode alterar entre configurações de pagamento conforme o uso, alterar a instância ou o tipo de VM e muito mais.

Alterar a instância ou o tipo de máquina para o Cloud Volumes ONTAP

Você pode escolher entre vários tipos de instância ou máquina ao iniciar o Cloud Volumes ONTAP na AWS, Azure ou GCP. Você pode alterar a instância ou o tipo de máquina a qualquer momento se você determinar que ela é subdimensionada ou superdimensionada para suas necessidades.

Sobre esta tarefa

- A giveback automática deve estar ativada num par de HA Cloud Volumes ONTAP (esta é a predefinição). Se não for, então a operação falhará.

  "Documentação do ONTAP 9: Comandos para configurar o giveback automático"

- Alterar a instância ou o tipo de máquina afeta as taxas de serviço do provedor de nuvem.
- A operação reinicia o Cloud Volumes ONTAP.

  Para sistemas de nó único, a e/S é interrompida.

  Para pares de HA, a alteração não causa interrupções. Os pares DE HA continuam fornecendo dados.

O Cloud Manager muda tranquilamente um nó de cada vez, iniciando o takeover e aguardando a devolução. A equipe de QA da NetApp testou tanto a escrita quanto a leitura de arquivos durante esse processo e não viu nenhum problema no lado do cliente. À medida que as conexões mudaram, vimos tentativas no nível de e/S, mas a camada de aplicativo superou esses "rewire" curtos de conexões NFS/CIFS.

Passos

1. No ambiente de trabalho, clique no ícone do menu e clique em **alterar licença ou instância** para AWS, **alterar licença ou VM** para Azure ou **alterar licença ou máquina** para GCP.
2. Se você estiver usando uma configuração de pagamento conforme o uso, você pode escolher uma licença diferente.
3. Selecione uma instância ou tipo de máquina, marque a caixa de seleção para confirmar que você entende as implicações da alteração e clique em **OK**.

Resultado

O Cloud Volumes ONTAP reinicializa com a nova configuração.

Alteração entre configurações de pagamento conforme o uso

Depois de iniciar os sistemas Cloud Volumes ONTAP com pagamento conforme o uso, você pode alterar as configurações explorar, padrão e Premium a qualquer momento, modificando a licença. Alterar a licença aumenta ou diminui o limite de capacidade bruta e permite que você escolha entre diferentes tipos de instância da AWS ou tipos de máquina virtual do Azure.

No GCP, um único tipo de máquina está disponível para cada configuração de pagamento conforme o uso. Você não pode escolher entre diferentes tipos de máquina.

Sobre esta tarefa

Observe o seguinte sobre como alterar entre licenças de pagamento conforme o uso:

- A operação reinicia o Cloud Volumes ONTAP.

  Para sistemas de nó único, a e/S é interrompida.

  Para pares de HA, a alteração não causa interrupções. Os pares DE HA continuam fornecendo dados.

- Alterar a instância ou o tipo de máquina afeta as taxas de serviço do provedor de nuvem.

Passos

1. No ambiente de trabalho, clique no ícone do menu e clique em **alterar licença ou instância** para AWS, **alterar licença ou VM** para Azure ou **alterar licença ou máquina** para GCP.
2. Selecione um tipo de licença e um tipo de instância ou tipo de máquina, marque a caixa de seleção para confirmar que você entende as implicações da alteração e clique em **OK**.

Resultado

O Cloud Volumes ONTAP reinicializa com a nova licença, tipo de instância ou tipo de máquina, ou ambos.

Movendo para uma configuração Cloud Volumes ONTAP alternativa

Se você quiser alternar entre uma assinatura paga conforme o uso e uma assinatura BYOL ou entre um único sistema Cloud Volumes ONTAP e um par de HA, precisará implantar um novo sistema e replicar dados do

sistema existente para o novo sistema.

Passos

1. Crie um novo ambiente de trabalho do Cloud Volumes ONTAP.

   "Iniciando o Cloud Volumes ONTAP na AWS" "Iniciar o Cloud Volumes ONTAP no Azure" "Iniciando o Cloud Volumes ONTAP na GCP"

2. "Configure a replicação de dados única" entre os sistemas para cada volume que você precisa replicar.
3. Encerre o sistema Cloud Volumes ONTAP que você não precisa mais "eliminar o ambiente de trabalho original"pelo .

Alterar a velocidade de gravação para normal ou alta

O Cloud Manager permite escolher uma configuração de velocidade de gravação para sistemas Cloud Volumes ONTAP de nó único. A velocidade de gravação padrão é normal. Você pode mudar para alta velocidade de gravação se a performance de gravação rápida for necessária para seu workload. Antes de alterar a velocidade de gravação, você deve "entenda as diferenças entre as configurações normal e alta".

Sobre esta tarefa

- Certifique-se de que operações como criação de volume ou agregado não estejam em andamento.
- Esteja ciente de que essa alteração reinicia o Cloud Volumes ONTAP, o que significa que a e/S é interrompida.

Passos

1. No ambiente de trabalho, clique no ícone do menu e, em seguida, clique em **Avançado > velocidade de escrita**.
2. Selecione **normal** ou **High**.

   Se você escolher Alto, então você precisará ler a declaração "Eu entendo…" e confirmar marcando a caixa.

3. Clique em **Salvar**, revise a mensagem de confirmação e clique em **continuar**.

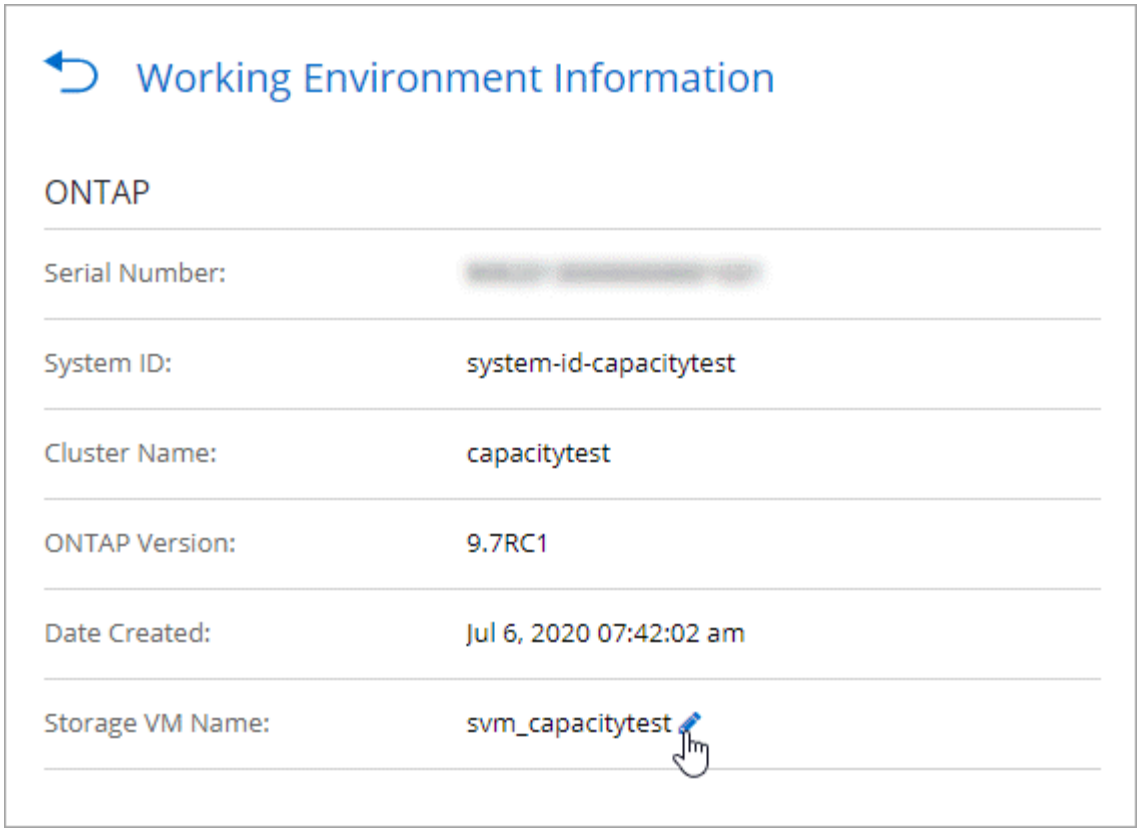
Modificação do nome da VM de armazenamento

O Cloud Manager nomeia automaticamente a única VM de storage (SVM) criada para o Cloud Volumes ONTAP. Você pode modificar o nome do SVM se tiver padrões de nomenclatura rigorosos. Por exemplo, talvez você queira que o nome corresponda ao nome dos SVMs para os clusters do ONTAP.

Mas se você criou quaisquer SVMs adicionais para o Cloud Volumes ONTAP, então você não pode renomear os SVMs do Cloud Manager. Você precisará fazer isso diretamente do Cloud Volumes ONTAP usando o Gerenciador de sistema ou a CLI.

Passos

1. No ambiente de trabalho, clique no ícone do menu e, em seguida, clique em **Informação**.
2. Clique no ícone de edição à direita do nome da VM de armazenamento.



3. Na caixa de diálogo Modificar Nome do SVM, altere o nome e clique em **Salvar**.

Alterar a palavra-passe do Cloud Volumes ONTAP

O Cloud Volumes ONTAP inclui uma conta de administrador do cluster. Você pode alterar a senha dessa conta no Cloud Manager, se necessário.

> Você não deve alterar a senha da conta de administrador por meio do System Manager ou da CLI. A senha não será refletida no Cloud Manager. Como resultado, o Cloud Manager não pode monitorar a instância corretamente.

Passos

1. No ambiente de trabalho, clique no ícone do menu e, em seguida, clique em **Avançado > Definir senha**.
2. Digite a nova senha duas vezes e clique em **Salvar**.

   A nova senha deve ser diferente de uma das últimas seis senhas que você usou.

Alteração da MTU da rede para instâncias c4,4xlarge e c4,8xlarge

Por padrão, o Cloud Volumes ONTAP é configurado para usar o MTU 9.000 (também chamado de quadros jumbo) quando você escolhe a instância c4,4xlarge ou a instância c4,8xlarge na AWS. Você pode alterar a MTU da rede para 1.500 bytes se isso for mais apropriado para a configuração da rede.

Sobre esta tarefa

Uma unidade de transmissão máxima de rede (MTU) de 9.000 bytes pode fornecer a taxa de transferência máxima de rede mais alta possível para configurações específicas.

9.000 MTU é uma boa escolha se os clientes na mesma VPC se comunicam com o sistema Cloud Volumes

ONTAP e alguns ou todos esses clientes também suportam 9.000 MTU. Se o tráfego sair da VPC, a fragmentação de pacotes pode ocorrer, o que degrada o desempenho.

Uma MTU de rede de 1.500 bytes é uma boa escolha se clientes ou sistemas fora da VPC se comunicam com o sistema Cloud Volumes ONTAP.

Passos

1. No ambiente de trabalho, clique no ícone do menu e, em seguida, clique em **Avançado > utilização da rede**.
2. Selecione **Standard** ou **Jumbo Frames**.
3. Clique em **alterar**.

Alterar tabelas de rota associadas a pares de HA em vários AWS AZs

Você pode modificar as tabelas de rota da AWS que incluem rotas para os endereços IP flutuantes de um par de HA. Você pode fazer isso se novos clientes NFS ou CIFS precisarem acessar um par de HA na AWS.

Passos

1. No ambiente de trabalho, clique no ícone do menu e, em seguida, clique em **Informação**.
2. Clique em **Tabelas de rotas**.
3. Modifique a lista de tabelas de rota selecionadas e clique em **Salvar**.

Resultado

O Cloud Manager envia uma solicitação da AWS para modificar as tabelas de rota.

Gerenciando o estado do Cloud Volumes ONTAP

Você pode interromper e iniciar o Cloud Volumes ONTAP do Cloud Manager para gerenciar seus custos de computação em nuvem.

Agendamento de paradas automáticas do Cloud Volumes ONTAP

Você pode querer desligar o Cloud Volumes ONTAP durante intervalos de tempo específicos para reduzir seus custos de computação. Em vez de fazer isso manualmente, você pode configurar o Cloud Manager para desligar automaticamente e reiniciar os sistemas em momentos específicos.

Sobre esta tarefa

Quando você agendar um desligamento automático do seu sistema Cloud Volumes ONTAP, o Cloud Manager adia o desligamento se uma transferência de dados ativa estiver em andamento. O Cloud Manager desliga o sistema após a transferência ser concluída.

Essa tarefa agenda paradas automáticas de ambos os nós em um par de HA.

Passos

1. No ambiente de trabalho, clique no ícone do relógio:

2. Especifique o agendamento de encerramento:

a. Escolha se deseja desligar o sistema todos os dias, todos os dias da semana, todos os fins de semana ou qualquer combinação das três opções.

b. Especifique quando pretende desligar o sistema e durante quanto tempo pretende que este seja desligado.

Exemplo

A imagem a seguir mostra uma programação que instrui o Cloud Manager a desligar o sistema todos os sábados às 12:00 da manhã por 48 horas. O Cloud Manager reinicia o sistema todas as segundas-feiras às 12:00 da manhã

3. Clique em **Salvar**.

Resultado

O Cloud Manager salva a programação. O ícone do relógio muda para indicar que está definido um agendamento: 

Parar o Cloud Volumes ONTAP

Parar o Cloud Volumes ONTAP evita que você acumule custos de computação e cria snapshots dos discos raiz e de inicialização, o que pode ser útil para a solução de problemas.

Sobre esta tarefa

Quando você interrompe um par de HA, o Cloud Manager desliga ambos os nós.

Passos

1. No ambiente de trabalho, clique no ícone **Desligar**.

2. Mantenha a opção de criar instantâneos ativada porque os instantâneos podem ativar a recuperação do sistema.
3. Clique em **Desligar**.

   Pode demorar alguns minutos para parar o sistema. Pode reiniciar os sistemas posteriormente a partir da página ambiente de trabalho.

Monitoramento dos custos de recursos da AWS

O Cloud Manager permite visualizar os custos de recursos associados à execução do Cloud Volumes ONTAP na AWS. Você também pode ver quanto dinheiro você economizou usando os recursos do NetApp que podem reduzir os custos de armazenamento.

Sobre esta tarefa

O Cloud Manager atualiza os custos ao atualizar a página. Você deve consultar a AWS para obter detalhes de custo final.

Passo

1. Verifique se o Cloud Manager pode obter informações de custo da AWS:
   a. Verifique se a política do IAM que fornece permissões ao Cloud Manager inclui as seguintes ações:

      ```
      "ce:GetReservationUtilization",
      "ce:GetDimensionValues",
      "ce:GetCostAndUsage",
      "ce:GetTags"
      ```

      Essas ações estão incluídas no último "Política do Cloud Manager". Os novos sistemas implantados a partir do NetApp Cloud Central incluem automaticamente essas permissões.

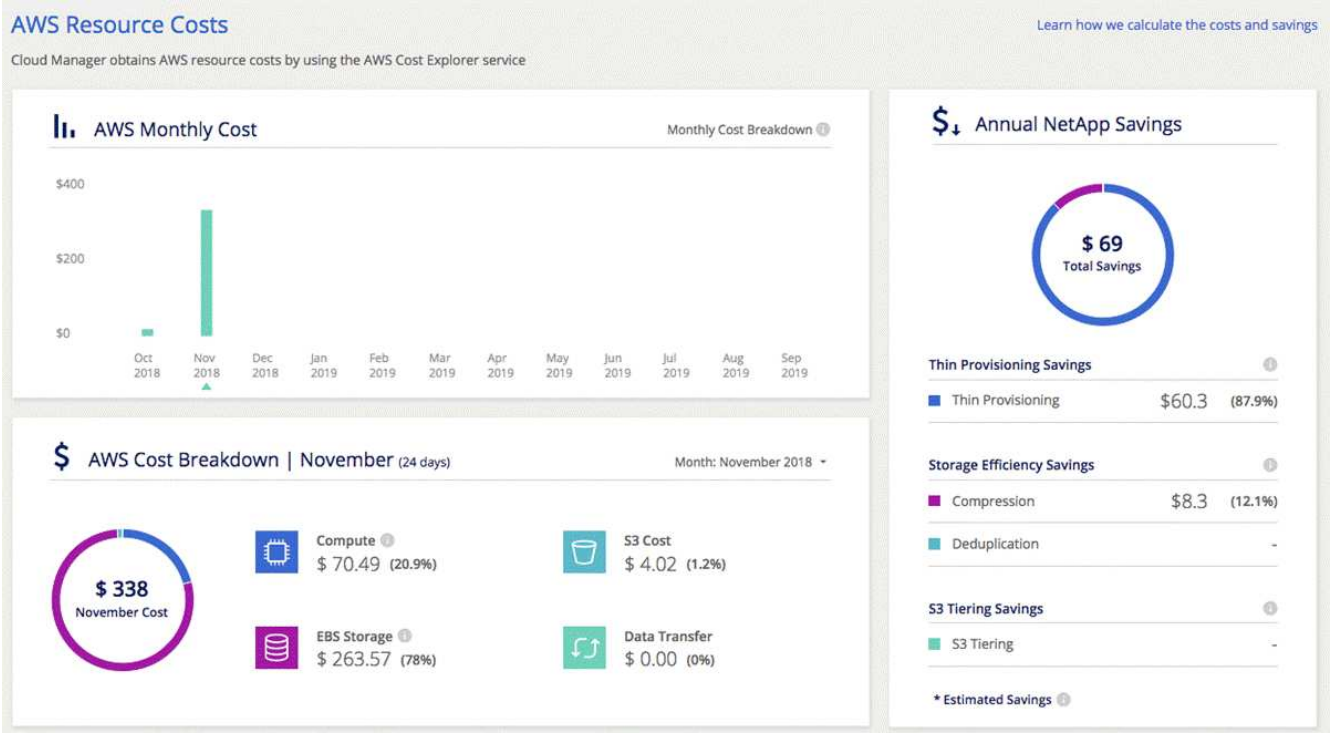
   b. "Ative a tag **WorkingEnvironmentId**".

      Para controlar seus custos da AWS, o Cloud Manager atribui uma tag de alocação de custos às instâncias do Cloud Volumes ONTAP. Depois de criar seu primeiro ambiente de trabalho, ative a tag **WorkingEnvironmentId**. As tags definidas pelo usuário não aparecem nos relatórios de cobrança da AWS até que você os ative no console de Gerenciamento de custos e cobrança.

2. Na página ambientes de trabalho, selecione um ambiente de trabalho Cloud Volumes ONTAP e clique em **custo**.

   A página custo exibe os custos dos meses atuais e anteriores e mostra suas economias anuais com o NetApp, se você ativou os recursos de economia de custos do NetApp em volumes.

   A imagem a seguir mostra uma página de custo de amostra:



A ligar ao Cloud Volumes ONTAP

Se você precisar executar o gerenciamento avançado do Cloud Volumes ONTAP, você pode fazê-lo usando o OnCommand System Manager ou a interface de linha de comando.

A ligar ao System Manager

Talvez você precise executar algumas tarefas do Cloud Volumes ONTAP do Gerenciador de sistema, que é uma ferramenta de gerenciamento baseada em navegador que é executada no sistema Cloud Volumes ONTAP. Por exemplo, você precisa usar o System Manager se quiser criar LUNs.

Antes de começar

O computador a partir do qual você está acessando o Cloud Manager deve ter uma conexão de rede com o Cloud Volumes ONTAP. Por exemplo, talvez seja necessário fazer login no Cloud Manager a partir de um host avançado na AWS ou no Azure.

Quando implantadas em várias zonas de disponibilidade da AWS, as configurações do Cloud Volumes ONTAP HA usam um endereço IP flutuante para a interface de gerenciamento de cluster, o que significa que o roteamento externo não está disponível. Você deve se conetar a partir de um host que faça parte do mesmo domínio de roteamento.

Passos

1. Na página ambientes de trabalho, clique duas vezes no sistema Cloud Volumes ONTAP que você deseja gerenciar com o Gerenciador de sistema.
2. Clique no ícone do menu e, em seguida, clique em **Avançado > Gestor de sistema**.
3. Clique em **Launch**.

   O System Manager é carregado em uma nova guia do navegador.

4. No ecrã de início de sessão, introduza **admin** no campo Nome de utilizador, introduza a palavra-passe que especificou quando criou o ambiente de trabalho e, em seguida, clique em **Iniciar sessão**.

Resultado

O console do System Manager é carregado. Agora você pode usá-lo para gerenciar o Cloud Volumes ONTAP.

Conexão com a CLI do Cloud Volumes ONTAP

A CLI do Cloud Volumes ONTAP permite executar todos os comandos administrativos e é uma boa escolha para tarefas avançadas ou se você estiver mais confortável usando a CLI. Você pode se conetar à CLI usando o Secure Shell (SSH).

Antes de começar

O host a partir do qual você usa SSH para se conetar ao Cloud Volumes ONTAP deve ter uma conexão de rede com o Cloud Volumes ONTAP. Por exemplo, você pode precisar usar SSH de um host de salto na AWS ou no Azure.

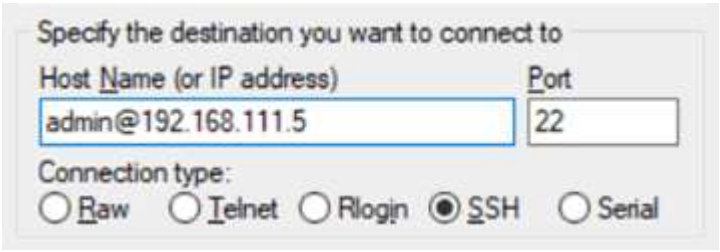
> Quando implantadas em vários AZs, as configurações do Cloud Volumes ONTAP HA usam um endereço IP flutuante para a interface de gerenciamento de cluster, o que significa que o roteamento externo não está disponível. Você deve se conetar a partir de um host que faça parte do mesmo domínio de roteamento.

Passos

1. No Cloud Manager, identifique o endereço IP da interface de gerenciamento de cluster:
   a. Na página ambientes de trabalho, selecione o sistema Cloud Volumes ONTAP.
   b. Copie o endereço IP de gerenciamento de cluster que aparece no painel direito.
2. Use SSH para se conetar ao endereço IP da interface de gerenciamento de cluster usando a conta de administrador.

   Exemplo

   A imagem a seguir mostra um exemplo usando PuTTY:



3. No prompt de login, insira a senha da conta de administrador.

   Exemplo

```
Password: ********
COT2::>
```

Adição de sistemas Cloud Volumes ONTAP existentes ao Cloud Manager

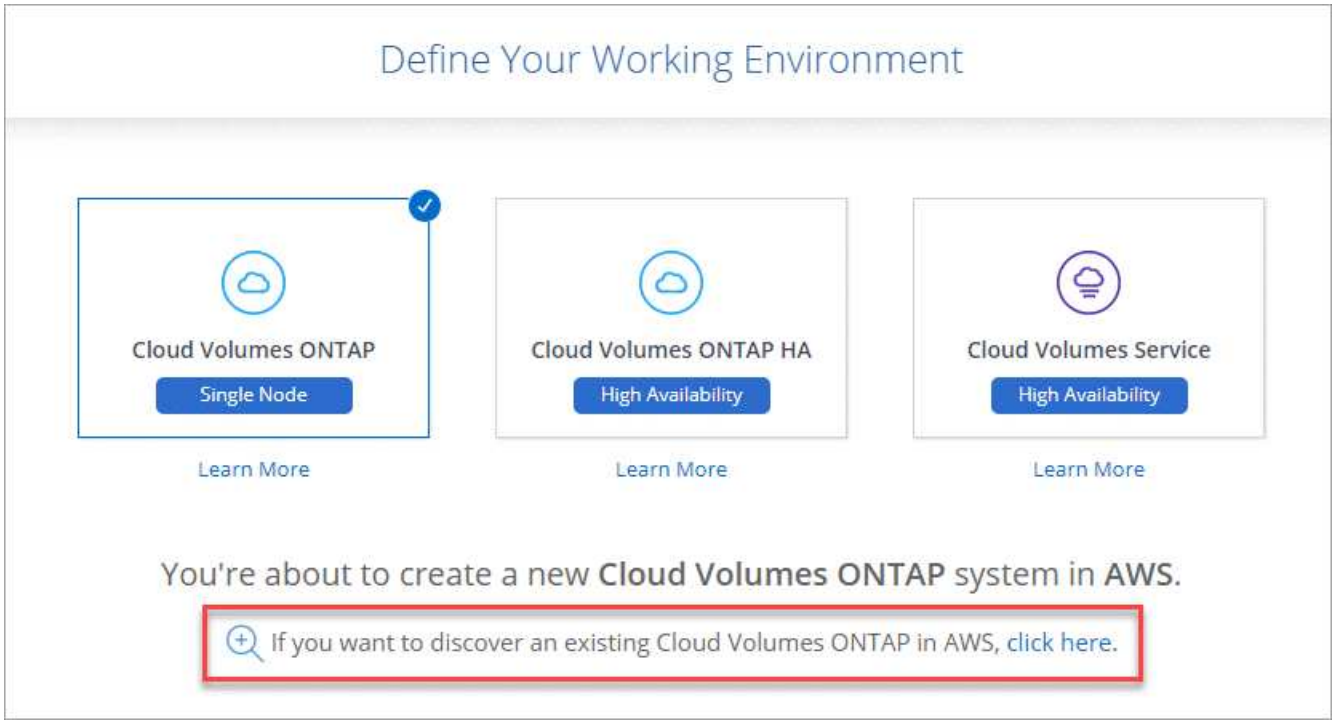
Você pode descobrir e adicionar sistemas Cloud Volumes ONTAP existentes ao Cloud Manager. Você pode fazer isso se você implantou um novo sistema do Cloud Manager.

Antes de começar

Você deve saber a senha da conta de usuário admin do Cloud Volumes ONTAP.

Passos

1. Na página ambientes de trabalho, clique em **Adicionar ambiente de trabalho**.
2. Selecione o provedor de nuvem no qual o sistema reside.
3. Escolha o tipo de sistema Cloud Volumes ONTAP.
4. Clique no link para descobrir um sistema existente.



5. Na página região, escolha a região em que as instâncias estão sendo executadas e selecione as instâncias.
6. Na página credenciais, digite a senha do usuário admin do Cloud Volumes ONTAP e clique em **Go**.

Resultado

O Cloud Manager adiciona as instâncias do Cloud Volumes ONTAP à área de trabalho.

Eliminar um ambiente de trabalho do Cloud Volumes ONTAP

É melhor excluir sistemas Cloud Volumes ONTAP do Gerenciador de nuvem, em vez de do console do seu provedor de nuvem. Por exemplo, se você encerrar uma instância do Cloud Volumes ONTAP licenciada da AWS, não poderá usar a chave de licença para outra instância. Você deve excluir o ambiente de trabalho do Cloud Manager para liberar a licença.

Sobre esta tarefa

Quando você exclui um ambiente de trabalho, o Cloud Manager encerra instâncias, exclui discos e snapshots.

> As instâncias do Cloud Volumes ONTAP têm proteção de terminação habilitada para ajudar a evitar o encerramento acidental da AWS. No entanto, se você encerrar uma instância do Cloud Volumes ONTAP da AWS, deverá ir para o console do AWS CloudFormation e excluir a pilha da instância. O nome da pilha é o nome do ambiente de trabalho.

Passos

1. No ambiente de trabalho, clique no ícone de menu e, em seguida, clique em **Delete**.
2. Digite o nome do ambiente de trabalho e clique em **Excluir**.

   Pode demorar até 5 minutos para eliminar o ambiente de trabalho.

Provisionar volumes usando um serviço de arquivos

Azure NetApp Files

Saiba mais sobre o Azure NetApp Files

O Azure NetApp Files permite que as empresas migrem e executem aplicações essenciais aos negócios essenciais aos negócios sensíveis à latência e exigentes no Azure, sem precisar refatorar a nuvem.

Caraterísticas

- O suporte a vários protocolos permite que as aplicações Linux e Windows sejam executadas de forma otimizada no Azure.
- Várias camadas de performance permitem um alinhamento próximo aos requisitos de performance de workload.
- As principais certificações, incluindo SAP HANA, GDPR e HIPPA, permitem a migração dos workloads mais exigentes para o Azure.

Recursos adicionais no Cloud Manager

- Migre dados NFS ou SMB para o Azure NetApp Files diretamente do Cloud Manager. As migrações de dados são alimentadas pelo serviço Cloud Sync da NetApp. "Saiba mais".
- Usando tecnologia orientada por inteligência artificial (AI), o Cloud Compliance pode ajudar você a entender o contexto dos dados e identificar dados confidenciais que residem em suas contas do Azure NetApp Files. "Saiba mais".

Custo

"Ver preços do Azure NetApp Files".

Observe que sua assinatura e cobrança são mantidos pelo serviço Azure NetApp Files e não pelo Cloud Manager.

Regiões suportadas

"Ver regiões do Azure suportadas".

A solicitar acesso

Você precisa ter acesso ao Azure NetApp Files por "enviando uma solicitação on-line". Você precisará esperar pela aprovação da equipe do Azure NetApp Files antes de prosseguir.

Obter ajuda

Para problemas de suporte técnico associados ao Azure NetApp Files, use o portal do Azure para Registrar uma solicitação de suporte à Microsoft. Selecione sua assinatura Microsoft associada e selecione o nome do serviço **Azure NetApp Files** em **armazenamento**. Forneça as informações restantes necessárias para criar sua solicitação de suporte da Microsoft.

Para problemas relacionados ao Cloud Sync e ao Azure NetApp Files, você pode começar com o NetApp usando o número de série do Cloud Sync diretamente do serviço Cloud Sync. Você precisará acessar o serviço Cloud Sync por meio do link no Cloud Manager. "Visualize o processo para ativar o suporte ao Cloud Sync".

Links relacionados

- "Centro de nuvem NetApp: Azure NetApp Files"
- "Documentação do Azure NetApp Files"
- "Documentação do Cloud Sync"

Configurar o Azure NetApp Files

Crie um ambiente de trabalho do Azure NetApp Files no Cloud Manager para criar e gerenciar contas, pools de capacidade, volumes e snapshots do NetApp.

Início rápido

Comece rapidamente seguindo estas etapas ou role para baixo até as seções restantes para obter detalhes completos.

Solicitar acesso

"Envie uma solicitação on-line" Para ser concedido acesso ao Azure NetApp Files.

Configurar uma aplicação Azure AD

No Azure, conceda permissões a um aplicativo do Azure AD e copie o ID do aplicativo (cliente), o ID do diretório (locatário) e o valor de um segredo do cliente.

Crie um ambiente de trabalho Azure NetApp Files

No Cloud Manager, clique em **Adicionar ambiente de trabalho** > **Microsoft Azure** > **Azure NetApp Files** e, em seguida, forneça detalhes sobre o aplicativo AD.

A solicitar acesso

Você precisa ter acesso ao Azure NetApp Files por "enviando uma solicitação on-line". Você precisará esperar pela aprovação da equipe do Azure NetApp Files antes de prosseguir.

Configurando um aplicativo do Azure AD

O Cloud Manager precisa de permissões para configurar e gerenciar o Azure NetApp Files. Você pode conceder as permissões necessárias a uma conta do Azure criando e configurando um aplicativo do Azure AD e obtendo as credenciais do Azure necessárias para o Cloud Manager.

Criando o aplicativo AD

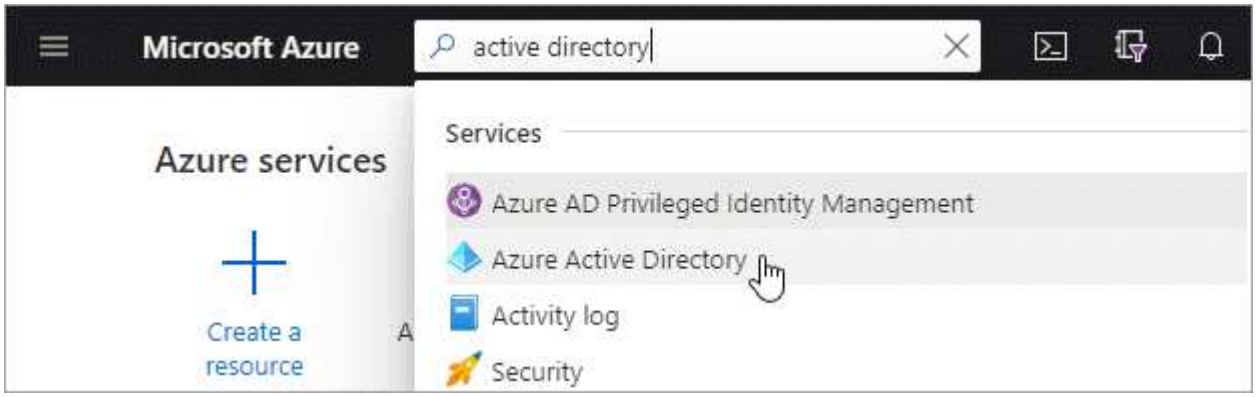
Crie um aplicativo e um diretor de serviço do Azure ative Directory (AD) que o Cloud Manager pode usar para controle de acesso baseado em funções.

Antes de começar

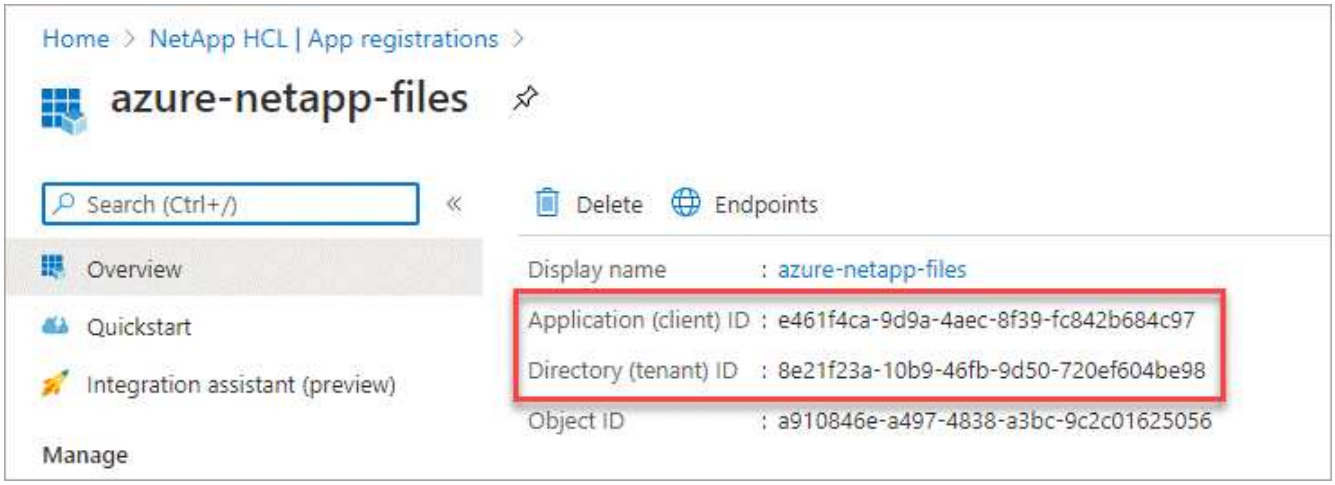
Você deve ter as permissões certas no Azure para criar um aplicativo do ative Directory e atribuir o aplicativo a uma função. Para obter detalhes, "Documentação do Microsoft Azure: Permissões necessárias" consulte .

Passos

1. No portal do Azure, abra o serviço **Azure ative Directory**.



2. No menu, clique em **inscrições de aplicativos**.
3. Crie a aplicação:
   a. Clique em **novo registo**.
   b. Especifique detalhes sobre o aplicativo:
      - **Nome**: Insira um nome para o aplicativo.
      - **Tipo de conta**: Selecione um tipo de conta (qualquer funcionará com o Cloud Manager).
      - * URI de redirecionamento*: Você pode deixar isso em branco.
   c. Clique em **Register**.
4. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.



Ao criar o ambiente de trabalho do Azure NetApp Files no Cloud Manager, você precisa fornecer o ID do

aplicativo (cliente) e o ID do diretório (locatário) para o aplicativo. O Cloud Manager usa as IDs para fazer login programaticamente.

5. Crie um segredo de cliente para o aplicativo para que o Cloud Manager possa usá-lo para autenticar com o Azure AD:
   a. Clique em **certificados e segredos > segredo de novo cliente**.
   b. Forneça uma descrição do segredo e uma duração.
   c. Clique em **Add**.
   d. Copie o valor do segredo do cliente.

Resultado

Seu aplicativo AD agora está configurado e você deve ter copiado o ID do aplicativo (cliente), o ID do diretório (locatário) e o valor do segredo do cliente. Você precisa inserir essas informações no Cloud Manager quando você adiciona um ambiente de trabalho do Azure NetApp Files.

Atribuindo o aplicativo a uma função

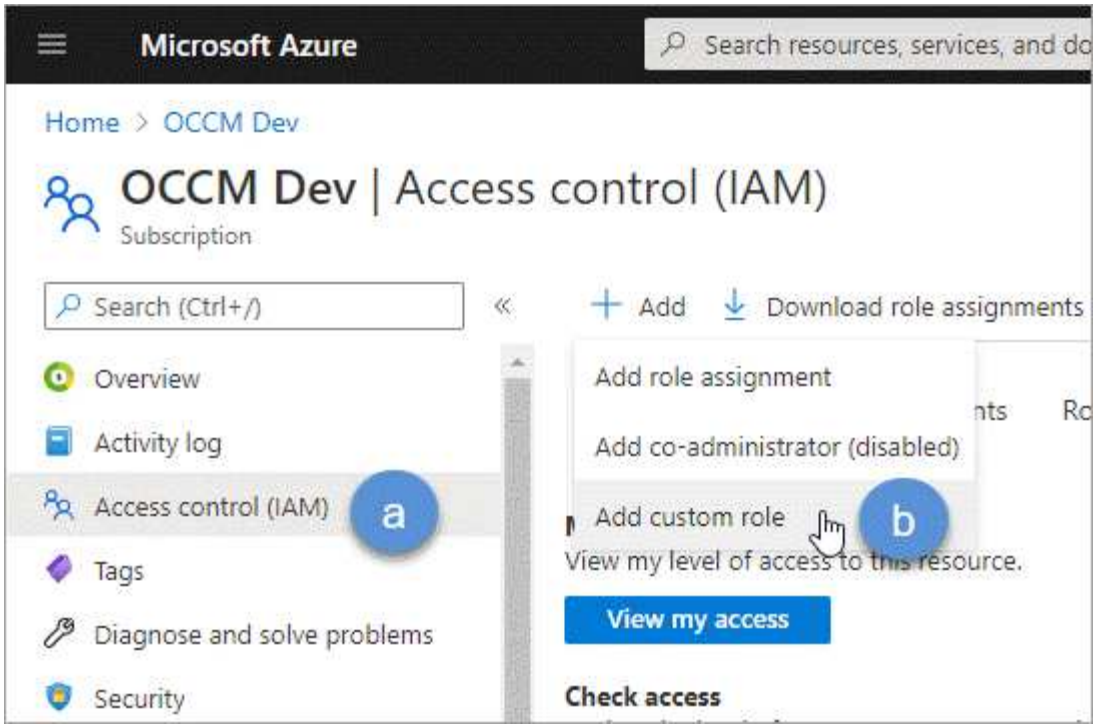
Você deve vincular o principal de serviço à sua assinatura do Azure e atribuir-lhe uma função personalizada que tenha as permissões necessárias.

Passos

1. "Crie uma função personalizada no Azure".

   As etapas a seguir descrevem como criar a função do portal do Azure.

   a. Abra a assinatura e clique em **Access Control (IAM)**.
   b. Clique em **Adicionar > Adicionar função personalizada**.



c. Na guia **Basics**, insira um nome e uma descrição para a função.

d. Clique em **JSON** e clique em **Edit** que aparece no canto superior direito do formato JSON.

e. Adicione as seguintes permissões em *ações*:

```
"actions": [
    "Microsoft.NetApp/*",
    "Microsoft.Resources/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Insights/Metrics/Read"
    ],
```

f. Clique em **Salvar**, clique em **Avançar** e, em seguida, clique em **criar**.

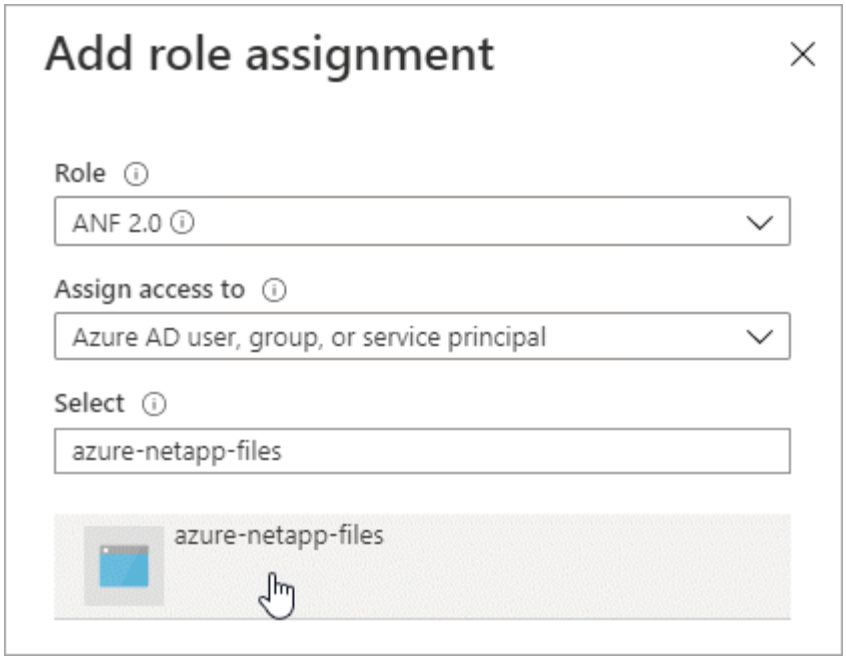
2. Agora atribua o aplicativo à função que você acabou de criar:

a. No portal do Azure, abra a subscrição e clique em **controlo de acesso (IAM) > Adicionar > Adicionar atribuição de função**.

b. Selecione a função personalizada que você criou.

c. Mantenha **Usuário, grupo ou responsável de serviço do Azure AD** selecionado.

d. Procure o nome do aplicativo (você não pode encontrá-lo na lista rolando).



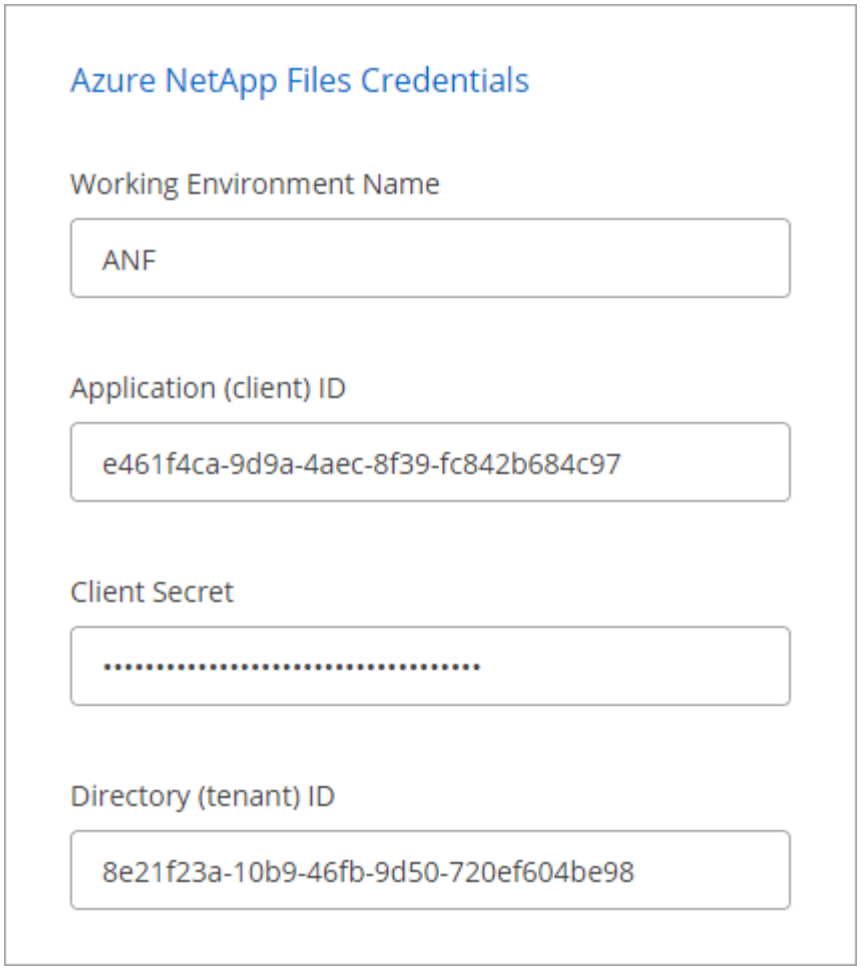
e. Selecione o aplicativo e clique em **Salvar**.

   O responsável de serviço do Cloud Manager agora tem as permissões necessárias do Azure para essa assinatura.

Criando um ambiente de trabalho Azure NetApp Files

Configure um ambiente de trabalho do Azure NetApp Files no Cloud Manager para começar a criar volumes.

1. Na página ambientes de trabalho, clique em **Adicionar ambiente de trabalho**.
2. Selecione **Microsoft Azure** e, em seguida, **Azure NetApp Files**.
3. Forneça detalhes sobre o aplicativo AD que você configurou anteriormente.



4. Clique em **Add**.

Resultado

Agora você deve ter um ambiente de trabalho Azure NetApp Files.

O que se segue?

"Comece a criar e gerenciar volumes".

Criação e gerenciamento de volumes para Azure NetApp Files

Depois de configurar seu ambiente de trabalho, você pode criar e gerenciar contas do Azure NetApp Files, pools de capacidade, volumes e snapshots.

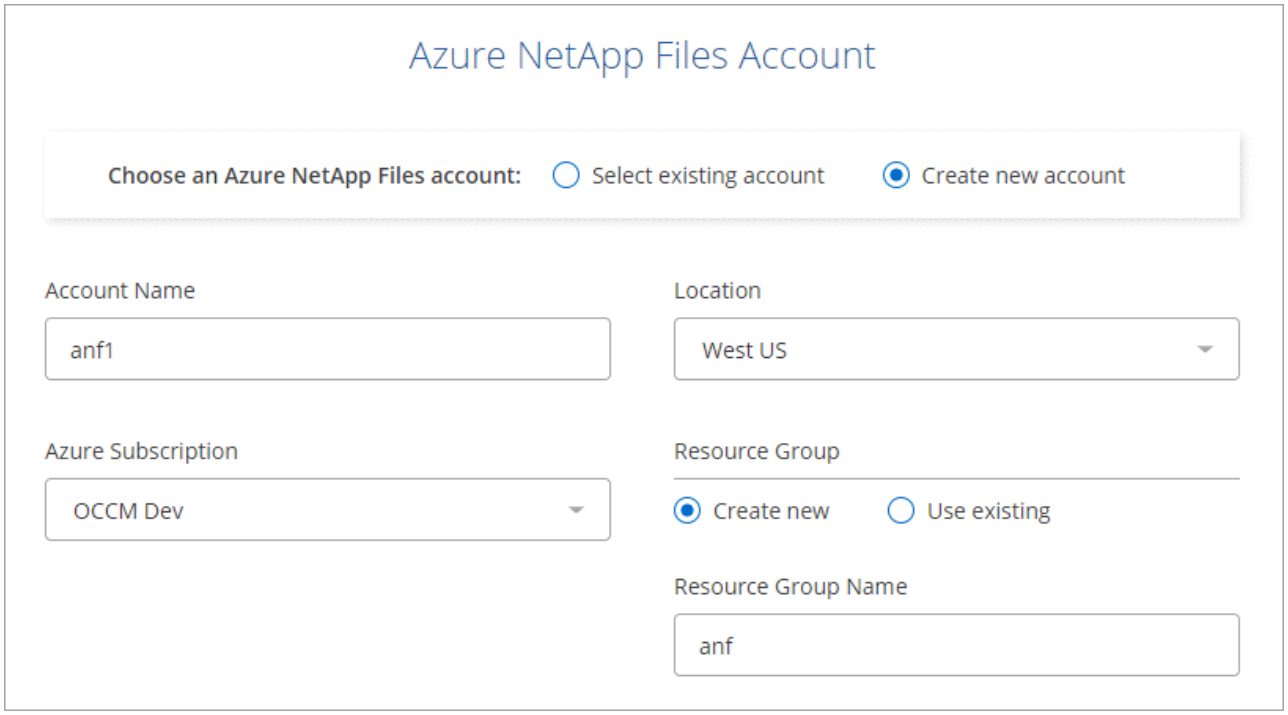
Criando volumes

Você pode criar volumes NFS ou SMB em uma conta do Azure NetApp Files nova ou existente.

Passos

1. Abra o ambiente de trabalho do Azure NetApp Files.
2. Clique em **Adicionar novo volume**.
3. Forneça as informações necessárias em cada página:

   - **Conta Azure NetApp Files**: Escolha uma conta Azure NetApp Files existente ou crie uma nova conta.



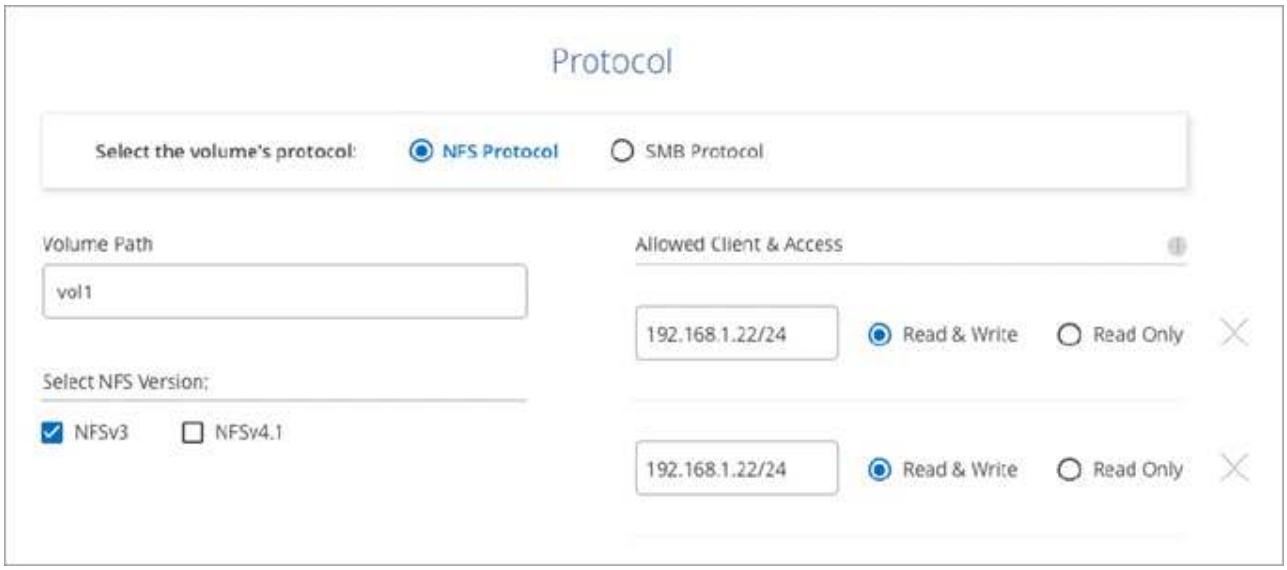
   - **Pool de capacidade**: Selecione um pool de capacidade existente ou crie um novo pool de capacidade.

     Se você criar um novo pool de capacidade, precisará especificar um tamanho e selecionar um "nível de serviço".

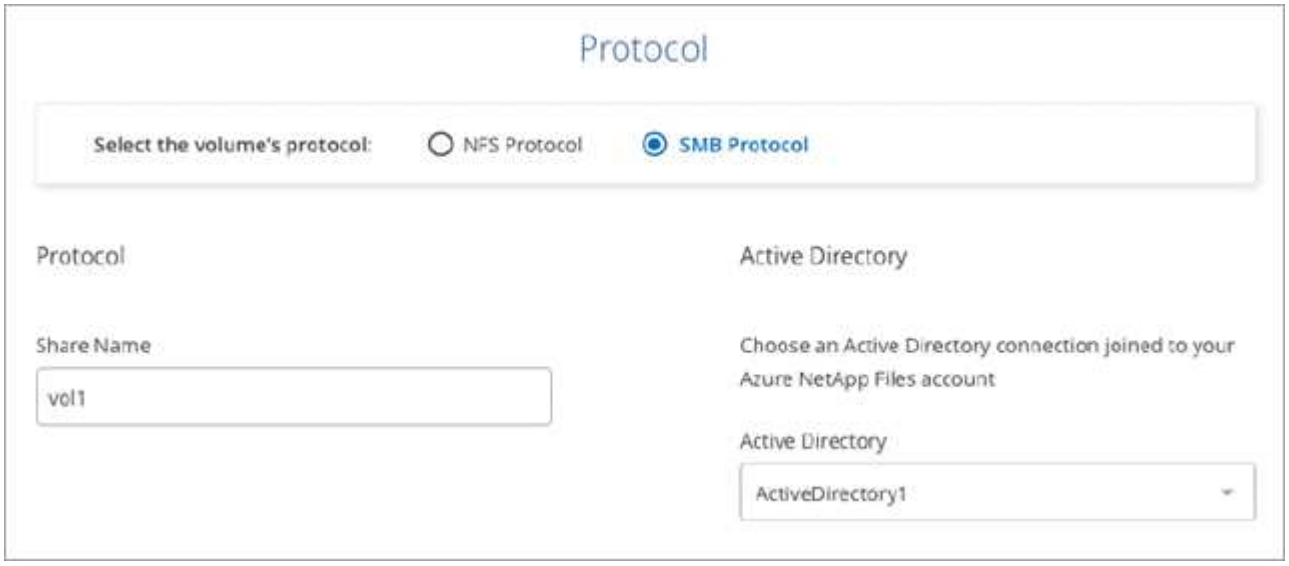
     O tamanho mínimo para o pool de capacidade é de 4 TB. Você pode especificar um tamanho em múltiplos de 4 TB.

   - **Detalhes e Tags**: Insira um nome e tamanho de volume, o VNet e a sub-rede onde o volume deve residir e, opcionalmente, especifique tags para o volume.
   - **Protocolo**: Escolha o protocolo NFS ou SMB e insira as informações necessárias.

     Aqui está um exemplo de detalhes para NFS.



Aqui está um exemplo de detalhes para SMB. Você precisará fornecer informações do ative Directory ao configurar seu primeiro volume SMB.



4. Clique em **Adicionar volume**.

Volumes de montagem

Acesse as instruções de montagem do Cloud Manager para que você possa montar o volume em um host.

Passos

1. Abra o ambiente de trabalho.
2. Passe o Mouse sobre o volume e selecione **Monte o volume**.

3. Siga as instruções para montar o volume.

Editando o tamanho e as tags de um volume

Depois de criar um volume, você pode modificar seu tamanho e tags a qualquer momento.

Passos

1. Abra o ambiente de trabalho.
2. Passe o Mouse sobre o volume e selecione **Editar**.
3. Modifique o tamanho e as tags conforme necessário.
4. Clique em **aplicar**.

Gerenciamento de cópias Snapshot

As cópias Snapshot fornecem uma cópia pontual do volume. Criar cópias Snapshot, restaurar os dados para um novo volume e excluir cópias Snapshot.

Passos

1. Abra o ambiente de trabalho.
2. Passe o Mouse sobre o volume e escolha uma das opções disponíveis para gerenciar cópias Snapshot:
   - **Criar uma cópia Snapshot**
   - **Restaurar para um novo volume**
   - **Excluir uma cópia Snapshot**
3. Siga as instruções para concluir a ação selecionada.

Eliminar volumes

Exclua os volumes que você não precisa mais.

Passos

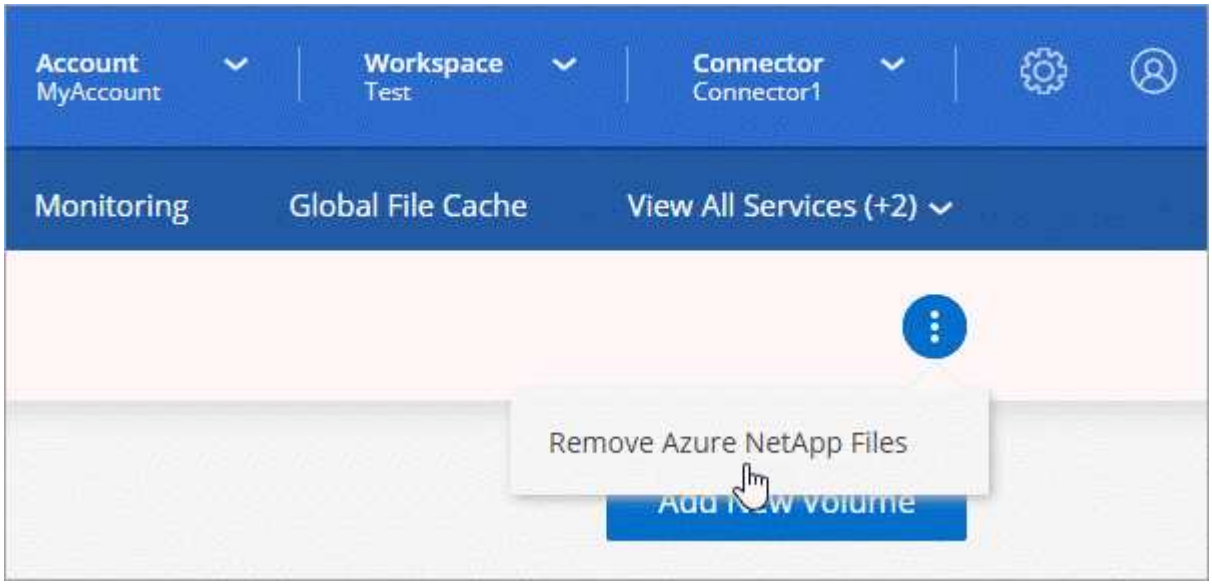
1. Abra o ambiente de trabalho.
2. Passe o Mouse sobre o volume e clique em **Excluir**.
3. Confirme se pretende eliminar o volume.

A remover Azure NetApp Files

Essa ação remove o Azure NetApp Files do Cloud Manager. Ele não exclui sua conta ou volumes do Azure NetApp Files. Você pode adicionar o Azure NetApp Files de volta ao Cloud Manager a qualquer momento.

Passos

1. Abra o ambiente de trabalho do Azure NetApp Files.
2. No canto superior direito da página, selecione o menu ações e clique em **Remover Azure NetApp Files**.



3. Clique em **Remover** para confirmar.

Cloud Volumes Service para AWS

Saiba mais sobre o Cloud Volumes Service para AWS

O NetApp Cloud Volumes Service para AWS é um serviço de arquivos nativo da nuvem que fornece volumes nas em NFS e SMB com performance all-flash. Esse serviço permite que qualquer workload, incluindo aplicações legadas, seja executado na nuvem do AWS.

Benefícios do uso do Cloud Volumes Service para AWS

O Cloud Volumes Service para AWS oferece os seguintes benefícios:

- Serviço totalmente gerenciado, portanto, não há necessidade de configurar ou gerenciar dispositivos de armazenamento
- Suporte para protocolos nas NFSv3 e NFSv4,1 e SMB 3,0 e 3.1.1
- Acesso seguro a instâncias do Linux e do Windows Elastic Container Service (ECS), com suporte incluindo o seguinte:
  - Amazon Linux 2, Red Hat Enterprise Linux 7,5, SLES 12 SP3 e Ubuntu 16,04 LTS
  - Windows Server 2008 R2, Windows Server 2012 R2 e Windows Server 2016
- Opções de preços com pacote e pagamento conforme o uso

Custo

Os volumes criados pelo Cloud Volumes Service para AWS são cobrados com base na sua subscrição do serviço, não pelo Cloud Manager.

Não há cobrança para descobrir uma região ou volume do Cloud Volumes Service para AWS a partir do Cloud Manager.

Antes de começar

- O Cloud Manager pode descobrir assinaturas e volumes existentes do Cloud Volumes Service para AWS. Consulte o "Guia de configuração da conta do NetApp Cloud Volumes Service para AWS" se ainda não tiver configurado a sua subscrição. Siga esse processo de configuração para cada região antes de adicionar as assinaturas e os volumes da AWS no Cloud Manager.
- Você precisa obter a chave da API do Cloud volumes e a chave secreta para fornecê-los ao Cloud Manager. "Para obter instruções, consulte a documentação do Cloud Volumes Service para AWS".

Início rápido

Comece rapidamente seguindo estes passos ou vá para a próxima secção para obter detalhes completos.

Verifique o suporte para sua configuração

Você configurou o AWS para Cloud Volumes Service e deve se inscrever em um dos "Ofertas do NetApp Cloud Volumes Service no AWS Marketplace".

Adicione sua assinatura do Cloud Volumes Service para AWS

Você precisa criar um ambiente de trabalho para os volumes com base na assinatura do Cloud Volumes Service para AWS.

Criar um Cloud volumes

Os volumes de nuvem que já existem para essa assinatura aparecem no novo ambiente de trabalho. Caso contrário, você cria novos volumes a partir do Cloud Manager.

Montar um volume de nuvem

Monte novos volumes de nuvem na instância da AWS para que os usuários possam começar a usar o storage.

Obter ajuda

Use o chat do Cloud Manager para perguntas gerais de serviço.

Para problemas de suporte técnico associados aos volumes da nuvem, use o número de série "930" de 20 dígitos localizado na guia "suporte" da interface de usuário do Cloud Volumes Service. Use esse ID de suporte ao abrir um ticket da Web ou chamar suporte. Certifique-se de ativar o número de série do Cloud Volumes

Service para obter suporte a partir da interface de usuário do Cloud Volumes Service. "Esses passos são explicados aqui".

Limitações

- O Cloud Manager não é compatível com a replicação de dados entre ambientes de trabalho ao usar o Cloud Volumes Service volumes.
- A remoção da assinatura do Cloud Volumes Service para AWS do Cloud Manager não é suportada. Você pode fazer isso somente por meio da interface do Cloud Volumes Service para AWS.

Links relacionados

- "Centro de nuvem da NetApp: Cloud Volumes Service para AWS"
- "Documentação do NetApp Cloud Volumes Service para AWS"

Gerenciamento do Cloud Volumes Service para AWS

Com o Cloud Manager, você cria volumes de nuvem com base na "Cloud Volumes Service para AWS" sua subscrição. Também é possível descobrir os volumes de nuvem que você já criou a partir da interface do Cloud Volumes Service e adicioná-los a um ambiente de trabalho.

Adicione sua assinatura do Cloud Volumes Service para AWS

Independentemente de você já ter criado volumes a partir da interface de usuário do Cloud Volumes Service ou se você acabou de se inscrever no Cloud Volumes Service para AWS e ainda não tiver volumes, a primeira etapa é criar um ambiente de trabalho para os volumes com base na assinatura da AWS.

Se o Cloud volumes já existir para essa assinatura, os volumes serão adicionados automaticamente ao novo ambiente de trabalho. Se você ainda não adicionou nenhum volume de nuvem para a assinatura da AWS, faça isso depois de criar o novo ambiente de trabalho.

Se você tiver assinaturas e volumes em várias regiões da AWS, precisará executar essa tarefa para cada região.

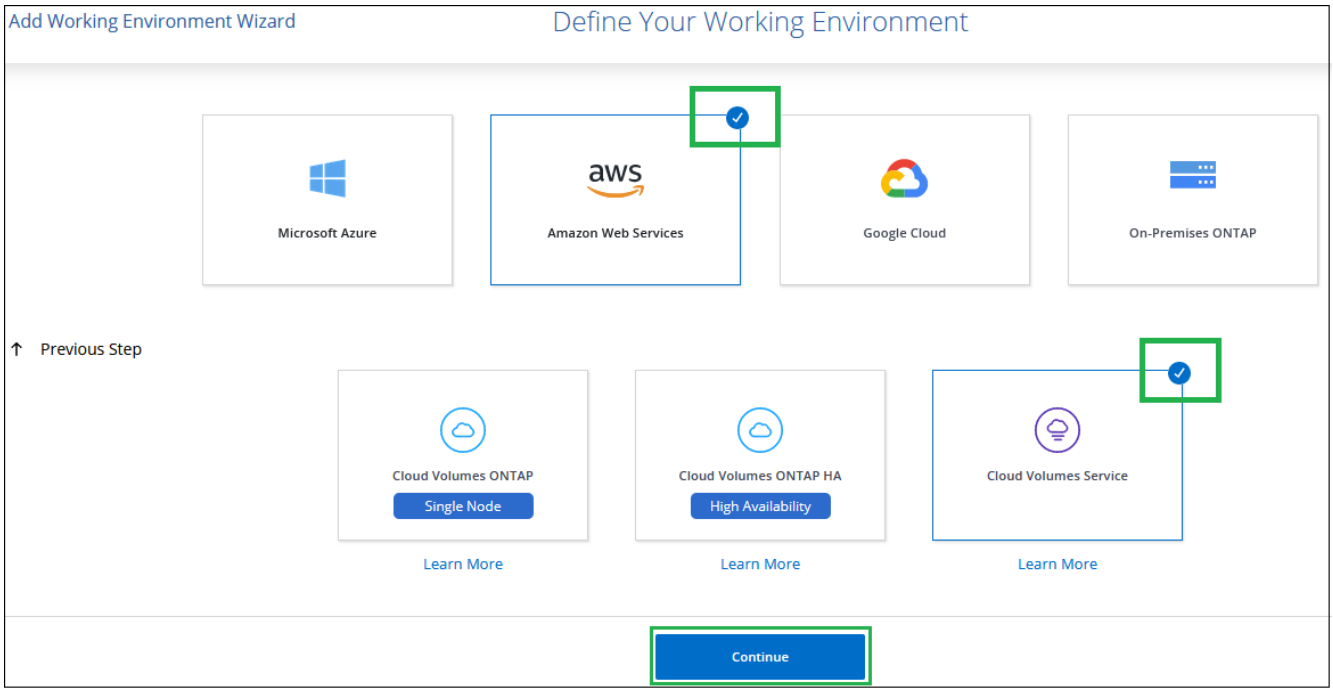
Antes de começar

Você deve ter as seguintes informações disponíveis ao adicionar uma assinatura em cada região:

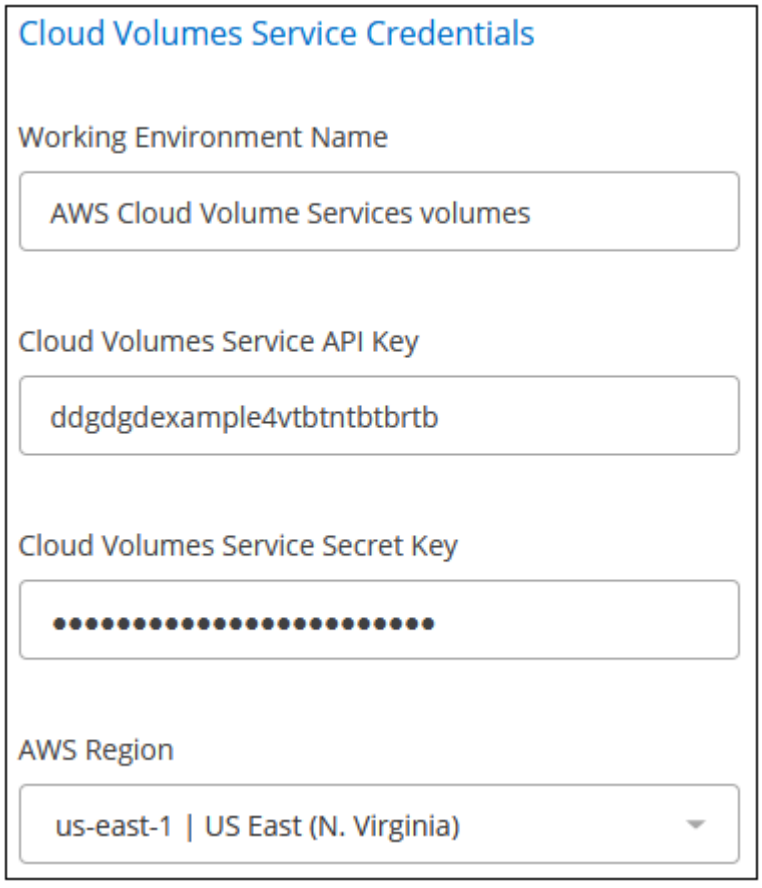
- Chave da API do Cloud volumes e chave secreta: "Consulte a documentação do Cloud Volumes Service para AWS para obter essas informações".
- A região da AWS onde a assinatura foi criada.

Passos

1. No Cloud Manager, adicione um novo ambiente de trabalho, selecione o local **Amazon Web Services** e clique em **continuar**.
2. Selecione **Cloud Volumes Service** e clique em **continuar**.



3. Forneça informações sobre sua assinatura do Cloud Volumes Service:
   a. Introduza o nome do ambiente de trabalho que pretende utilizar.
   b. Insira a chave da API do Cloud Volumes Service e a chave secreta.
   c. Selecione a região da AWS onde residem seus volumes de nuvem ou onde serão implantados.
   d. Clique em **Add**.



Resultado

O Cloud Manager exibe a configuração do Cloud Volumes Service para AWS na página ambientes de trabalho.

Se o Cloud volumes já existir para essa assinatura, os volumes serão adicionados automaticamente ao novo ambiente de trabalho, como mostra a captura de tela. Você pode adicionar volumes de nuvem adicionais do Cloud Manager.

Se não houver volumes de nuvem para essa assinatura, você pode criá-los agora.

Criar o Cloud volumes

Para configurações em que os volumes já existem no ambiente de trabalho do Cloud Volumes Service, siga estas etapas para adicionar novos volumes.

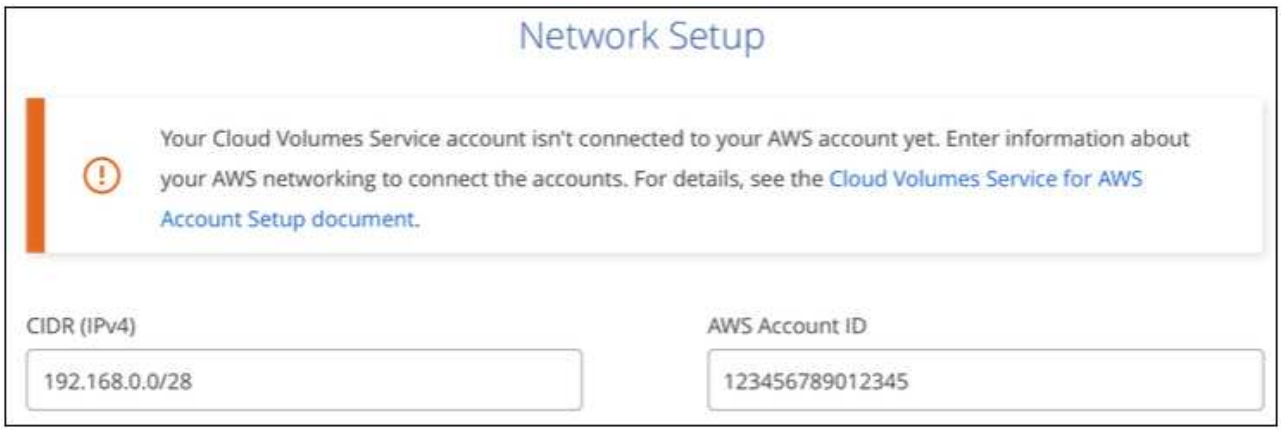
Para configurações onde não existem volumes, você pode criar seu primeiro volume diretamente no Cloud Manager depois de configurar a assinatura do Cloud Volumes Service para AWS. No passado, o primeiro volume tinha que ser criado diretamente na interface de usuário do Cloud Volumes Service.

Antes de começar

- Se você quiser usar o SMB na AWS, você deve ter configurado o DNS e o ative Directory.
- Ao Planejar criar um volume SMB, você deve ter um servidor do Windows ative Directory disponível para o qual você pode se conetar. Você inserirá essas informações ao criar o volume. Além disso, certifique-se de que o usuário Admin é capaz de criar uma conta de máquina no caminho da unidade organizacional (ou) especificado.
- Você precisará dessas informações ao criar o primeiro volume em uma nova região/ambiente de trabalho:
  - ID de conta da AWS: Um identificador de conta da Amazon de 12 dígitos sem traços. Para encontrar o ID da sua conta, consulte este "Tópico da AWS".
  - Bloco CIDR (Roteamento entre domínios sem classes): Um bloco CIDR IPv4 não utilizado. O prefixo da rede deve variar entre /16 e /28, e também deve estar dentro dos intervalos reservados para redes privadas (RFC 1918). Não escolha uma rede que sobreponha suas alocações CIDR da VPC.

Passos

1. Selecione o novo ambiente de trabalho e clique em **Adicionar novo volume**.
2. Se você estiver adicionando o primeiro volume ao ambiente de trabalho na região, será necessário adicionar informações de rede da AWS.
   a. Introduza o intervalo IPv4 (CIDR) para a região.
   b. Insira o ID da conta da AWS de 12 dígitos (sem traços) para conectar sua conta do Cloud volumes à sua conta da AWS.
   c. Clique em **continuar**.



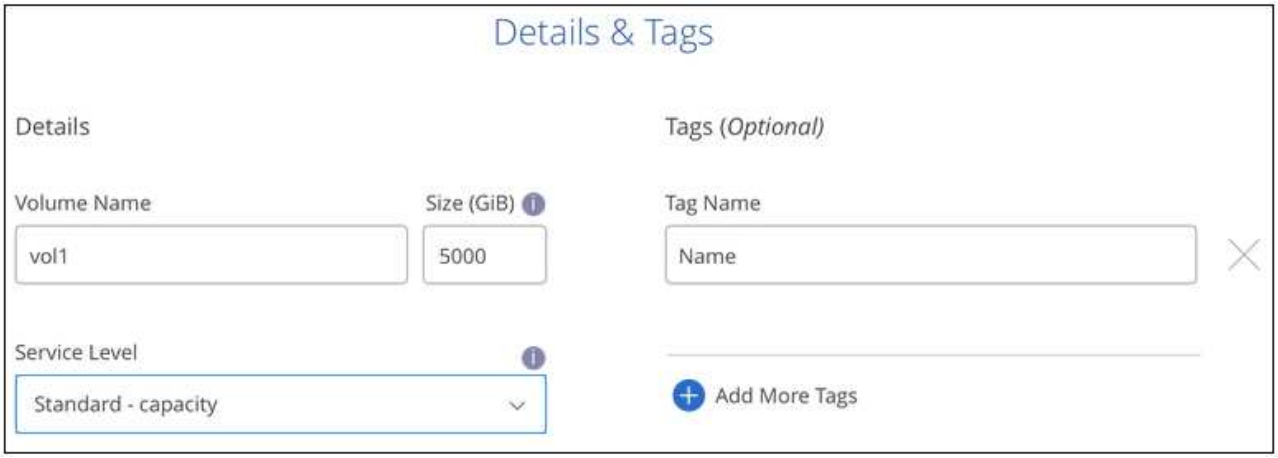
3. A página aceitar interfaces virtuais descreve algumas etapas que você precisará executar depois de adicionar o volume para que você esteja preparado para concluir essa etapa. Basta clicar em **continuar** novamente.
4. Na página Detalhes e etiquetas, introduza os detalhes sobre o volume:
   a. Introduza um nome para o volume.
   b. Especifique um tamanho dentro do intervalo de 100 GiB a 90.000 GiB (equivalente a 88 Tibs).

      "Saiba mais sobre a capacidade alocada".

   c. Especifique um nível de serviço: Standard, Premium ou Extreme.

      "Saiba mais sobre os níveis de serviço".

   d. Introduza um ou mais nomes de etiquetas para categorizar o volume, se pretender.
   e. Clique em **continuar**.



5. Na página Protocolo, selecione NFS, SMB ou Dual Protocol e, em seguida, defina os detalhes. As entradas necessárias para NFS e SMB são mostradas em seções separadas abaixo.
6. No campo caminho do volume , especifique o nome da exportação de volume que você verá quando montar o volume.
7. Se selecionar Dual-Protocol (protocolo duplo), pode selecionar o estilo de segurança selecionando NTFS ou UNIX. Os estilos de segurança afetam o tipo de permissão de arquivo usado e como as permissões podem ser modificadas.

- O UNIX usa bits de modo NFSv3 e somente clientes NFS podem modificar permissões.
- NTFS usa ACLs NTFS e somente clientes SMB podem modificar permissões.

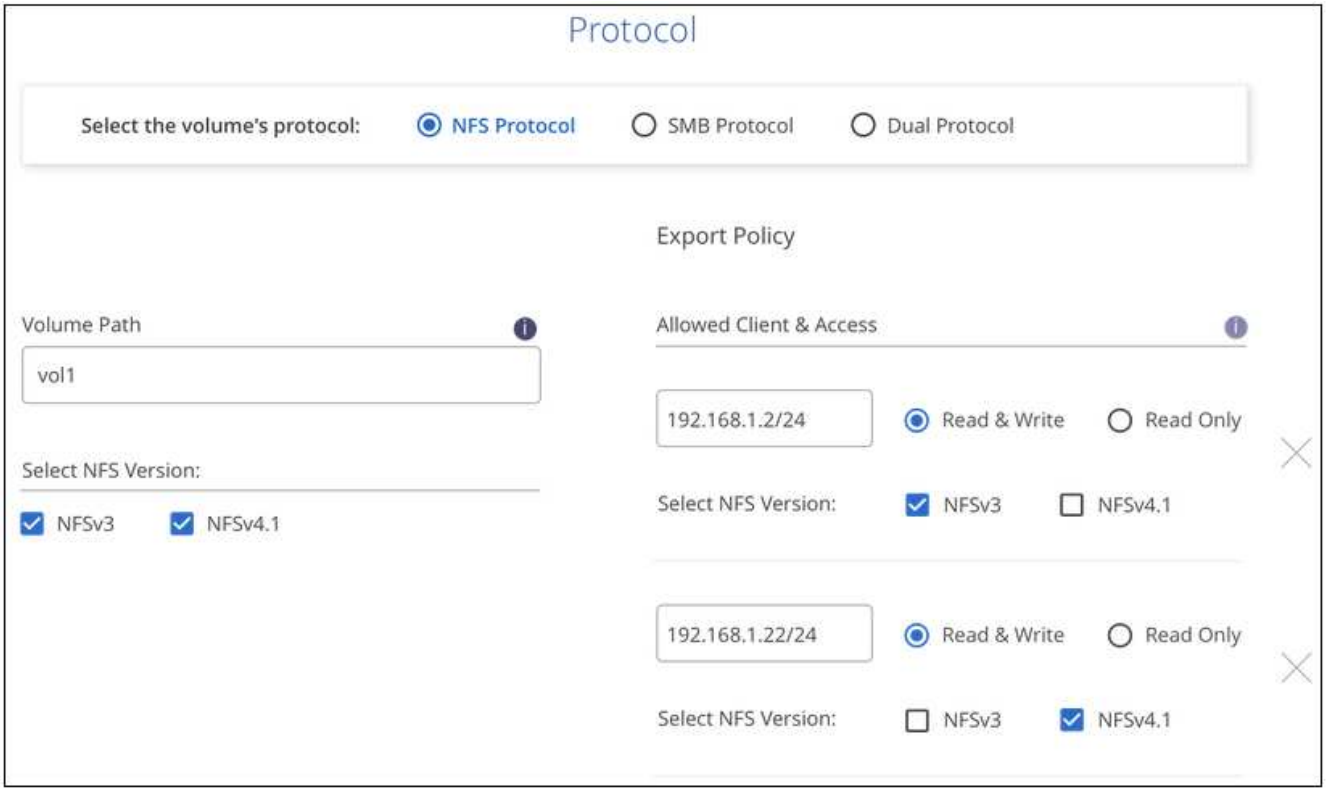
8. Para NFS:

   a. No campo versão NFS, selecione NFSv3, NFSv4,1 ou ambos, dependendo dos seus requisitos.

   b. Opcionalmente, você pode criar uma política de exportação para identificar os clientes que podem acessar o volume. Especifique:

      - Clientes permitidos usando um endereço IP ou CIDR (Classless Inter-Domain Routing).
      - Direitos de acesso como somente leitura e gravação ou leitura.
      - Protocolo de acesso (ou protocolos se o volume permitir o acesso NFSv3 e NFSv4,1) utilizado para os utilizadores.
      - Clique em Adicionar regra de política de exportação* se quiser definir regras de política de exportação adicionais.

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



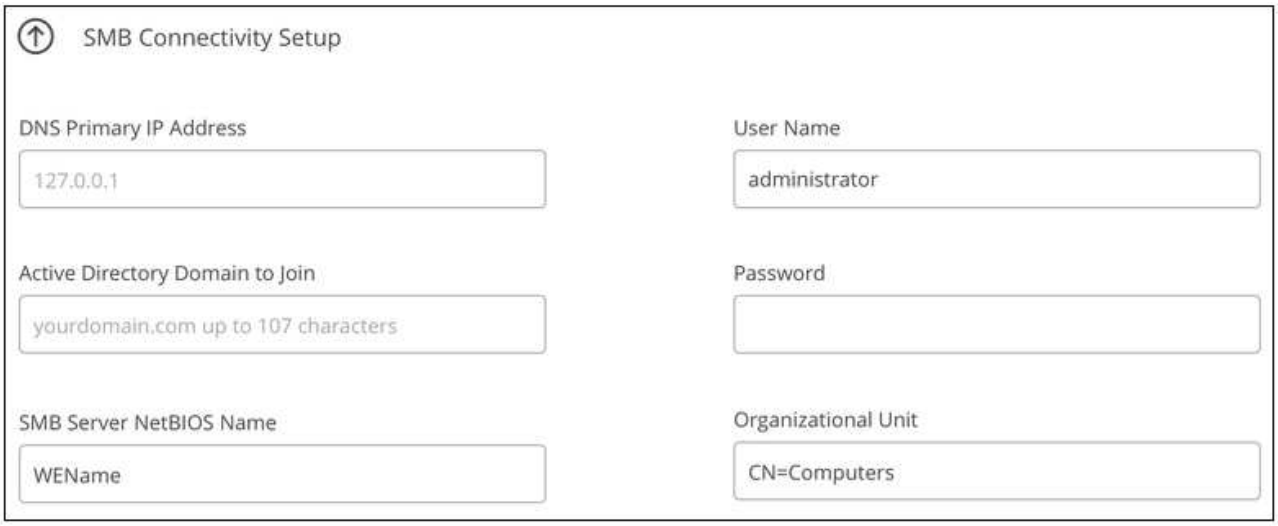
9. Para SMB:

   a. Pode ativar a encriptação de sessão SMB marcando a caixa para encriptação de protocolo SMB.

   b. Você pode integrar o volume com um servidor Windows ative Directory existente preenchendo os campos na seção ative Directory:

Campo	Descrição
Endereço IP primário do DNS	Os endereços IP dos servidores DNS que fornecem resolução de nomes para o servidor SMB. Use uma vírgula para separar os endereços IP ao fazer referência a vários servidores, por exemplo, 172.31.25.223, 172.31.2.74.
Ative Directory Domain para aderir	O FQDN do domínio do ative Directory (AD) ao qual você deseja que o servidor SMB se associe. Ao usar o AWS Managed Microsoft AD, use o valor do campo "Directory DNS name".
Nome NetBIOS do servidor SMB	Um nome NetBIOS para o servidor SMB que será criado.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores à unidade organizacional especificada (ou) dentro do domínio do AD.
Unidade organizacional	A unidade organizacional dentro do domínio AD a associar ao servidor SMB. A predefinição é computadores para ligações ao seu próprio servidor Windows ative Directory. Se você configurar o AWS Managed Microsoft AD como o servidor AD para o Cloud Volumes Service, deverá inserir neste campo **ou computadores**.

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



Você deve seguir as orientações sobre as configurações do grupo de segurança da AWS para permitir que o Cloud volumes se integre corretamente aos servidores do Windows ative Directory. Consulte "Configurações do grupo de segurança da AWS para servidores Windows AD" para obter mais informações.

10. Na página volume a partir de instantâneo, se você quiser que esse volume seja criado com base em um instantâneo de um volume existente, selecione o instantâneo na lista suspensa Nome do instantâneo.
11. Na página Política de Snapshot, é possível habilitar o Cloud Volumes Service a criar cópias snapshot de seus volumes com base em uma programação. Pode fazê-lo agora ou editar o volume mais tarde para definir a política de instantâneos.

    Consulte "Criando uma política de snapshot" para obter mais informações sobre a funcionalidade de instantâneos.

12. Clique em **Adicionar volume**.

O novo volume é adicionado ao ambiente de trabalho.

Depois de terminar

Se esse for o primeiro volume criado nessa assinatura da AWS, será necessário iniciar o Console de Gerenciamento da AWS para aceitar as duas interfaces virtuais que serão usadas nessa região da AWS para conetar todos os volumes da nuvem. Consulte "Guia de configuração da conta do NetApp Cloud Volumes Service para AWS" para obter detalhes.

Você deve aceitar as interfaces dentro de 10 minutos depois de clicar no botão **Adicionar volume** ou o sistema pode acabar. Se isso acontecer, envie um e-mail para cvs-support NetApp.com com com sua ID de cliente da AWS e número de série do NetApp. O suporte corrigirá o problema e você poderá reiniciar o processo de integração.

Em seguida, continue com "Montagem do volume de nuvem".

Montar o volume de nuvem

Você pode montar um volume de nuvem na instância da AWS. Atualmente, o Cloud volumes suporta NFSv3 e NFSv4,1 para clientes Linux e UNIX e SMB 3,0 e 3.1.1 para clientes Windows.

Nota: por favor, use o protocolo/dialeto destacado suportado pelo seu cliente.

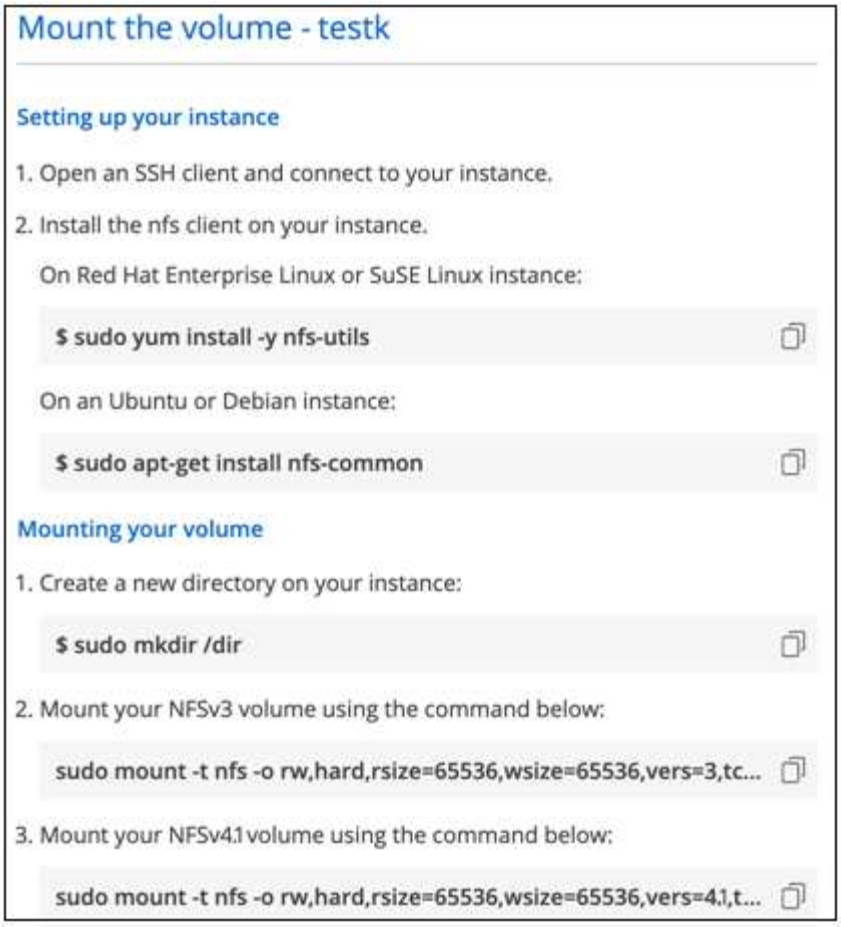
Passos

1. Abra o ambiente de trabalho.
2. Passe o Mouse sobre o volume e clique em **Monte o volume**.

   Os volumes NFS e SMB exibem instruções de montagem para esse protocolo. Os volumes de protocolo duplo fornecem ambos os conjuntos de instruções.

3. Passe o Mouse sobre os comandos e copie-os para a área de transferência para facilitar este processo. Basta adicionar o diretório de destino/ponto de montagem no final do comando.

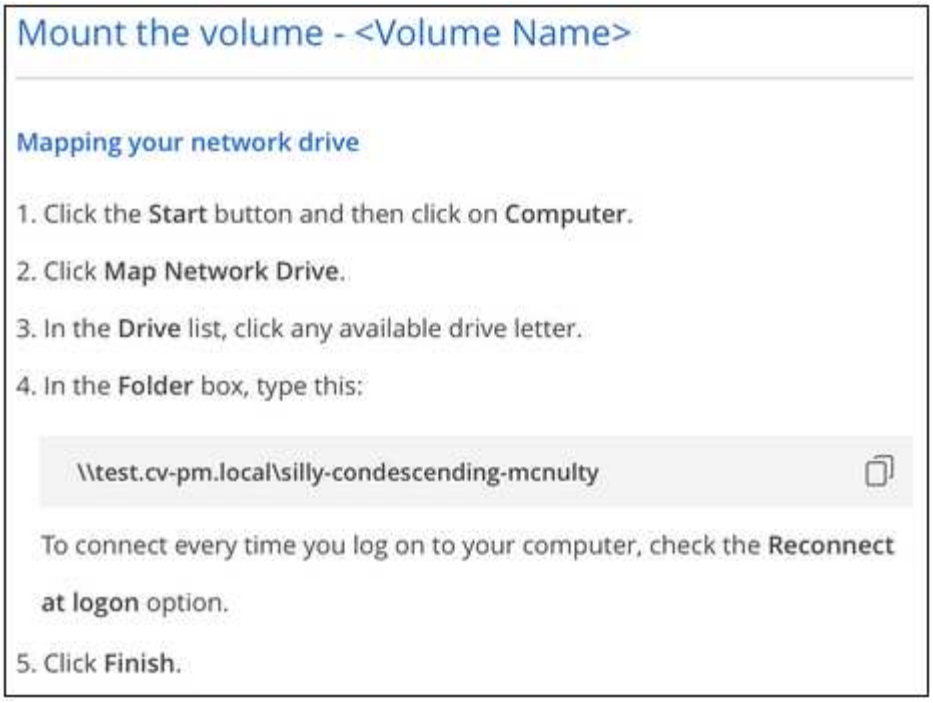
   Exemplo de NFS:



O tamanho máximo de e/S definido `rsize` pelas opções e `wsize` é 1048576, no entanto, 65536 é o padrão recomendado para a maioria dos casos de uso.

Observe que os clientes Linux serão padrão para NFSv4,1, a menos que a versão seja especificada com a `vers=<nfs_version>` opção.

Exemplo SMB:



4. Conete-se à instância do Amazon Elastic Compute Cloud (EC2) usando um cliente SSH ou RDP e siga as instruções de montagem da instância.

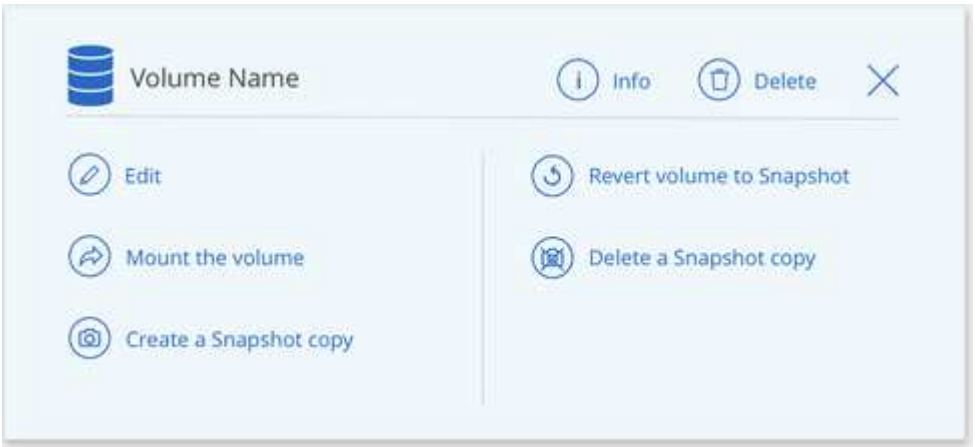
   Depois de concluir as etapas nas instruções de montagem, você montou com sucesso o volume da nuvem na sua instância da AWS.

Gerenciamento de volumes existentes

Você pode gerenciar volumes existentes conforme suas necessidades de storage mudam. Você pode exibir, editar, restaurar e excluir volumes.

Passos

1. Abra o ambiente de trabalho.
2. Passe o Mouse sobre o volume.



3. Gerencie seus volumes:

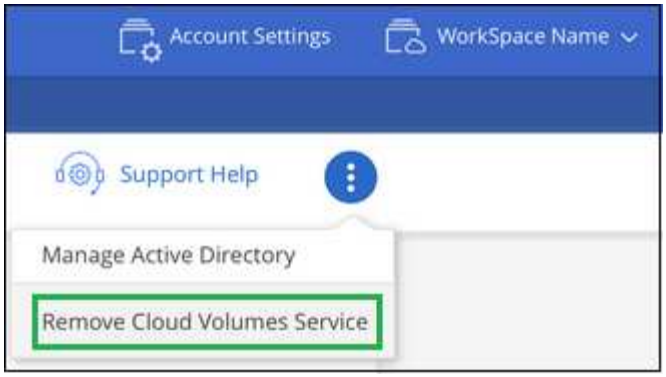
Tarefa	Ação
Exibir informações sobre um volume	Selecione um volume e clique em **Info**.
Editar um volume (incluindo política de instantâneos)	a. Selecione um volume e clique em **Editar**. b. Modifique as propriedades do volume e clique em **Update**.
Obtenha o comando de montagem NFS ou SMB	a. Selecione um volume e clique em **montar o volume**. b. Clique em **Copy** para copiar o(s) comando(s).
Criar uma cópia Snapshot sob demanda	a. Selecione um volume e clique em **criar uma cópia Snapshot**. b. Altere o nome do instantâneo, se necessário, e clique em **criar**.
Substitua o volume pelo conteúdo de uma cópia Snapshot	a. Selecione um volume e clique em **Reverter volume para Instantâneo**. b. Selecione uma cópia Snapshot e clique em **Revert**.
Excluir uma cópia Snapshot	a. Selecione um volume e clique em **Excluir uma cópia Snapshot**. b. Selecione a cópia Snapshot que deseja excluir e clique em **Excluir**. c. Clique em **Delete** novamente para confirmar.
Eliminar um volume	a. Desmonte o volume de todos os clientes: ◦ Em clientes Linux, use o `umount` comando. ◦ Em clientes Windows, clique em **Disconnect network drive**. b. Selecione um volume e, em seguida, clique em **Delete**. c. Clique em **Delete** novamente para confirmar.

Remova o Cloud Volumes Service do Cloud Manager

Você pode remover uma assinatura do Cloud Volumes Service para AWS e todos os volumes existentes do Cloud Manager. Os volumes não são excluídos. Eles acabaram de ser removidos da interface do Cloud Manager.

Passos

1. Abra o ambiente de trabalho.



2. Clique no botão na parte superior da página e clique em **Remover Cloud Volumes Service**.
3. Na caixa de diálogo de confirmação, clique em **Remover**.

Gerenciar a configuração do ative Directory

Se você alterar seus servidores DNS ou domínio do ative Directory, precisará modificar o servidor SMB no Cloud volumes Services para que ele possa continuar fornecendo storage aos clientes.

Você também pode excluir o link para um ative Directory se não precisar mais dele.

Passos

1. Abra o ambiente de trabalho.
2. Clique no botão na parte superior da página e clique em **Gerenciar ative Directory**.
3. Se nenhum ative Directory estiver configurado, você poderá adicionar um agora. Se uma estiver configurada, pode modificar as definições ou eliminá-las utilizando o botão.
4. Especifique as configurações para o ative Directory em que você deseja ingressar:

Campo	Descrição
Endereço IP primário do DNS	Os endereços IP dos servidores DNS que fornecem resolução de nomes para o servidor SMB. Use uma vírgula para separar os endereços IP ao fazer referência a vários servidores, por exemplo, 172.31.25.223, 172.31.2.74.
Ative Directory Domain para aderir	O FQDN do domínio do ative Directory (AD) ao qual você deseja que o servidor SMB se associe. Ao usar o AWS Managed Microsoft AD, use o valor do campo "Directory DNS name".
Nome NetBIOS do servidor SMB	Um nome NetBIOS para o servidor SMB que será criado.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores à unidade organizacional especificada (ou) dentro do domínio do AD.
Unidade organizacional	A unidade organizacional dentro do domínio AD a associar ao servidor SMB. A predefinição é computadores para ligações ao seu próprio servidor Windows ative Directory. Se você configurar o AWS Managed Microsoft AD como o servidor AD para o Cloud Volumes Service, deverá inserir neste campo **ou computadores**.

5. Clique em **Salvar** para salvar suas configurações.

Gerenciar snapshots do Cloud volumes

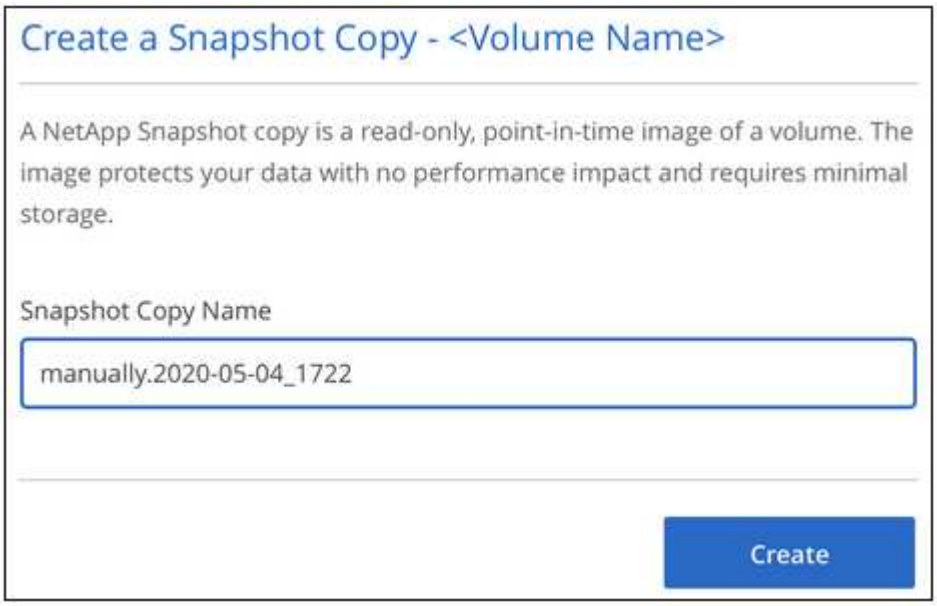
Você pode criar uma política de snapshot para cada volume para que você possa recuperar ou restaurar todo o conteúdo de um volume de um tempo anterior. Você também pode criar um snapshot sob demanda de um volume de nuvem quando necessário.

Crie um snapshot sob demanda

Você pode criar um snapshot sob demanda de um volume de nuvem se quiser criar um snapshot com o estado do volume atual.

Passos

1. Abra o ambiente de trabalho.
2. Passe o Mouse sobre o volume e clique em **criar uma cópia instantânea**.
3. Insira um nome para o instantâneo ou use o nome gerado automaticamente e clique em **criar**.



Criar ou modificar uma política de instantâneos

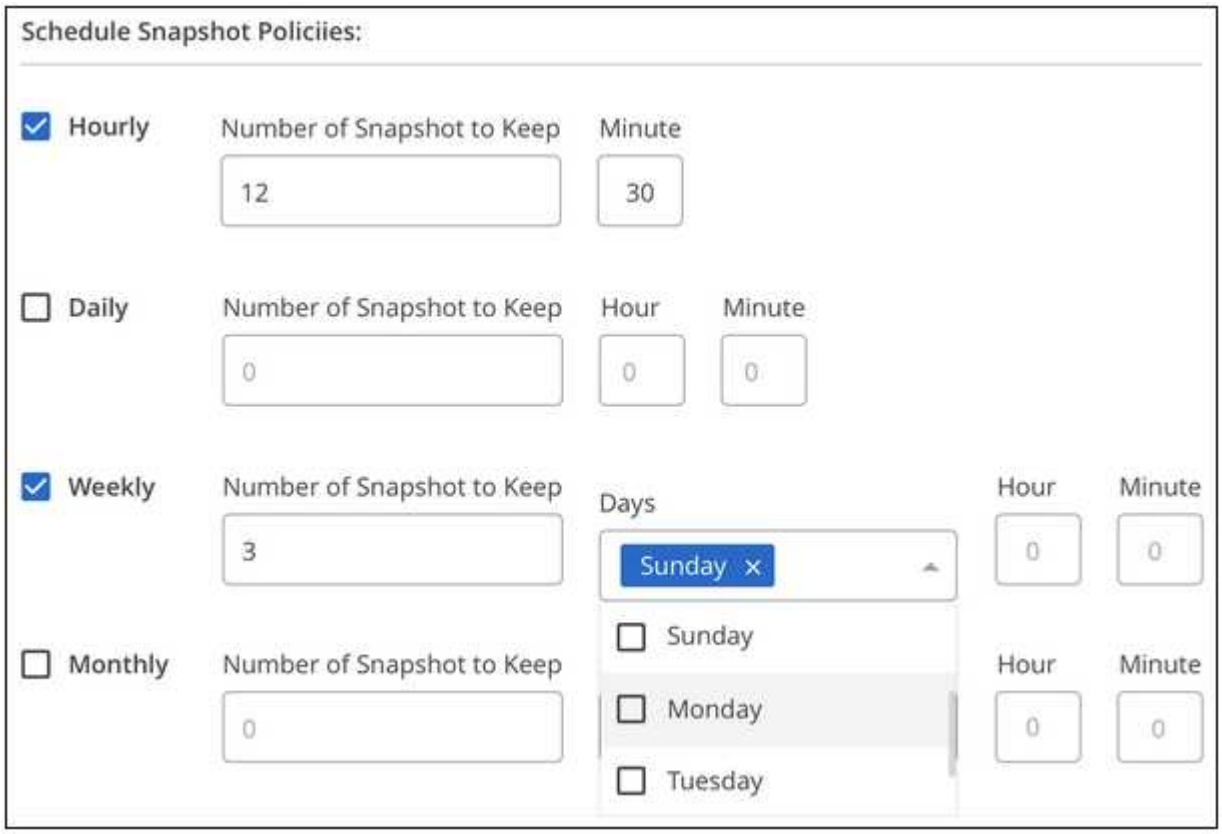
Você pode criar ou modificar uma política de snapshot conforme necessário para um volume de nuvem. Você define a política de snapshot na guia *Política de snapshot* ao criar um volume ou ao editar um volume.

Passos

1. Abra o ambiente de trabalho.
2. Passe o Mouse sobre o volume e clique em **Editar**.
3. Na guia *Política de instantâneos*, mova o controle deslizante Ativar snapshots para a direita.
4. Definir a programação para instantâneos:
    a. Selecione a frequência: **Hourly**, **Daily**, **Weekly** ou **Monthly**

b. Selecione o número de instantâneos que pretende manter.

c. Selecione o dia, a hora e o minuto em que o instantâneo deve ser obtido.



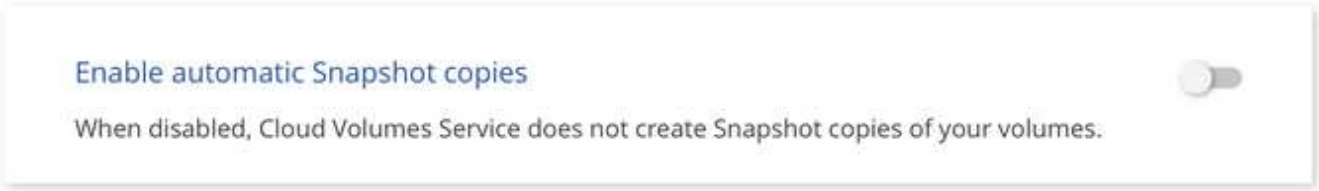
5. Clique em **Adicionar volume** ou **Atualizar volume** para salvar suas configurações de política.

Desativar uma política de instantâneos

Pode desativar uma política de instantâneos para impedir que os instantâneos sejam criados durante um curto período de tempo, mantendo as definições da política de instantâneos.

Passos

1. Abra o ambiente de trabalho.
2. Passe o Mouse sobre o volume e clique em **Editar**.
3. Na guia *Política de instantâneos*, mova o controle deslizante Ativar snapshots para a esquerda.



4. Clique em **Atualizar volume**.

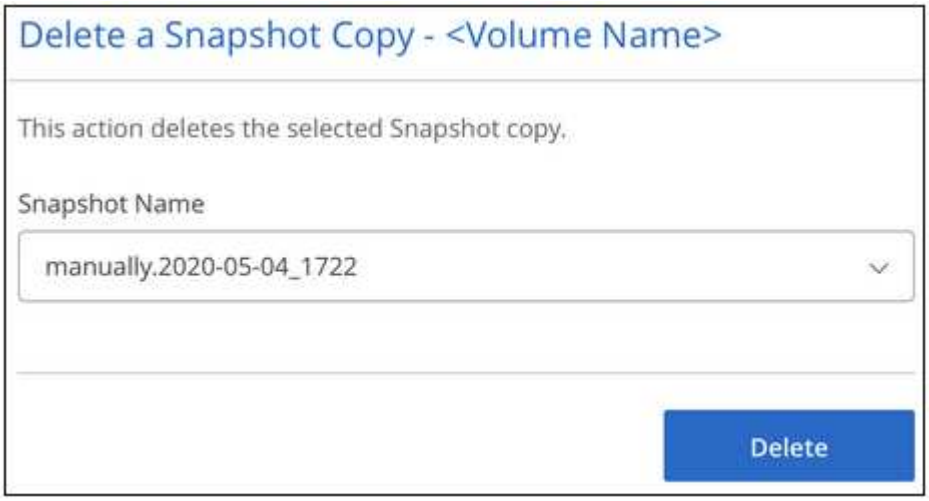
Quando quiser reativar a política de instantâneos, mova o controle deslizante Ativar instantâneos para a direita e clique em **Atualizar volume**.

Eliminar um instantâneo

Pode eliminar um instantâneo da página volumes.

Passos

1. Abra o ambiente de trabalho.
2. Passe o Mouse sobre o volume e clique em **Excluir uma cópia Snapshot**.
3. Selecione o instantâneo na lista suspensa e clique em **Excluir**.



4. Na caixa de diálogo de confirmação, clique em **Excluir**.

Reverter um volume de um instantâneo

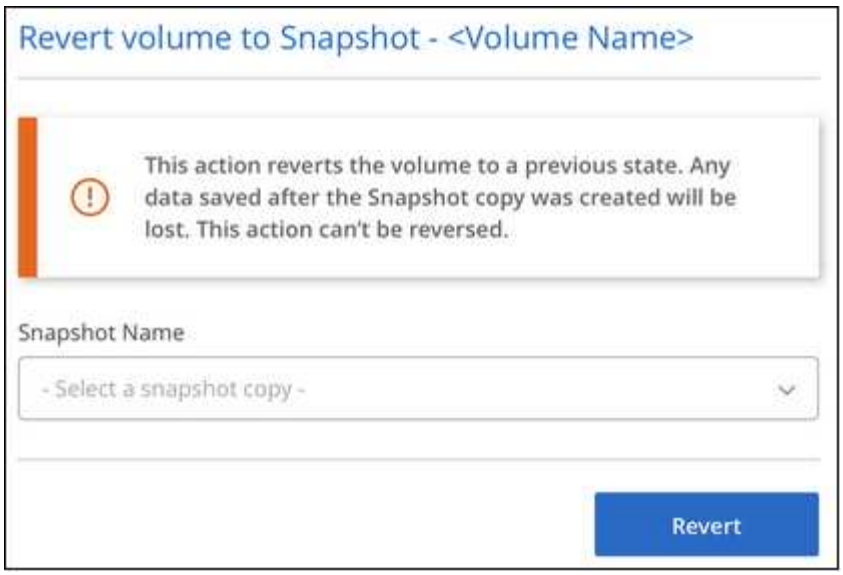
Você pode reverter um volume para um ponto anterior no tempo de um snapshot existente.

Quando você reverte um volume, o conteúdo do snapshot substitui a configuração de volume existente. Todas as alterações feitas aos dados no volume após a criação do instantâneo são perdidas.

Observe que os clientes não precisam remontar o volume após a operação de reversão.

Passos

1. Abra o ambiente de trabalho.
2. Passe o Mouse sobre o volume e clique em **Revert volume to Snapshot**.
3. Selecione o instantâneo que deseja usar para restaurar o volume existente na lista suspensa e clique em **Reverter**.



Referência

Níveis de serviço e capacidade alocada

O custo do Cloud Volumes Service para AWS é baseado no *nível de serviço* e na *capacidade alocada* que você selecionar. Selecionar o nível de serviço e a capacidade apropriados ajuda você a atender às necessidades de storage pelo menor custo possível.

Considerações

As necessidades de storage incluem dois aspectos fundamentais:

- O armazenamento *capacidade* para armazenar dados
- O armazenamento *bandwidth* para interagir com os dados

Se você consumir mais espaço de armazenamento do que a capacidade selecionada para o volume, as seguintes considerações se aplicam:

- Você será cobrado pela capacidade de armazenamento adicional consumida pelo preço definido pelo seu nível de serviço.
- A quantidade de largura de banda de storage disponível para o volume não aumenta até que você aumente o tamanho da capacidade alocada ou altere o nível de serviço.

Níveis de serviço

O Cloud Volumes Service para AWS oferece suporte a três níveis de serviço. Você especifica seu nível de serviço ao criar ou modificar o volume.

Os níveis de serviço são atendidos com diferentes necessidades de capacidade de storage e largura de banda de storage:

- **Standard** (capacidade)

  Se você deseja capacidade com o menor custo e suas necessidades de largura de banda são limitadas,

então o nível de serviço padrão pode ser mais apropriado para você. Um exemplo é usar o volume como um destino de backup.

    - Largura de banda: 16 KB de largura de banda por GB de capacidade provisionada

- **Premium** (equilíbrio de capacidade e desempenho)

  Se a sua aplicação tiver uma necessidade equilibrada de capacidade de armazenamento e largura de banda, o nível de serviço Premium pode ser mais adequado para você. Esse nível é mais barato por MB/s do que o nível de serviço padrão e também é mais barato por GB de capacidade de armazenamento do que o nível de serviço Extreme.

    - Largura de banda: 64 KB de largura de banda por GB de capacidade provisionada

- **Extreme** (desempenho)

  O nível de serviço Extreme é menos caro em termos de largura de banda de storage. Se o aplicativo exigir largura de banda de storage sem a demanda associada por muita capacidade de storage, o nível de serviço Extremo poderá ser o mais apropriado para você.

    - Largura de banda: 128 KB de largura de banda por GB de capacidade provisionada

Capacidade alocada

Você especifica a capacidade alocada para o volume ao criar ou modificar o volume.

Embora você selecione seu nível de serviço com base em suas necessidades comerciais gerais e de alto nível, você deve selecionar o tamanho da capacidade alocada com base nas necessidades específicas dos aplicativos, por exemplo:

- Quanto espaço de armazenamento as aplicações precisam
- Quanta largura de banda de armazenamento por segundo as aplicações ou os usuários exigem

A capacidade alocada é especificada em GBs. A capacidade alocada de um volume pode ser definida dentro do intervalo de 100 GB a 100.000 GB (equivalente a 100 TBs).

Número de inodes

Volumes menores ou iguais a 1 TB podem usar até 20 milhões de inodes. O número de inodes aumenta em 20 milhões para cada TB que você alocar, até um máximo de 100 milhões de inodes.

- 1TB: 20 milhões de inodes
- >1 TB a 2 TB é de 40 milhões de inodes
- >2 TB a 3 TB é de 60 milhões de inodes
- >3 TB a 4 TB é de 80 milhões de inodes
- >4 TB a 100 TB é de 100 milhões de inodes

Largura de banda

A combinação do nível de serviço e da capacidade alocada selecionada determina a largura de banda máxima para o volume.

Se seus aplicativos ou usuários precisarem de mais largura de banda do que suas seleções, você poderá alterar o nível de serviço ou aumentar a capacidade alocada. As alterações não interrompem o acesso aos

dados.

Selecionar o nível de serviço e a capacidade atribuída

Para selecionar o nível de serviço mais adequado e a capacidade alocada para suas necessidades, você precisa saber quanta capacidade e largura de banda você precisa no pico ou na borda.

Lista de níveis de serviço e capacidade alocada

A coluna mais à esquerda indica a capacidade e as outras colunas definem os MB/s disponíveis em cada ponto de capacidade com base no nível de serviço.

"Preços de assinatura do contrato"Consulte e "Preços mensurados para assinatura" para obter detalhes completos sobre preços.

Capacidade (TB)	Padrão (MB/s)	Premium (MB/s)	Extreme (MB/s)
0,1 GB (100 GB)	1,6	6,4	12,8
1	16	64	128
2	32	128	256
3	48	192	384
4	64	256	512
5	80	320	640
6	96	384	768
7	112	448	896
8	128	512	1.024
9	144	576	1.152
10	160	640	1.280
11	176	704	1.408
12	192	768	1.536
13	208	832	1.664
14	224	896	1.792
15	240	960	1.920
16	256	1.024	2.048
17	272	1.088	2.176
18	288	1.152	2.304
19	304	1.216	2.432
20	320	1.280	2.560
21	336	1.344	2.688
22	352	1.408	2.816
23	368	1.472	2.944

Capacidade (TB)	Padrão (MB/s)	Premium (MB/s)	Extreme (MB/s)
24	384	1.536	3.072
25	400	1.600	3.200
26	416	1.664	3.328
27	432	1.728	3.456
28	448	1.792	3.584
29	464	1.856	3.712
30	480	1.920	3.840
31	496	1.984	3.968
32	512	2.048	4.096
33	528	2.112	4.224
34	544	2.176	4.352
35	560	2.240	4.480
36	576	2.304	4.500
37	592	2.368	4.500
38	608	2.432	4.500
39	624	2.496	4.500
40	640	2.560	4.500
41	656	2.624	4.500
42	672	2.688	4.500
43	688	2.752	4.500
44	704	2.816	4.500
45	720	2.880	4.500
46	736	2.944	4.500
47	752	3.008	4.500
48	768	3.072	4.500
49	784	3.136	4.500
50	800	3.200	4.500
51	816	3.264	4.500
52	832	3.328	4.500
53	848	3.392	4.500
54	864	3.456	4.500
55	880	3.520	4.500
56	896	3.584	4.500

Capacidade (TB)	Padrão (MB/s)	Premium (MB/s)	Extreme (MB/s)
57	912	3.648	4.500
58	928	3.712	4.500
59	944	3.776	4.500
60	960	3.840	4.500
61	976	3.904	4.500
62	992	3.968	4.500
63	1.008	4.032	4.500
64	1.024	4.096	4.500
65	1.040	4.160	4.500
66	1.056	4.224	4.500
67	1.072	4.288	4.500
68	1.088	4.352	4.500
69	1.104	4.416	4.500
70	1.120	4.480	4.500
71	1.136	4.500	4.500
72	1.152	4.500	4.500
73	1.168	4.500	4.500
74	1.184	4.500	4.500
75	1.200	4.500	4.500
76	1.216	4.500	4.500
77	1.232	4.500	4.500
78	1.248	4.500	4.500
79	1.264	4.500	4.500
80	1.280	4.500	4.500
81	1.296	4.500	4.500
82	1.312	4.500	4.500
83	1.328	4.500	4.500
84	1.344	4.500	4.500
85	1.360	4.500	4.500
86	1.376	4.500	4.500
87	1.392	4.500	4.500
88	1.408	4.500	4.500
89	1.424	4.500	4.500

Capacidade (TB)	Padrão (MB/s)	Premium (MB/s)	Extreme (MB/s)
90	1.440	4.500	4.500
91	1.456	4.500	4.500
92	1.472	4.500	4.500
93	1.488	4.500	4.500
94	1.504	4.500	4.500
95	1.520	4.500	4.500
96	1.536	4.500	4.500
97	1.552	4.500	4.500
98	1.568	4.500	4.500
99	1.584	4.500	4.500
100	1.600	4.500	4.500

Exemplo 1

Por exemplo, seu aplicativo requer 25 TB de capacidade e 100 MB/s de largura de banda. Com 25 TB de capacidade, o nível de serviço padrão forneceria 400 MB/s de largura de banda a um custo de $2.500 (estimativa: Ver preços atuais), tornando a Standard o nível de serviço mais adequado neste caso.

	Standard		Premium		Extreme	
capacity TB	Bandwidth MB/s	Cost	Bandwidth MB/s	Cost	Bandwidth MB/s	Cost
24	384	$2,400	1,536	$4,800	3,072	$7,200
25	400	$2,500	1,600	$5,000	3,200	$7,500
26	416	$2,600	1,664	$5,200	3,328	$7,800

Exemplo 2

Por exemplo, seu aplicativo requer 12 TB de capacidade e 800 MB/s de largura de banda máxima. Embora o nível de serviço Extreme possa atender às demandas do aplicativo na marca de 12 TB, é mais econômico (estimativa: Consulte o preço atual) selecionar 13 TB no nível de serviço Premium.

	Standard		Premium		Extreme	
capacity TB	Bandwidth MB/s	Cost	Bandwidth MB/s	Cost	Bandwidth MB/s	Cost
12	192	$1,200	768	$2,400	1,536	$3,600
13	208	$1,300	832	$2,600	1,664	$3,900
14	224	$1,400	896	$2,800	1,792	$4,200

Configurações do grupo de segurança da AWS para servidores Windows AD

Se você usar servidores do Windows ative Directory (AD) com volumes na nuvem,

familiarize-se com as orientações sobre as configurações do grupo de segurança da AWS. As configurações permitem que os volumes de nuvem se integrem corretamente ao AD.

Por padrão, o grupo de segurança da AWS aplicado a uma instância do Windows EC2 não contém regras de entrada para nenhum protocolo, exceto RDP. Você deve adicionar regras aos grupos de segurança anexados a cada instância do Windows AD para habilitar a comunicação de entrada do Cloud Volumes Service. As portas necessárias são as seguintes:

Serviço	Porta	Protocolo
AD Web Services	9389	TCP
DNS	53	TCP
DNS	53	UDP
ICMPv4	N/A.	Resposta de eco
Kerberos	464	TCP
Kerberos	464	UDP
Kerberos	88	TCP
Kerberos	88	UDP
LDAP	389	TCP
LDAP	389	UDP
LDAP	3268	TCP
Nome NetBIOS	138	UDP
SAM/LSA	445	TCP
SAM/LSA	445	UDP
LDAP seguro	636	TCP
LDAP seguro	3269	TCP
w32time	123	UDP

Se você estiver implantando e gerenciando controladores de domínio de instalação do AD e servidores membros em uma instância do AWS EC2, precisará de várias regras de grupo de segurança para permitir o tráfego para o Cloud Volumes Service. Abaixo está um exemplo de como implementar essas regras para aplicativos do AD como parte do modelo do AWS CloudFormation.

```
{
    "AWSTemplateFormatVersion" : "2010-09-09",
    "Description" : "Security Group for AD",
    "Parameters" :
    {
        "VPC" :
        {
            "Type" : "AWS::EC2::VPC::Id",
```

```
            "Description" : "VPC where the Security Group will belong:"
        },
        "Name" :
        {
            "Type" : "String",
            "Description" : "Name Tag of the Security Group:"
        },
        "Description" :
        {
            "Type" : "String",
            "Description" : "Description Tag of the Security Group:",
            "Default" : "Security Group for Active Directory for CVS "
        },
        "CIDRrangeforTCPandUDP" :
        {
            "Type" : "String",
            "Description" : "CIDR Range for the UDP ports
445,138,464,389,53,123 and for the TCP ports
464,339,3389,3268,88,636,9389,445 and 0-65535: *CIDR range format:
10.0.0.0/24"
        }
    },
    "Resources" :
    {
        "ADSGWest" :
        {
            "Type" : "AWS::EC2::SecurityGroup",
            "Properties" :
            {
                "GroupDescription" : {"Ref" : "Description"},
                "VpcId" : { "Ref" : "VPC" },
                "SecurityGroupIngress" : [
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "445",
                        "ToPort" : "445"
                    },
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "138",
                        "ToPort" : "138"
                    },
                    {
                        "IpProtocol" : "udp",
```

```
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "464",
                    "ToPort" : "464"
                },
                {
                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "464",
                    "ToPort" : "464"
                },
                {
                    "IpProtocol" : "udp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "389",
                    "ToPort" : "389"
                },
                {
                    "IpProtocol" : "udp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "53",
                    "ToPort" : "53"
                },
                {
                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "339",
                    "ToPort" : "339"
                },
                {
                    "IpProtocol" : "udp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "123",
                    "ToPort" : "123"
                },
                {
                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "3389",
                    "ToPort" : "3389"
                },
                {
                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "3268",
                    "ToPort" : "3268"
                },
```

```
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "88",
                        "ToPort" : "88"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "636",
                        "ToPort" : "636"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "3269",
                        "ToPort" : "3269"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "53",
                        "ToPort" : "53"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "0",
                        "ToPort" : "65535"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "9389",
                        "ToPort" : "9389"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "445",
                        "ToPort" : "445"
                    }
                ]
            }
        }
    },
```

```
    "Outputs" :
    {
        "SecurityGroupID" :
        {
            "Description" : "Security Group ID",
            "Value" : { "Ref" : "ADSGWest" }
        }
    }
}
```

Cloud Volumes Service para GCP

Saiba mais sobre o Cloud Volumes Service

O NetApp Cloud Volumes Service para Google Cloud permite adicionar rapidamente cargas de trabalho multiprotocolo, bem como criar e implantar aplicativos baseados em Windows e UNIX.

Principais recursos:

- Migre dados entre o local e o Google Cloud.
- Provisionar volumes de 1 a 100 TIB em segundos.
- Suporte a vários protocolos (você pode criar um volume NFS ou SMB).
- Proteger dados com snapshots automatizados e eficientes.
- Acelerar o desenvolvimento de aplicações com clonagem rápida.

Custo

Os volumes criados pelo Cloud Volumes Service para Google Cloud são cobrados na sua subscrição do serviço, não pelo Cloud Manager.

"Ver preços"

Não há cobrança para descobrir uma região ou volume do Cloud Volumes Service para o Google Cloud.

Regiões suportadas

"Veja regiões compatíveis do Google Cloud."

Antes de começar

O Cloud Manager pode descobrir assinaturas e volumes existentes do Cloud Volumes Service para GCP. Consulte o "Documentação do NetApp Cloud Volumes Service para Google Cloud" se ainda não tiver configurado a sua subscrição.

Obter ajuda

Use o chat do Cloud Manager para perguntas gerais sobre a operação do Cloud Volumes Service no Cloud Manager.

Para perguntas gerais sobre o Cloud Volumes Service, envie um e-mail para a equipe do NetApp em NetApp.com.

Para problemas técnicos associados ao Cloud volumes, você pode criar um caso de suporte técnico no Google Cloud Console. "obtenção de apoio"Consulte para obter detalhes.

Limitações

- O Cloud Manager não é compatível com a replicação de dados entre ambientes de trabalho ao usar o Cloud Volumes Service volumes.
- Excluir sua assinatura do Cloud Volumes Service para Google Cloud do Gerenciador de nuvem não é compatível. Você só pode fazer isso por meio do Google Cloud Console.

Links relacionados

- "NetApp Cloud Central: Cloud Volumes Service para Google Cloud"
- "Documentação do NetApp Cloud Volumes Service para Google Cloud"

Configure o Cloud Volumes Service para o Google Cloud

Crie um ambiente de trabalho do Cloud Volumes Service para o Google Cloud Manager para criar e gerenciar volumes e snapshots.

Início rápido

Comece rapidamente seguindo estes passos ou vá para a próxima secção para obter detalhes completos.

Ative a API Cloud Volumes Service

Ative a API do Cloud Volumes Service para GCP para que o Cloud Manager gerencie a assinatura e os volumes de nuvem.

Crie uma conta de serviço do GCP e faça download de credenciais

No Google, crie uma conta de serviço e uma função do GCP para que o Cloud Manager possa acessar sua conta do Cloud Volumes Service para GCP.

Crie um ambiente de trabalho do Cloud Volumes Service para GCP

No Cloud Manager, clique em **Adicionar ambiente de trabalho** > **Google Cloud** > **Cloud Volumes Service** e, em seguida, forneça detalhes sobre a conta de serviço e o projeto Google Cloud.

Ative a API Cloud Volumes Service

No Google Cloud Shell, execute o seguinte comando para ativar a API Cloud Volumes Service:

```
gcloud --project=<my-cvs-project> services enable cloudvolumesgcp-api.netapp.com
```

Dê acesso ao Cloud Manager à conta do Cloud Volumes Service para GCP

Você deve concluir as tarefas a seguir para que o Cloud Manager possa acessar seu projeto do Google Cloud:

- Crie uma nova conta de serviço
- Adicione o novo membro da conta de serviço ao seu projeto e atribua funções específicas de TI (permissões)
- Crie e faça o download de um par de chaves para a conta de serviço que é usada para autenticar no Google

Passos

1. No Google Cloud Console, vá para a página **Contas de serviço**.
2. Clique em **Selecione um projeto**, escolha seu projeto e clique em **abrir**.
3. Clique em **criar conta de serviço**, digite o nome da conta de serviço (nome de exibição amigável) e a descrição e clique em **criar**.
4. Na página *IAM* clique em **Add** e preencha os campos na página *Add Members*:
   a. No campo novos membros, insira o ID completo da conta de serviço, por exemplo, user1-service-account-cvs@project1.iam.gserviceaccount.com.
   b. Adicione estas funções:
      - *Administrador do NetApp volumes*
      - *Compute Network Viewer*
      - *Folder Viewer*
   c. Clique em **Salvar**.
5. Na página *Detalhes da conta de serviço*, clique em **Adicionar chave > criar nova chave**.
6. Selecione **JSON** como o tipo de chave e clique em **Create**.

   Ao clicar em **criar**, o novo par de chaves público/privado é gerado e transferido para o seu sistema. Serve como a única cópia da chave privada. Armazene este ficheiro de forma segura porque pode ser utilizado para autenticar como a sua conta de serviço.

Para obter etapas detalhadas, consulte tópicos do Google Cloud "Criação e gerenciamento de contas de serviço", "Concessão, alteração e revogação do acesso aos recursos"e "Criando e gerenciando chaves de conta de serviço".

Crie um ambiente de trabalho do Cloud Volumes Service para GCP

Configure um ambiente de trabalho do Cloud Volumes Service para GCP no Cloud Manager para começar a criar volumes.

Independentemente de você já ter criado volumes a partir do Console do Google Cloud ou se acabou de se inscrever no Cloud Volumes Service para GCP e ainda não tem volumes, a primeira etapa é criar um ambiente de trabalho para os volumes com base na assinatura do GCP.

Se o Cloud volumes já existir para essa assinatura, os volumes aparecerão no novo ambiente de trabalho. Se você ainda não adicionou nenhum volume de nuvem à assinatura do GCP, faça isso depois de criar o novo ambiente de trabalho.

Se você tiver assinaturas e volumes em vários projetos do GCP, precisará executar essa tarefa para cada projeto.

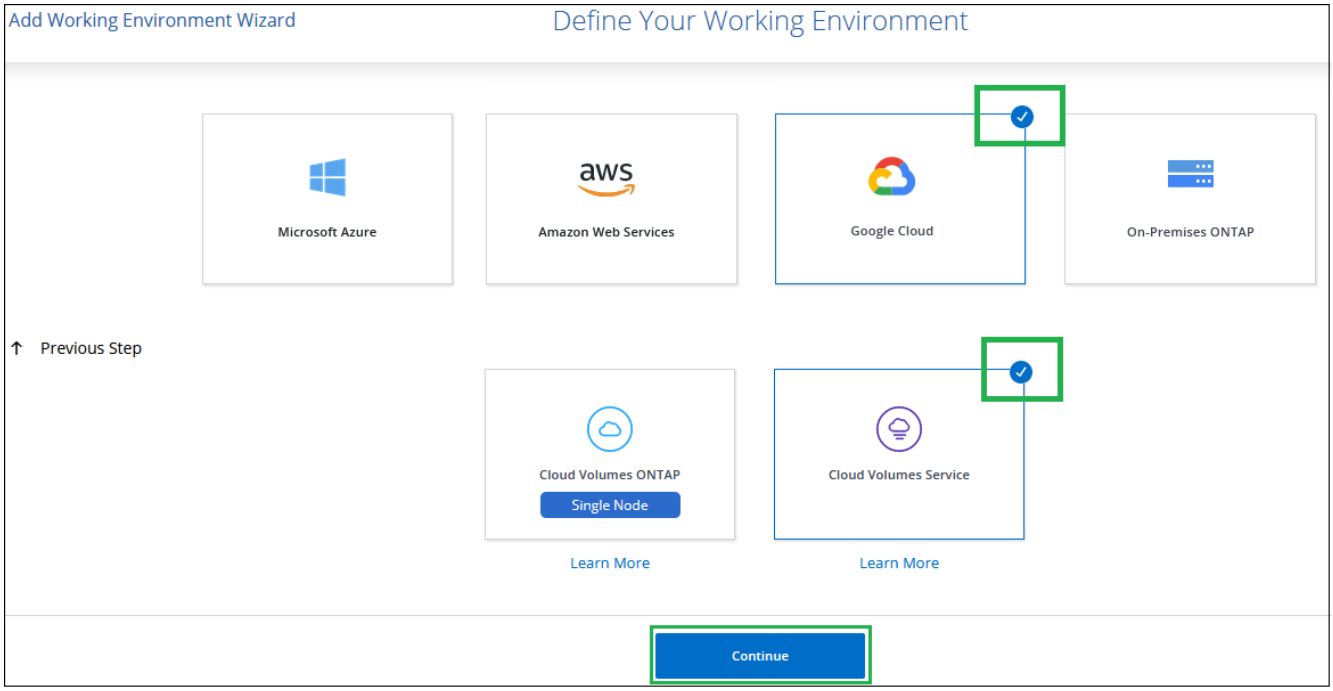
Antes de começar

Você deve ter as seguintes informações disponíveis ao adicionar uma assinatura para cada projeto:

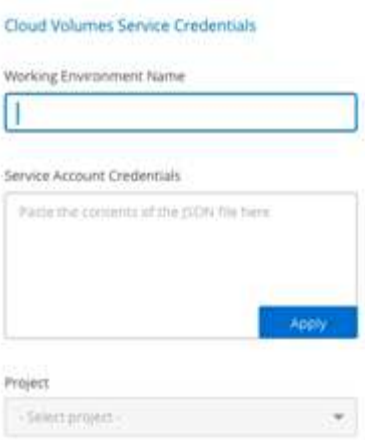
- Credenciais da conta de serviço (chave privada JSON que você baixou)
- Nome do projeto

Passos

1. No Cloud Manager, adicione um novo ambiente de trabalho, selecione o local **Google Cloud** e clique em **continuar**.
2. Selecione **Cloud Volumes Service** e clique em **continuar**.



3. Forneça informações sobre sua assinatura do Cloud Volumes Service:
   a. Introduza o nome do ambiente de trabalho que pretende utilizar.
   b. Copie/cole a chave privada JSON que você baixou nas etapas anteriores.
   c. Selecione o nome do seu projeto Google Cloud.
   d. Clique em **Add**.



Resultado

O Cloud Manager exibe seu ambiente de trabalho do Cloud Volumes Service para Google Cloud.

Se os volumes de nuvem já existirem para essa assinatura, os volumes aparecerão no novo ambiente de trabalho, como mostrado na captura de tela. Você pode adicionar volumes de nuvem adicionais do Cloud Manager.

Se não houver volumes de nuvem para essa assinatura, crie-os agora.

O que se segue?

"Comece a criar e gerenciar volumes".

Crie e gerencie volumes para Cloud Volumes Service para Google Cloud

Com o Cloud Manager, você cria volumes de nuvem com base na "Cloud Volumes Service para Google Cloud" sua subscrição. Você também pode editar certos atributos de um volume, obter os comandos de montagem relevantes, criar cópias snapshot e excluir volumes de nuvem.

Criar o Cloud volumes

É possível criar volumes NFS ou SMB em uma conta do Cloud Volumes Service for Google Cloud nova ou existente. Atualmente, o Cloud volumes suporta NFSv3 e NFSv4,1 para clientes Linux e UNIX e SMB 3.x para clientes Windows.

Antes de começar

- Se você quiser usar o SMB na GCP, você deve ter configurado o DNS e o ative Directory.
- Ao Planejar criar um volume SMB, você deve ter um servidor do Windows ative Directory disponível para o qual você pode se conetar. Você inserirá essas informações ao criar o volume. Além disso, certifique-se

de que o usuário Admin é capaz de criar uma conta de máquina no caminho da unidade organizacional (ou) especificado.

Passos

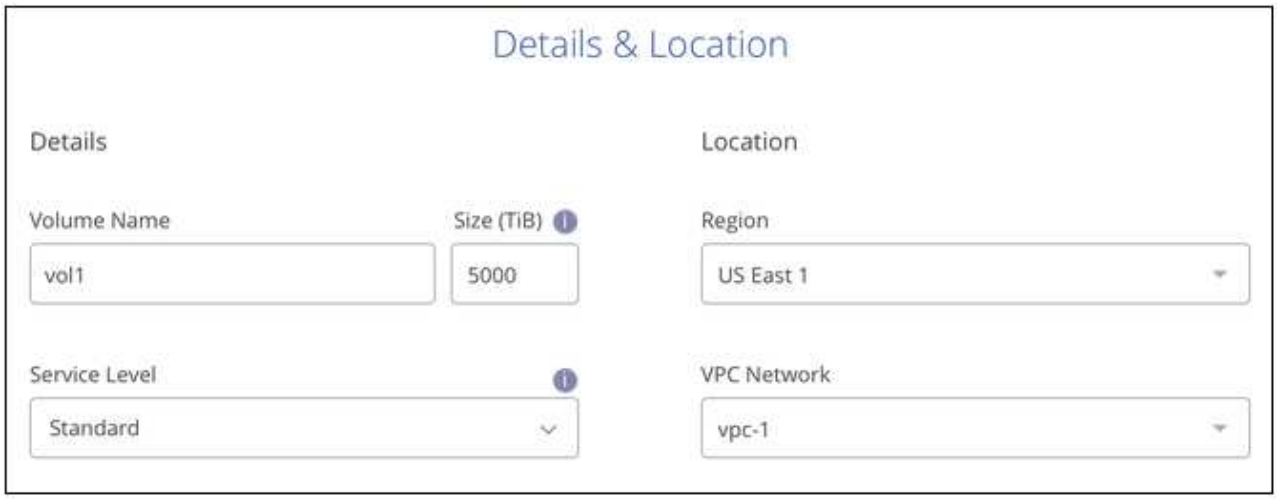
1. Selecione o ambiente de trabalho e clique em **Adicionar novo volume**.
2. Na página Detalhes e localização, introduza os detalhes sobre o volume:
   a. Introduza um nome para o volume.
   b. Especifique um tamanho dentro do intervalo de 1 TIB (1024 GiB) a 100 TIB.

      "Saiba mais sobre a capacidade alocada".

   c. Especifique um nível de serviço: Standard, Premium ou Extreme.

      "Saiba mais sobre os níveis de serviço".

   d. Selecione a região Google Cloud.
   e. Selecione a rede VPC a partir da qual o volume será acessível. Observe que a VPC não pode ser alterada ou editada após a criação do volume.
   f. Clique em **continuar**.

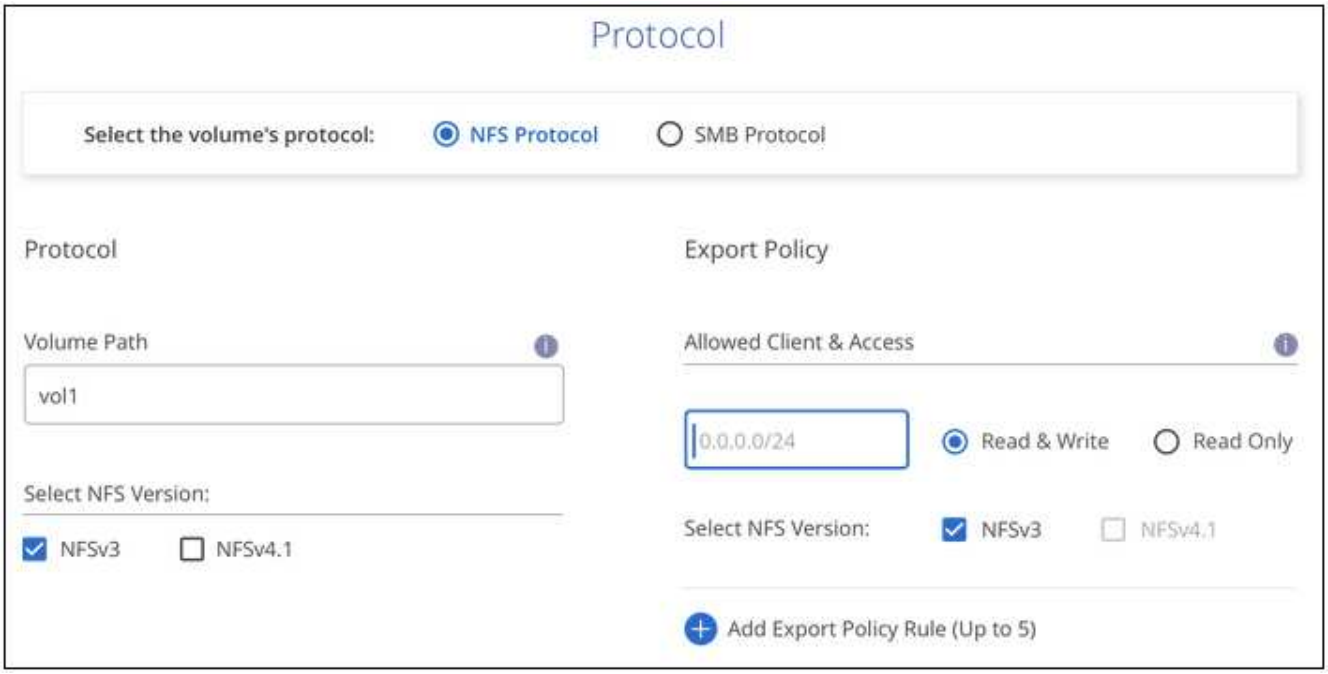


3. Na página Protocolo, selecione NFS ou SMB e, em seguida, defina os detalhes. As entradas necessárias para NFS e SMB são mostradas em seções separadas abaixo.
4. Para NFS:

   a. No campo caminho do volume , especifique o nome da exportação de volume que você verá quando montar o volume.
   b. Selecione NFSv3, NFSv4,1 ou ambos, dependendo dos seus requisitos.
   c. Opcionalmente, você pode criar uma política de exportação para identificar os clientes que podem acessar o volume. Especifique:
      - Clientes permitidos usando um endereço IP ou CIDR (Classless Inter-Domain Routing).
      - Direitos de acesso como somente leitura e gravação ou leitura.
      - Protocolo de acesso (ou protocolos se o volume permitir o acesso NFSv3 e NFSv4,1) utilizado para os utilizadores.

- Clique em Adicionar regra de política de exportação* se quiser definir regras de política de exportação adicionais.

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



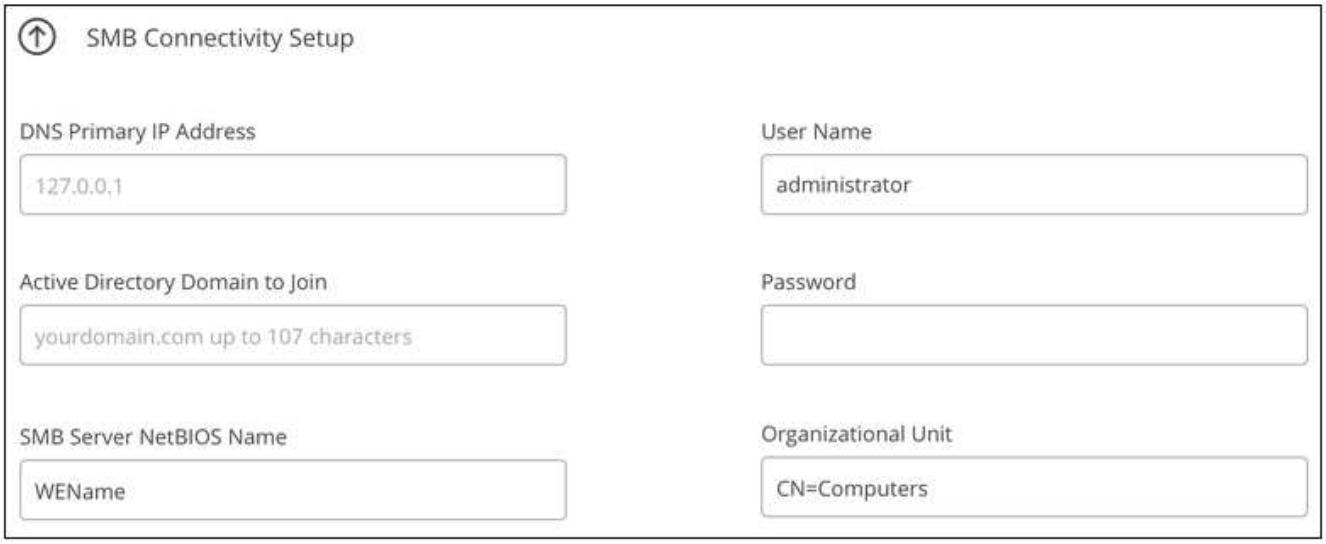
5. Para SMB:

   a. No campo caminho do volume , especifique o nome da exportação de volume que você verá quando montar o volume e clique em **continuar**.

   b. Se o ative Directory tiver sido configurado, você verá a configuração. Se for o primeiro volume a ser configurado e não tiver sido configurado o ative Directory, pode ativar a encriptação de sessão SMB na página Configuração de conetividade SMB:

Campo	Descrição
Endereço IP primário do DNS	Os endereços IP dos servidores DNS que fornecem resolução de nomes para o servidor SMB. Use uma vírgula para separar os endereços IP ao fazer referência a vários servidores, por exemplo, 172.31.25.223, 172.31.2.74.
Ative Directory Domain para aderir	O FQDN do domínio do ative Directory (AD) ao qual você deseja que o servidor SMB se associe.
Nome NetBIOS do servidor SMB	Um nome NetBIOS para o servidor SMB que será criado.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores à unidade organizacional especificada (ou) dentro do domínio do AD.
Unidade organizacional	A unidade organizacional dentro do domínio AD a associar ao servidor SMB. A predefinição é computadores para ligações ao seu próprio servidor Windows ative Directory.

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



6. Clique em **continuar**.
7. Se quiser criar o volume com base em um instantâneo de um volume existente, selecione o instantâneo na lista suspensa Nome do instantâneo. Caso contrário, basta clicar em **continuar**.
8. Na página Política de Snapshot, é possível habilitar o Cloud Volumes Service a criar cópias snapshot de seus volumes com base em uma programação. Pode fazê-lo agora movendo o seletor para a direita ou pode editar o volume mais tarde para definir a política de instantâneos.

   Consulte "Criando uma política de snapshot" para obter mais informações sobre a funcionalidade de instantâneos.

9. Clique em **Adicionar volume**.

O novo volume é adicionado ao ambiente de trabalho.

Continue com "Montagem do volume de nuvem".

Montar o Cloud volumes

Acesse as instruções de montagem do Cloud Manager para que você possa montar o volume em um host.

Nota: por favor, use o protocolo/dialeto destacado suportado pelo seu cliente.

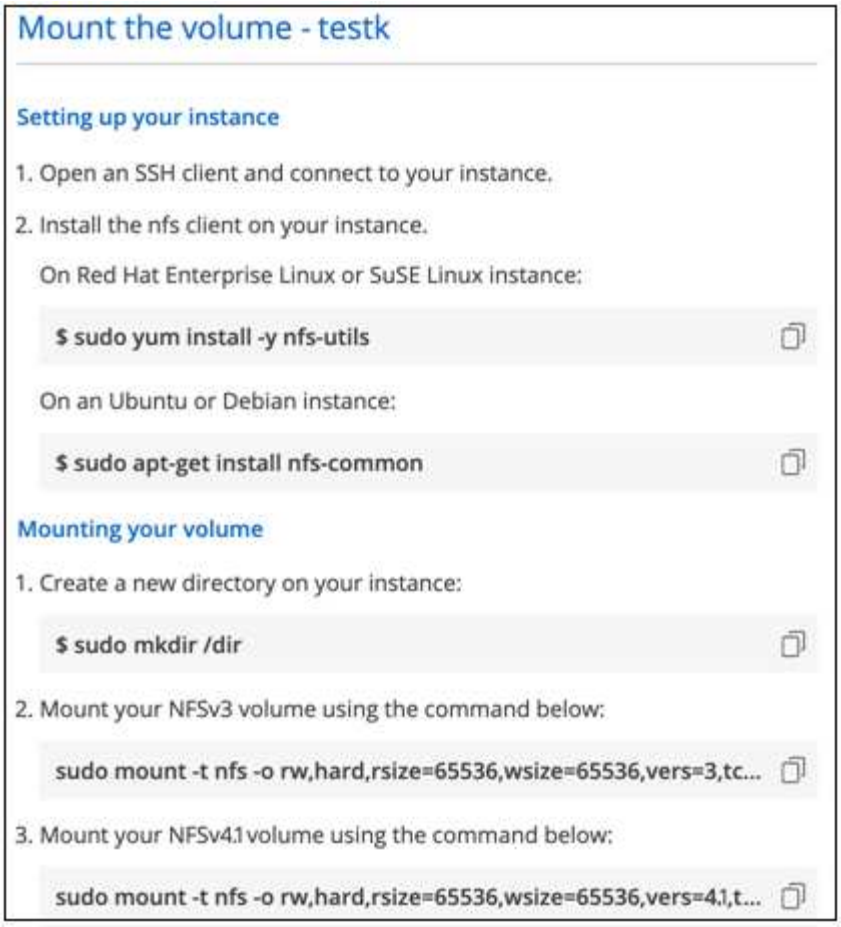
Passos

1. Abra o ambiente de trabalho.
2. Passe o Mouse sobre o volume e clique em **Monte o volume**.

   Os volumes NFS e SMB exibem instruções de montagem para esse protocolo.

3. Passe o Mouse sobre os comandos e copie-os para a área de transferência para facilitar este processo. Basta adicionar o diretório de destino/ponto de montagem no final do comando.

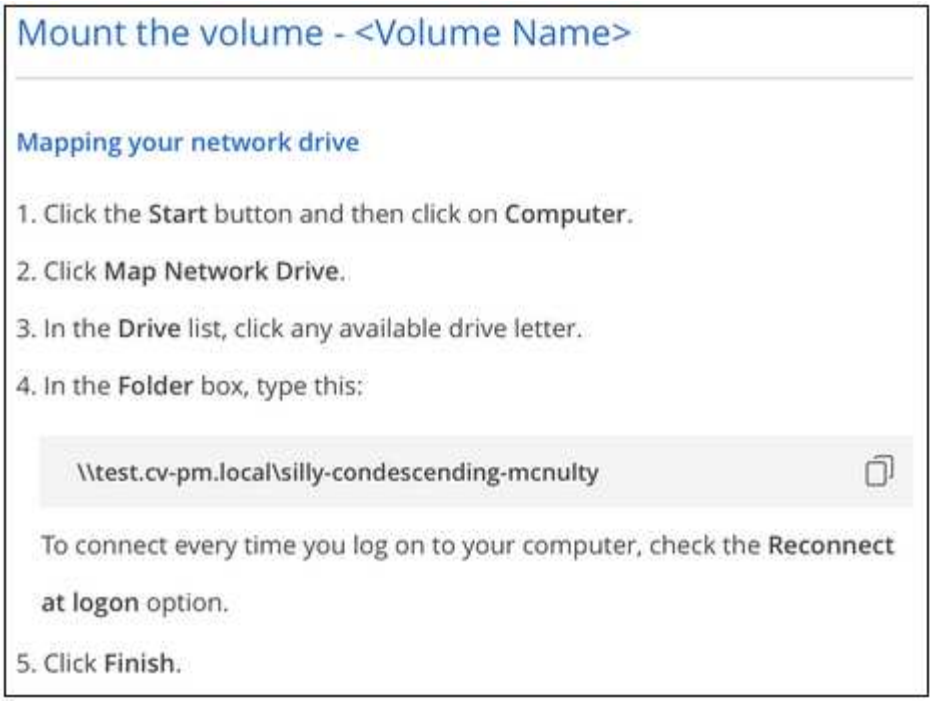
   Exemplo de NFS:



O tamanho máximo de e/S definido `rsize` pelas opções e `wsize` é 1048576, no entanto, 65536 é o padrão recomendado para a maioria dos casos de uso.

Observe que os clientes Linux serão padrão para NFSv4,1, a menos que a versão seja especificada com a `vers=<nfs_version>` opção.

Exemplo SMB:



4. Mapeie a unidade de rede seguindo as instruções de montagem da instância.

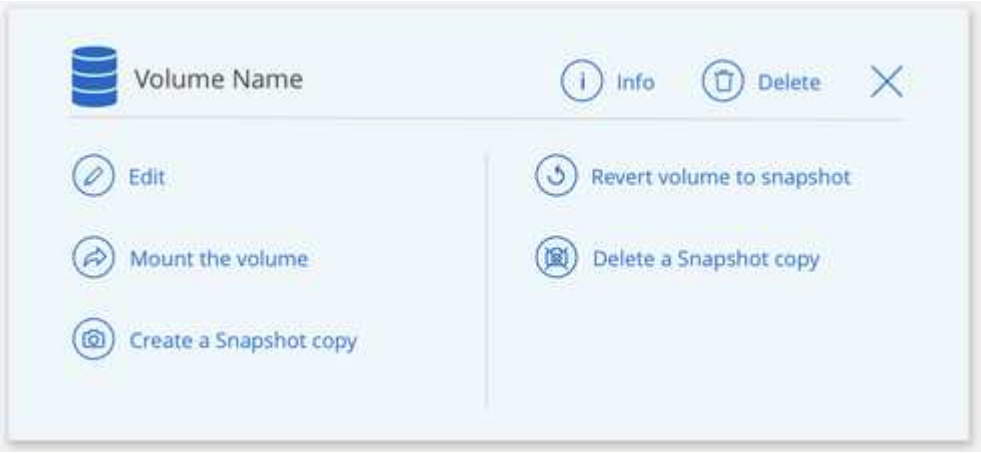
   Depois de concluir as etapas nas instruções de montagem, você montou com sucesso o volume da nuvem na instância do GCP.

Gerenciar volumes existentes

Você pode gerenciar volumes existentes conforme suas necessidades de storage mudam. Você pode exibir, editar, restaurar e excluir volumes.

Passos

1. Abra o ambiente de trabalho.
2. Passe o Mouse sobre o volume.



3. Gerencie seus volumes:

Tarefa	Ação
Exibir informações sobre um volume	Clique em **Info**.
Editar um volume (incluindo política de instantâneos)	a. Clique em **Editar**. b. Modifique as propriedades do volume e clique em **Update**.
Obtenha o comando de montagem NFS ou SMB	a. Clique em **montar o volume**. b. Clique em **Copy** para copiar o(s) comando(s).
Criar uma cópia Snapshot sob demanda	a. Clique em **criar uma cópia Snapshot**. b. Altere o nome, se necessário, e clique em **criar**.
Substitua o volume pelo conteúdo de uma cópia Snapshot	a. Clique em **Reverter volume para instantâneo**. b. Selecione uma cópia Snapshot e clique em **Restore**.
Excluir uma cópia Snapshot	a. Clique em **Excluir uma cópia Snapshot**. b. Selecione o instantâneo e clique em **Delete**. c. Clique em **Delete** novamente quando solicitado a confirmar.
Eliminar um volume	a. Desmonte o volume de todos os clientes: ◦ Em clientes Linux, use o `umount` comando. ◦ Em clientes Windows, clique em **Disconnect network drive**. b. Selecione um volume e, em seguida, clique em **Delete**. c. Clique em **Delete** novamente para confirmar.

Remova o Cloud Volumes Service do Cloud Manager

Você pode remover uma assinatura do Cloud Volumes Service para Google Cloud e todos os volumes existentes do Cloud Manager. Os volumes não são excluídos. Eles acabaram de ser removidos da interface do Cloud Manager.

Passos

1. Abra o ambiente de trabalho.
2. Clique no botão na parte superior da página e clique em **Remover Cloud Volumes Service**.
3. Na caixa de diálogo de confirmação, clique em **Remover**.

Gerenciar a configuração do ative Directory

Se você alterar seus servidores DNS ou domínio do ative Directory, precisará modificar o servidor SMB no Cloud volumes Services para que ele possa continuar fornecendo storage aos clientes.

Passos

1. Abra o ambiente de trabalho.
2. Clique no botão na parte superior da página e clique em **Gerenciar ative Directory**. Se nenhum ative Directory estiver configurado, você poderá adicionar um agora. Se uma estiver configurada, pode modificar ou eliminar as definições utilizando o botão.
3. Especifique as configurações para o servidor SMB:

Campo	Descrição
Endereço IP primário do DNS	Os endereços IP dos servidores DNS que fornecem resolução de nomes para o servidor SMB. Use uma vírgula para separar os endereços IP ao fazer referência a vários servidores, por exemplo, 172.31.25.223, 172.31.2.74.
Ative Directory Domain para aderir	O FQDN do domínio do ative Directory (AD) ao qual você deseja que o servidor SMB se associe.
Nome NetBIOS do servidor SMB	Um nome NetBIOS para o servidor SMB que será criado.
Credenciais autorizadas para ingressar no domínio	O nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores à unidade organizacional especificada (ou) dentro do domínio do AD.
Unidade organizacional	A unidade organizacional dentro do domínio AD a associar ao servidor SMB. A predefinição é computadores para ligações ao seu próprio servidor Windows ative Directory.

4. Clique em **Salvar** para salvar suas configurações.

Gerenciar snapshots do Cloud volumes

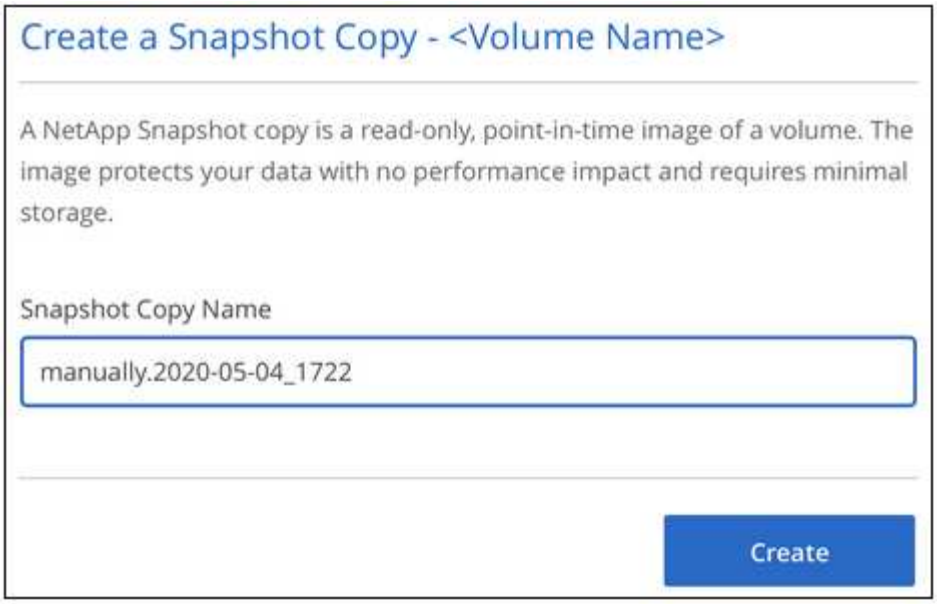
Você pode criar uma política de snapshot para cada volume para que você possa recuperar ou restaurar todo o conteúdo de um volume de um tempo anterior. Você também pode criar um snapshot sob demanda de um volume de nuvem quando necessário.

Crie um snapshot sob demanda

Você pode criar um snapshot sob demanda de um volume de nuvem se quiser criar um snapshot com o estado do volume atual.

Passos

1. Abra o ambiente de trabalho.
2. Passe o Mouse sobre o volume e clique em **criar uma cópia instantânea**.
3. Insira um nome para o instantâneo ou use o nome gerado automaticamente e clique em **criar**.



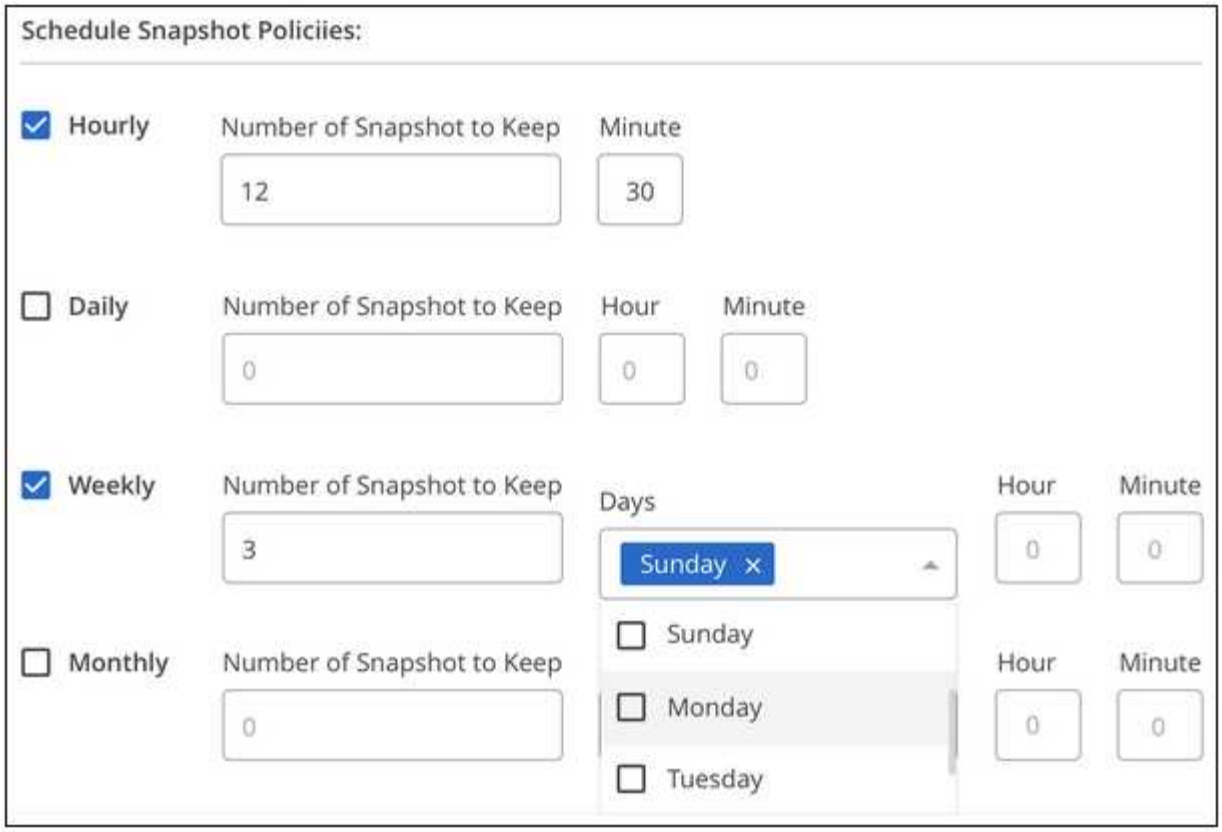
O instantâneo é criado.

Criar ou modificar uma política de instantâneos

Você pode criar ou modificar uma política de snapshot conforme necessário para um volume de nuvem. Você define a política de snapshot na guia *Política de snapshot* ao criar um volume ou ao editar um volume.

Passos

1. Abra o ambiente de trabalho.
2. Passe o Mouse sobre o volume e clique em **Editar**.
3. Na guia *Política de instantâneos*, mova o controle deslizante Ativar snapshots para a direita.
4. Definir a programação para instantâneos:
   a. Selecione a frequência: **Hourly**, **Daily**, **Weekly** ou **Monthly**
   b. Selecione o número de instantâneos que pretende manter.
   c. Selecione o dia, a hora e o minuto em que o instantâneo deve ser obtido.



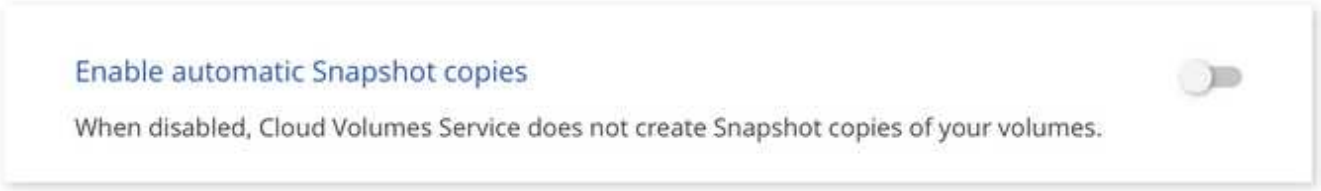
5. Clique em **Adicionar volume** ou **Atualizar volume** para salvar suas configurações de política.

Desativar uma política de instantâneos

Pode desativar uma política de instantâneos para impedir que os instantâneos sejam criados durante um curto período de tempo, mantendo as definições da política de instantâneos.

Passos

1. Abra o ambiente de trabalho.
2. Passe o Mouse sobre o volume e clique em **Editar**.
3. Na guia *Política de instantâneos*, mova o controle deslizante Ativar snapshots para a esquerda.



4. Clique em **Atualizar volume**.

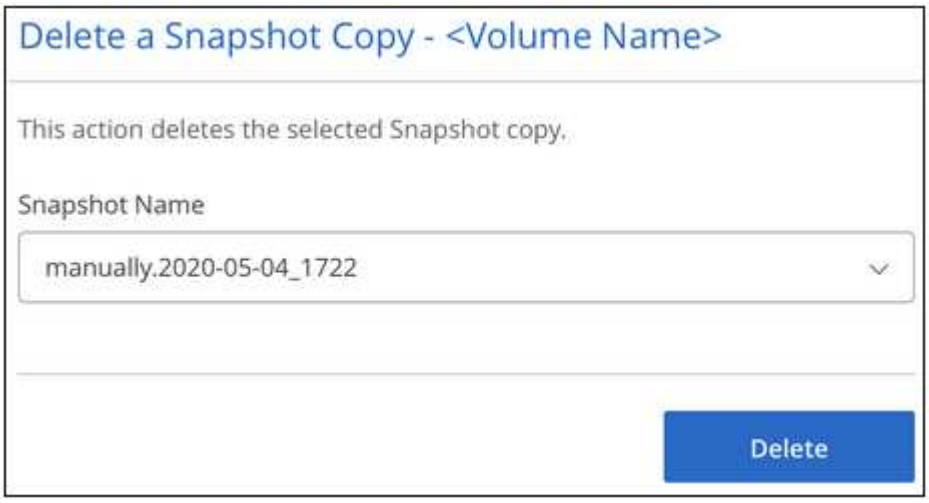
Quando quiser reativar a política de instantâneos, mova o controle deslizante Ativar instantâneos para a direita e clique em **Atualizar volume**.

Eliminar um instantâneo

Você pode excluir um instantâneo se ele não for mais necessário.

Passos

1. Abra o ambiente de trabalho.
2. Passe o Mouse sobre o volume e clique em **Excluir uma cópia Snapshot**.
3. Selecione o instantâneo na lista suspensa e clique em **Excluir**.



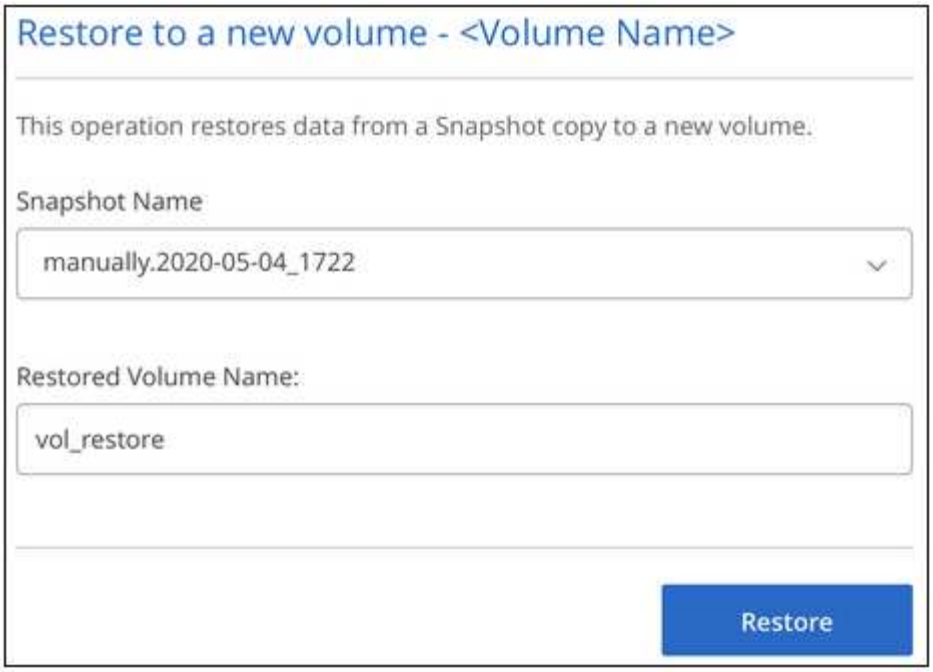
4. Na caixa de diálogo de confirmação, clique em **Excluir**.

Restaurar um snapshot para um novo volume

Você pode restaurar um snapshot para um novo volume, conforme necessário.

Passos

1. Abra o ambiente de trabalho.
2. Passe o Mouse sobre o volume e clique em **Restaurar para um novo volume**.
3. Selecione o instantâneo que pretende utilizar para criar o novo volume a partir da lista pendente.
4. Digite um nome para o novo volume e clique em **Restore**.



O volume é criado no ambiente de trabalho.

5. Se você precisar alterar qualquer um dos atributos de volume, como caminho de volume ou nível de serviço:
   a. Passe o Mouse sobre o volume e clique em **Editar**.
   b. Faça suas alterações e clique em **Atualizar volume**.

Depois de terminar

Continue com "Montagem do volume de nuvem".

Gerenciar clusters do ONTAP

Descobrindo clusters do ONTAP

O Cloud Manager pode descobrir os clusters do ONTAP em seu ambiente local, em uma configuração de storage privado do NetApp e na nuvem da IBM. Ao descobrir um cluster do ONTAP, você provisiona storage, replica dados, faz backup e categoriza dados inativos de um cluster no local para a nuvem.

O que você vai precisar

- Um conetor instalado em um fornecedor de nuvem ou no local.

  Se você quiser categorizar dados inativos na nuvem, leia os requisitos do conector com base em onde planeja categorizar dados inativos.

  - "Saiba mais sobre conetores"
  - "Comutação entre conetores"
  - "Saiba mais sobre o Cloud Tiering"
- O endereço IP de gerenciamento de cluster e a senha da conta de usuário admin para adicionar o cluster ao Cloud Manager.

  O Cloud Manager descobre clusters do ONTAP usando HTTPS. Se você usar políticas de firewall personalizadas, elas devem atender aos seguintes requisitos:

  - O host do conetor deve permitir o acesso HTTPS de saída através da porta 443.

    Se o conetor estiver na nuvem, toda a comunicação de saída é permitida pelo grupo de segurança predefinido.

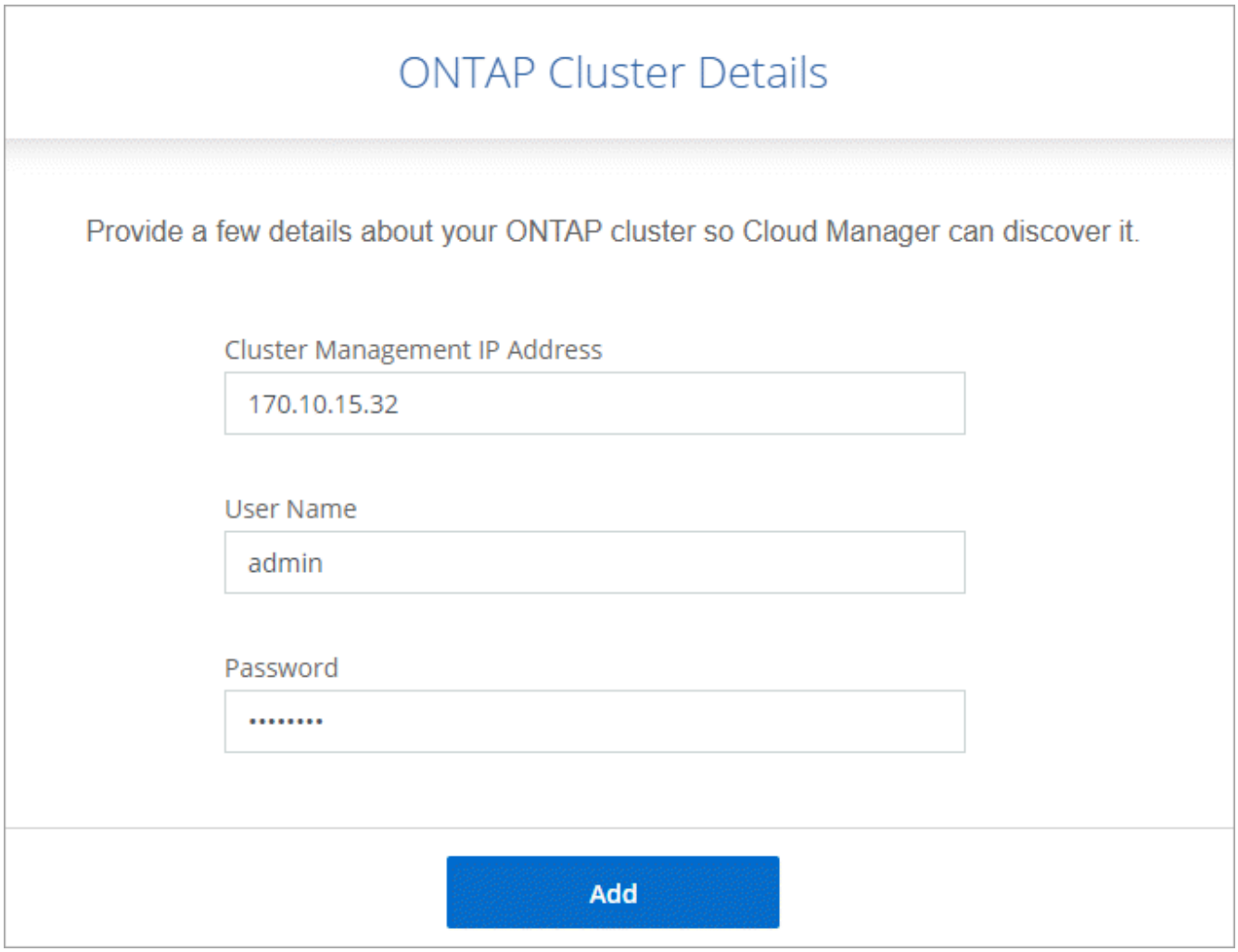
  - O cluster ONTAP deve permitir acesso HTTPS de entrada através da porta 443.

    A política de firewall "mgmt" padrão permite o acesso HTTPS de entrada de todos os endereços IP. Se você modificou essa política padrão, ou se criou sua própria política de firewall, associe o protocolo HTTPS a essa política e habilite o acesso do host do conetor.

Passos

1. Na página ambientes de trabalho, clique em **Adicionar ambiente de trabalho** e selecione **ONTAP on-premises**.
2. Se você for solicitado, crie um conetor.

   Consulte os links acima para obter mais detalhes.
3. Na página **Detalhes do cluster do ONTAP**, insira o endereço IP de gerenciamento de cluster, a senha da conta de usuário do administrador e a localização do cluster.



4. Na página Detalhes, insira um nome e uma descrição para o ambiente de trabalho e clique em **Go**.

Resultado

O Cloud Manager descobre o cluster. Agora, você pode criar volumes, replicar dados de e para o cluster, configurar a disposição de dados em categorias na nuvem, fazer backup de volumes na nuvem e iniciar o System Manager para executar tarefas avançadas.

Gerenciamento do storage para clusters do ONTAP

Depois de descobrir o cluster do ONTAP no Cloud Manager, é possível abrir o ambiente de trabalho para provisionar e gerenciar storage.

Criação de volumes para clusters ONTAP

O Cloud Manager permite provisionar volumes NFS, CIFS e iSCSI em clusters ONTAP.

Antes de começar

Os protocolos de dados devem ser configurados no cluster usando o System Manager ou a CLI.

Sobre esta tarefa

Você pode criar volumes em agregados existentes. Não é possível criar novos agregados a partir do Cloud Manager.

Passos

1. Na página ambientes de trabalho, clique duas vezes no nome do cluster do ONTAP no qual você deseja provisionar volumes.
2. Clique em **Adicionar novo volume**.
3. Na página criar novo volume, insira os detalhes do volume e clique em **criar**.

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

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

Replicação de dados

É possível replicar dados entre sistemas Cloud Volumes ONTAP e clusters do ONTAP escolhendo uma replicação de dados única, que pode ajudar você a migrar dados de e para a nuvem, ou uma programação recorrente que pode ajudar na recuperação de desastres ou retenção de longo prazo.

"Clique aqui para mais detalhes".

Backup de dados

É possível fazer backup dos dados do sistema ONTAP local para o storage de objetos econômico na nuvem usando o serviço Backup to Cloud do Cloud Manager. Esse serviço oferece recursos de backup e restauração para proteção e arquivamento de longo prazo de seus dados de nuvem.

"Clique aqui para mais detalhes".

Disposição em camadas dos dados na nuvem

Estenda seu data center para a nuvem ao dispor automaticamente em camadas os dados inativos de clusters do ONTAP para o storage de objetos.

"Clique aqui para mais detalhes".

Fazer backup na nuvem

Saiba mais sobre o backup na nuvem

O backup na nuvem é um serviço complementar para clusters Cloud Volumes ONTAP e ONTAP on-premises que oferece recursos de backup e restauração para proteção e arquivamento de longo prazo dos seus dados de nuvem. Os backups são armazenados em um armazenamento de objetos na sua conta de nuvem, independentemente das cópias do Snapshot de volume usadas para recuperação ou clonagem de curto prazo.

O backup para a nuvem é alimentado pelo "Cloud Backup Service".

Use o Cloud Manager para todas as operações de backup e restauração. Qualquer ação realizada diretamente do ONTAP ou do seu provedor de nuvem resulta em uma configuração não suportada.

Caraterísticas

- Fazer backup de cópias independentes de seus volumes de dados para storage de objetos econômico na nuvem.
- Os dados de backup são protegidos com criptografia AES-256 bits em repouso e conexões HTTPS TLS 1,2 em trânsito.
- Fazer backup da nuvem para a nuvem e dos sistemas ONTAP on-premises para a nuvem.
- Suporte para até 1.019 backups de um único volume.
- Restaure dados de um ponto específico no tempo.
- Restaure os dados para um volume no sistema de origem ou para um sistema diferente.

Ambientes de trabalho compatíveis e provedores de storage de objetos

O backup na nuvem é compatível com os seguintes tipos de ambientes de trabalho:

- Cloud Volumes ONTAP na AWS
- Cloud Volumes ONTAP no Azure
- Clusters ONTAP on-premises

Custo

O backup para a nuvem está disponível em duas opções de preço: Traga sua própria licença (BYOL) e Pay as You Go (PAYGO).

Para o BYOL, você paga a NetApp para usar o serviço por um período de tempo, por exemplo, 6 meses e por um valor máximo de capacidade de backup, por exemplo, 10 GB (antes das eficiências de storage). Além disso, você precisará pagar ao fornecedor de nuvem pelos custos de storage de objetos. Você receberá um número de série inserido na página Licenciamento do Cloud Manager para ativar o serviço. Quando um dos limites for atingido, você precisará renovar a licença. "Adicionar e atualizar sua licença do Backup BYOL"Consulte . A licença BYOL de backup se aplica a todos os sistemas Cloud Volumes ONTAP associados ao "Conta no Cloud Central".

Para o PAYGO, você precisará pagar seu provedor de nuvem pelos custos de storage de objetos e NetApp pelos custos de licenciamento de backup. Os custos de licenciamento são baseados na capacidade usada (antes da eficiência de storage):

- AWS: "Acesse a oferta do Cloud Manager Marketplace para obter detalhes de preços".
- Azure: "Acesse a oferta do Cloud Manager Marketplace para obter detalhes de preços".

Avaliação gratuita

Está disponível um teste gratuito de 30 dias. Ao usar a versão de avaliação, você é notificado sobre o número de dias de avaliação gratuitos que permanecem. No final da avaliação gratuita, os backups param de ser criados. Você deve assinar o serviço ou comprar uma licença para continuar usando o serviço.

A cópia de segurança não é eliminada quando o serviço está desativado. Você continuará sendo cobrado pelo seu provedor de nuvem pelos custos de storage de objetos pela capacidade que seus backups usam, a menos que você exclua os backups.

Como funciona o backup na nuvem

Ao habilitar o backup na nuvem em um sistema Cloud Volumes ONTAP ou ONTAP no local, o serviço realiza um backup completo dos dados. Os instantâneos de volume não estão incluídos na imagem de cópia de segurança. Após o backup inicial, todos os backups adicionais são incrementais, o que significa que somente blocos alterados e novos blocos são copiados.

Onde os backups residem

As cópias de backup são armazenadas em um bucket do S3 ou contêiner do Blob do Azure que o Cloud Manager cria na sua conta de nuvem. Para sistemas Cloud Volumes ONTAP, o armazenamento de objetos é criado na mesma região onde o sistema Cloud Volumes ONTAP está localizado. Para sistemas ONTAP no local, você identifica a região quando ativa o serviço.

Há um armazenamento de objetos por Cloud Volumes ONTAP ou sistema ONTAP no local. O Cloud Manager nomeia o armazenamento de objetos da seguinte forma: NetApp-backup-*clusteruuuid*

Certifique-se de não excluir este armazenamento de objetos.

Notas:

- Na AWS, o Cloud Manager ativa o "Recurso de acesso público do Amazon S3 Block" bucket do S3.
- No Azure, o Cloud Manager usa um grupo de recursos novo ou existente com uma conta de storage para o contêiner de Blob.

Classes de armazenamento S3 suportadas

No Amazon S3, os backups são iniciados na classe de armazenamento *Standard* e passam para a classe de armazenamento *Standard-unreasable access* após 30 dias.

Camadas de acesso Azure Blob compatíveis

No Azure, cada backup está associado ao nível de acesso *cold*.

As definições de cópia de segurança são de todo o sistema

Ao habilitar o Backup na nuvem, é feito o backup de todos os volumes identificados no sistema na nuvem.

O agendamento e o número de backups a serem mantidos são definidos no nível do sistema. As definições de cópia de segurança afetam todos os volumes no sistema.

O horário é diário, semanal, mensal ou uma combinação

Você pode escolher backups diários, semanais ou mensais de todos os volumes. Você também pode selecionar uma das políticas definidas pelo sistema que fornece backups e retenção por 3 meses, 1 ano e 7 anos. Essas políticas são:

Nome da política	Backups por intervalo…			Máx. De backups
	Diária	Semanal	Mensal	
Netapp3MonthsRetention	30	13	3	46
Netapp1YearRetention	30	13	12	55
Netapp7YearsRetention	30	53	84	167

Depois de atingir o número máximo de backups para uma categoria ou intervalo, os backups mais antigos são removidos para que você sempre tenha os backups mais atuais.

Observe que o período de retenção para backups de volumes de proteção de dados é o mesmo definido na relação de origem do SnapMirror. Você pode alterar isso se quiser usando a API.

Os backups são feitos à meia-noite

- Os backups diários começam logo após a meia-noite todos os dias.
- Os backups semanais começam logo após a meia-noite nas manhãs de domingo.
- Os backups mensais começam logo após a meia-noite do primeiro de cada mês.

Neste momento, você não pode agendar operações de backup em um horário especificado pelo usuário.

As cópias de backup estão associadas à sua conta do Cloud Central

As cópias de backup estão associadas ao "Conta no Cloud Central"no qual o Cloud Manager reside.

Se você tiver vários sistemas do Cloud Manager na mesma conta do Cloud Central, cada sistema do Cloud Manager exibirá a mesma lista de backups. Isso inclui os backups associados ao Cloud Volumes ONTAP e instâncias ONTAP locais de outros sistemas do Cloud Manager.

Considerações sobre a licença BYOL

Ao usar uma licença BYOL do Backup to Cloud, o Cloud Manager notifica você quando os backups estão se aproximando do limite de capacidade ou se aproximando da data de expiração da licença. Você recebe estas notificações:

- quando os backups atingirem 80% da capacidade licenciada e novamente quando você atingir o limite
- 30 dias antes da expiração de uma licença e novamente quando a licença expirar

Use o ícone de bate-papo no canto inferior direito da interface do Cloud Manager para renovar sua licença

quando receber essas notificações.

Duas coisas podem acontecer quando sua licença expirar:

- Se a conta que você está usando para seus sistemas ONTAP tiver uma conta de mercado, o serviço de backup continuará sendo executado, mas você será transferido para um modelo de licenciamento PAYGO. Você será cobrado pelo seu fornecedor de nuvem por custos de storage de objetos e pela NetApp por custos de licenciamento de backup, pela capacidade que seus backups estão usando.
- Se a conta que você está usando para seus sistemas ONTAP não tiver uma conta de mercado, o serviço de backup continuará sendo executado, mas você continuará recebendo a mensagem de expiração.

Depois de renovar sua assinatura BYOL, o Cloud Manager obtém automaticamente a nova licença do NetApp e a instala. Se o Cloud Manager não puder acessar o arquivo de licença pela conexão segura à Internet, você poderá obter o arquivo sozinho e enviá-lo manualmente para o Cloud Manager. Para obter instruções, "Adicionar e atualizar sua licença do Backup BYOL"consulte .

Os sistemas que foram transferidos para uma licença PAYGO são devolvidos à licença BYOL automaticamente. E os sistemas que estavam em execução sem uma licença deixarão de receber a mensagem de aviso e serão cobrados pelos backups que ocorreram enquanto a licença expirou.

Volumes compatíveis

O backup to Cloud é compatível com volumes de leitura-gravação e volumes de proteção de dados (DP).

Atualmente, os volumes FlexGroup não são suportados.

Limitações

- O STORAGE WORM (SnapLock) não é suportado em um sistema Cloud Volumes ONTAP ou no local quando o backup na nuvem está habilitado.
- Restrições de backup na nuvem ao fazer backups de sistemas ONTAP locais:
  - O cluster no local deve estar executando o ONTAP 9.7P5 ou posterior.
  - O Cloud Manager deve ser implantado no Azure. Não há suporte para implantações no local do Cloud Manager.
  - O local de destino para backups é apenas o storage de objetos no Azure.
  - Os backups só podem ser restaurados em sistemas Cloud Volumes ONTAP implantados no Azure. Não é possível restaurar um backup para um sistema ONTAP no local ou para um sistema Cloud Volumes ONTAP que esteja usando um fornecedor de nuvem diferente.
- Ao fazer backup de volumes de proteção de dados (DP), a regra definida para a política SnapMirror no volume de origem deve usar um rótulo que corresponda aos nomes de políticas de backup para nuvem permitidos de **diária**, **semanal** ou **mensal**. Caso contrário, o backup falhará para esse volume DP.
- No Azure, se você habilitar o backup na nuvem quando o Cloud Volumes ONTAP for implantado, o Cloud Manager criará o grupo de recursos para você e não poderá alterá-lo. Se você quiser escolher seu próprio grupo de recursos ao ativar o Backup na nuvem, **Disable** Backup na nuvem ao implantar o Cloud Volumes ONTAP e, em seguida, ative o Backup na nuvem e escolha o grupo de recursos na página Configurações de Backup para nuvem.
- Ao fazer backup de volumes de sistemas Cloud Volumes ONTAP, os volumes criados fora do Cloud Manager não são automaticamente copiados.

  Por exemplo, se você criar um volume a partir da CLI do ONTAP, da API do ONTAP ou do Gerenciador de

sistema, o backup do volume não será feito automaticamente.

Se você quiser fazer backup desses volumes, será necessário desativar o Backup to Cloud e ativá-lo novamente.

Comece agora

Fazer backup de dados para o Amazon S3

Conclua algumas etapas para começar a fazer backup de dados do Cloud Volumes ONTAP para o Amazon S3.

Início rápido

Comece rapidamente seguindo estas etapas ou role para baixo até as seções restantes para obter detalhes completos.

Verifique o suporte para sua configuração

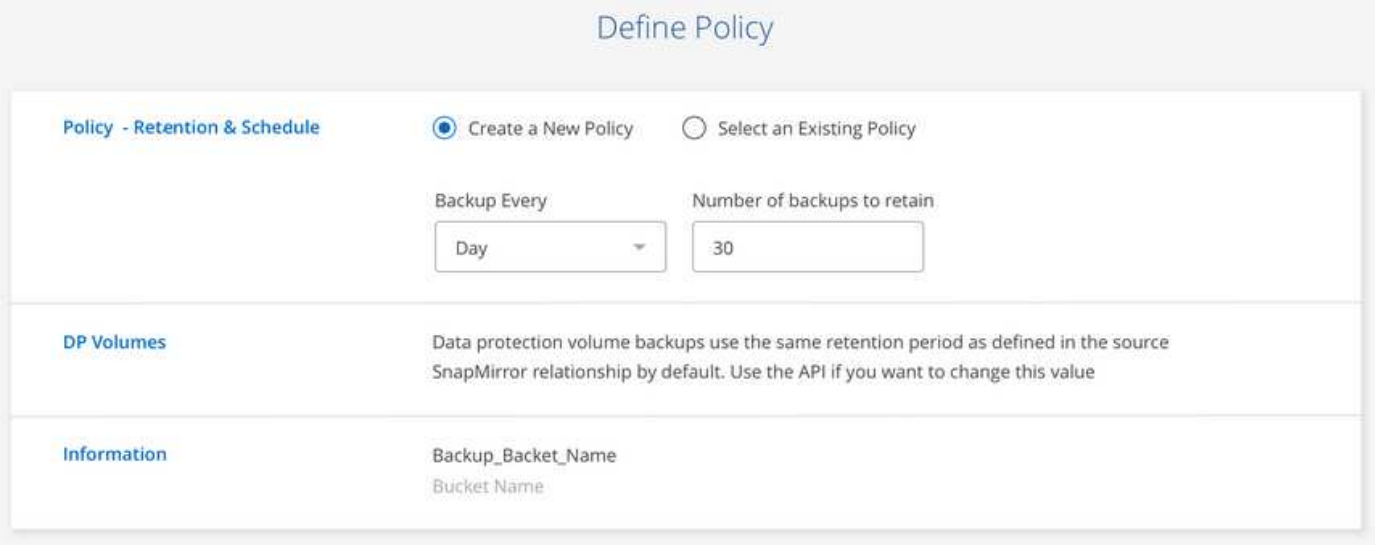
- Você está executando o Cloud Volumes ONTAP 9,6 ou posterior na AWS.
- Você se inscreveu no "Oferta de backup do Cloud Manager Marketplace", ou comprou "e ativado" uma licença BYOL de backup para nuvem da NetApp.
- A função do IAM que fornece permissões ao Cloud Manager inclui permissões S3 do último "Política do Cloud Manager".

Habilite o backup na nuvem em seu sistema novo ou existente

- Novos sistemas: O backup para a nuvem é habilitado por padrão no assistente de ambiente de trabalho. Certifique-se de que mantém a opção ativada.
- Sistemas existentes: Selecione o ambiente de trabalho e clique em **Activate** ao lado do serviço Backup to Cloud no painel direito e, em seguida, siga o assistente de configuração.

Defina a política de cópia de segurança

A política padrão faz backup de volumes todos os dias e retém as 30 cópias de backup mais recentes de cada volume. Altere para backups semanais ou mensais ou selecione uma das políticas definidas pelo sistema que oferecem mais opções. Você também pode alterar o número de cópias de backup a serem mantidas.

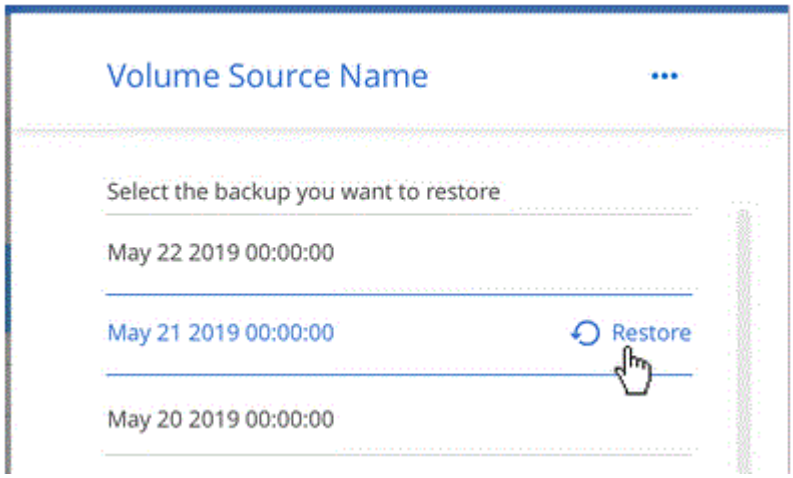


4 Selecione os volumes que deseja fazer backup

Identifique quais volumes você deseja fazer backup na página Selecionar volumes.

5 Restaure seus dados conforme necessário

Na Lista de cópias de segurança, selecione um volume, selecione uma cópia de segurança e, em seguida, restaure os dados da cópia de segurança para um novo volume.



Requisitos

Leia os requisitos a seguir para garantir que você tenha uma configuração compatível antes de iniciar o backup de volumes para S3.

Versões de ONTAP compatíveis

Cloud Volumes ONTAP 9,6 e posterior.

Regiões AWS compatíveis

O backup na nuvem é compatível com todas as regiões da AWS "Onde o Cloud Volumes ONTAP é suportado" .

Requisitos de licença

Para o licenciamento do Backup to Cloud PAYGO, uma assinatura do Cloud Manager está disponível no AWS Marketplace que permite implantações do Cloud Volumes ONTAP 9,6 e posteriores (PAYGO) e backup na nuvem. Antes de habilitar o backup na nuvem, você precisa "Assine esta assinatura do Cloud Manager" ativar o backup na nuvem. A cobrança do Backup to Cloud é feita por meio dessa assinatura.

Para o licenciamento BYOL do Backup to Cloud, você não precisa de uma assinatura do AWS Backup to Cloud. Você precisa do número de série da NetApp que permite usar o serviço durante a duração e a capacidade da licença. "Adicionar e atualizar sua licença do Backup BYOL"Consulte .

E você precisa ter uma assinatura da AWS para o espaço de armazenamento onde seus backups estarão localizados.

Permissões da AWS necessárias

A função do IAM que fornece permissões ao Cloud Manager deve incluir permissões S3 do último "Política do Cloud Manager".

Aqui estão as permissões específicas da política:

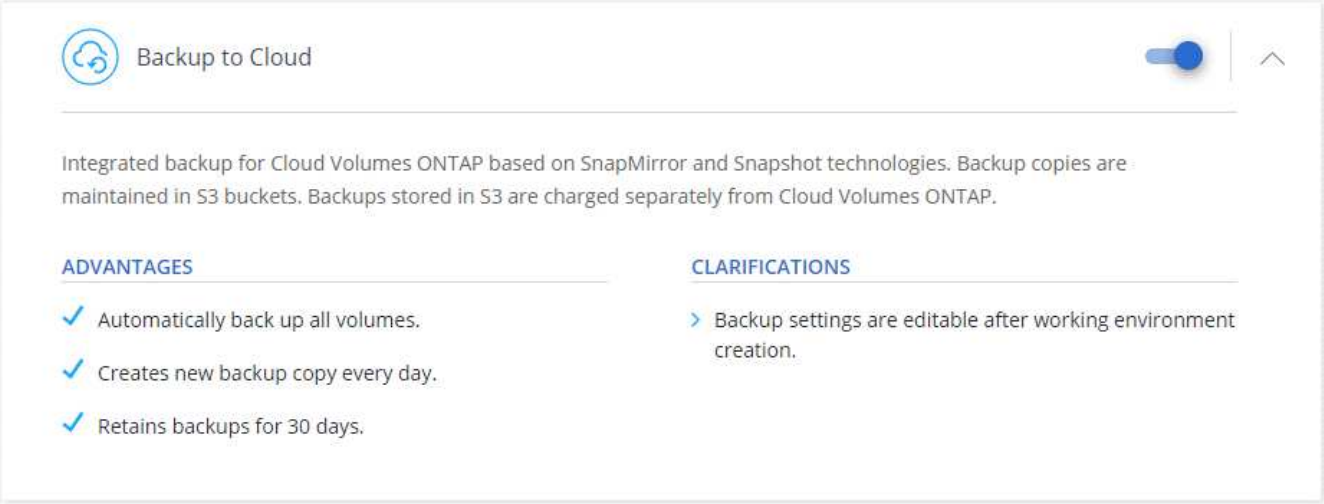
```
{
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
            ]
        },
```

Habilitando o backup para a nuvem em um novo sistema

O backup para a nuvem é habilitado por padrão no assistente de ambiente de trabalho. Certifique-se de que mantém a opção ativada.

Passos

1. Clique em **Create Cloud Volumes ONTAP**.
2. Selecione Amazon Web Services como provedor de nuvem e escolha um único nó ou sistema de HA.
3. Preencha a página Detalhes e credenciais.
4. Na página Serviços, deixe o serviço ativado e clique em **continuar**.



5. Complete as páginas no assistente para implantar o sistema.

Resultado

O backup na nuvem está ativado no sistema, faz backup de volumes todos os dias e mantém as cópias de backup mais recentes de 30.

O que se segue?

"Você pode gerenciar backups alterando o agendamento de backup, restaurando volumes e muito mais".

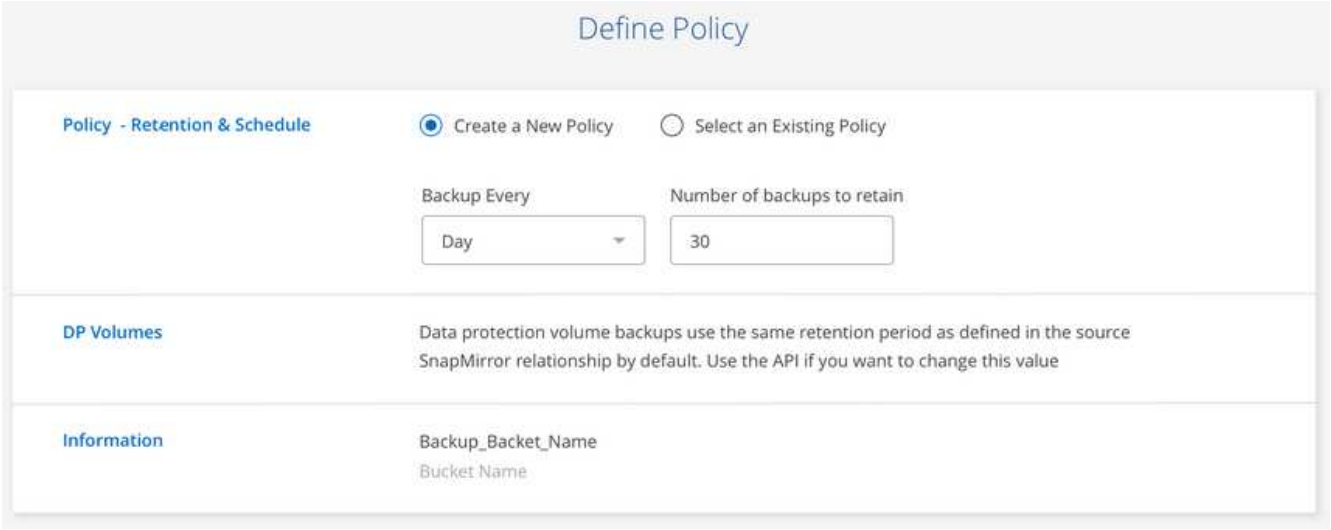
Habilitando o backup para a nuvem em um sistema existente

Habilite o backup na nuvem a qualquer momento diretamente do ambiente de trabalho.

Passos

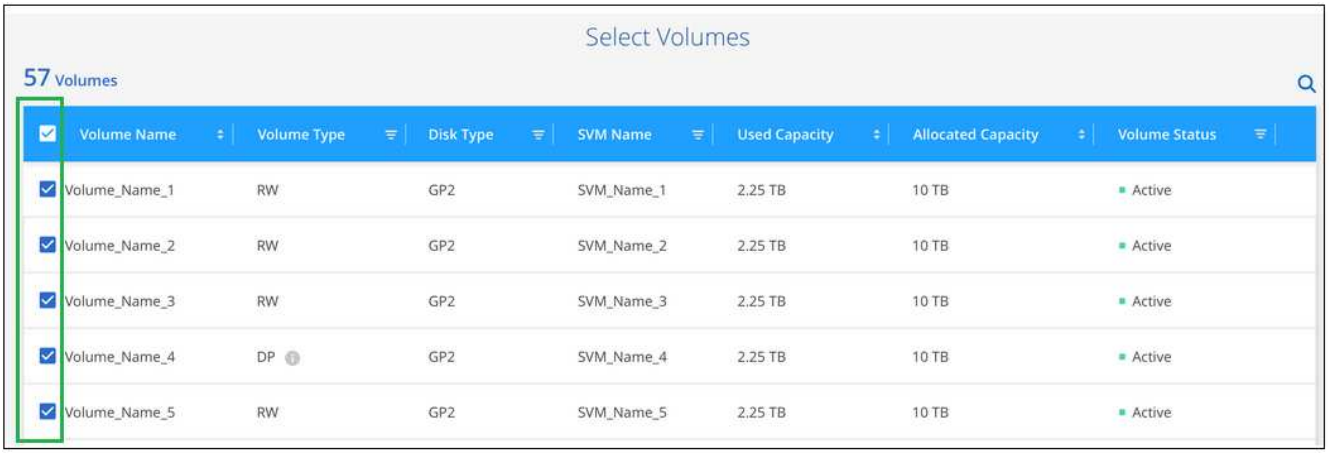
1. Selecione o ambiente de trabalho e clique em **Activate** ao lado do serviço Backup to Cloud no painel direito.

2. Defina o agendamento de backup e o valor de retenção e clique em **continuar**.



"a lista de políticas existentes"Consulte .

3. Selecione os volumes que deseja fazer backup e clique em **Ativar**.



Resultado

O backup na nuvem começa a fazer os backups iniciais de cada volume selecionado.

O que se segue?

"Você pode gerenciar backups alterando o agendamento de backup, restaurando volumes e muito mais".

Fazer backup de dados para o armazenamento Azure Blob

Conclua algumas etapas para começar a fazer backup de dados do Cloud Volumes ONTAP para o armazenamento de Blobs do Azure.

Início rápido

Comece rapidamente seguindo estas etapas ou role para baixo até as seções restantes para obter detalhes completos.

Verifique o suporte para sua configuração

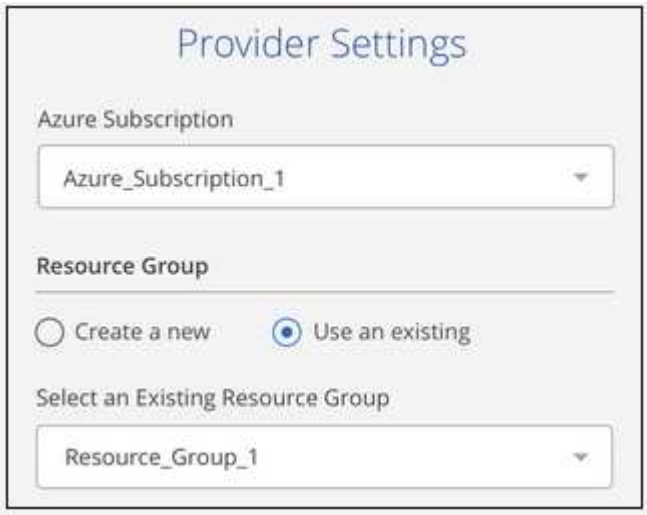
- Você está executando o Cloud Volumes ONTAP 9,7 ou posterior no Azure.
- Você tem uma assinatura válida do provedor de nuvem para o espaço de armazenamento onde seus backups serão localizados.
- Você se inscreveu no "Oferta de backup do Cloud Manager Marketplace", ou comprou "e ativado" uma licença BYOL de backup para nuvem da NetApp.

Habilite o backup na nuvem em seu sistema novo ou existente

- Novos sistemas: O backup para a nuvem é habilitado por padrão no assistente de ambiente de trabalho. Certifique-se de que mantém a opção ativada.
- Sistemas existentes: Selecione o ambiente de trabalho e clique em **Activate** ao lado do serviço Backup to Cloud no painel direito e, em seguida, siga o assistente de configuração.

Introduza os detalhes do fornecedor

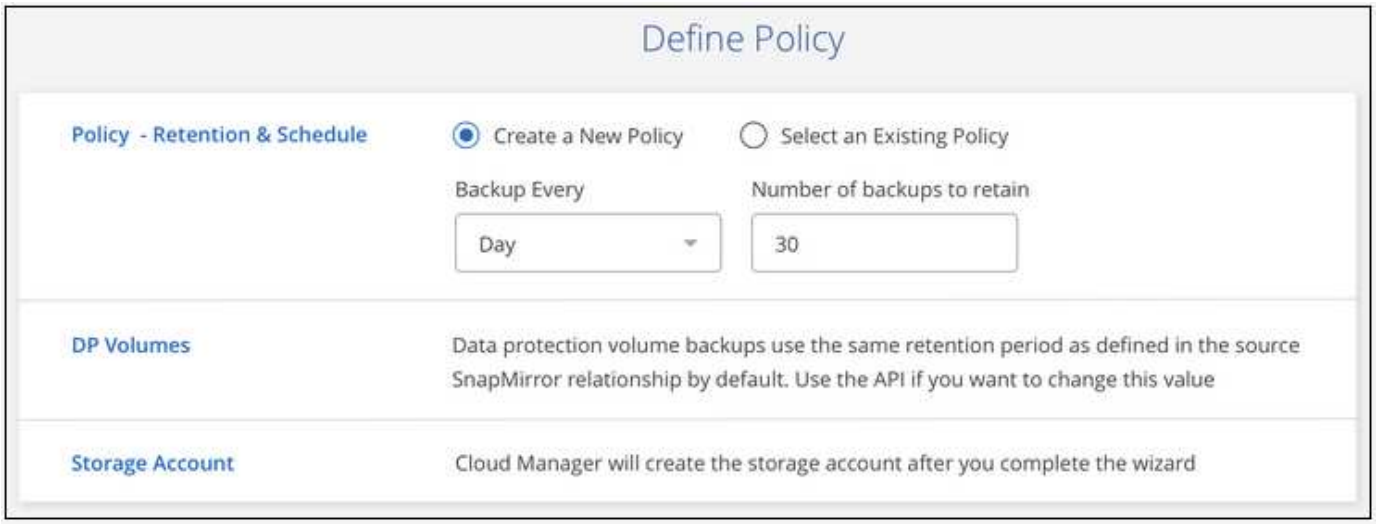
Selecione a assinatura do provedor e escolha se deseja criar um novo grupo de recursos ou usar um grupo de recursos já existente.



Defina a política de cópia de segurança

A política padrão faz backup de volumes todos os dias e retém as 30 cópias de backup mais recentes de cada volume. Altere para backups semanais ou mensais ou selecione uma das políticas definidas pelo sistema que

oferecem mais opções.

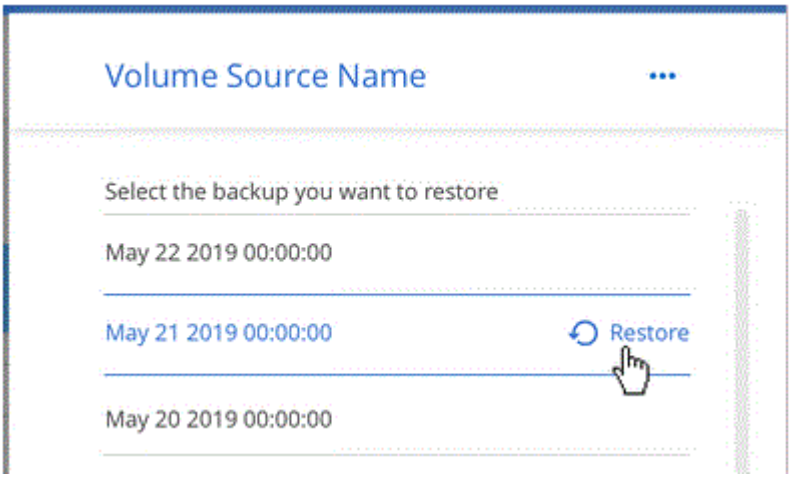


5 Selecione os volumes que deseja fazer backup

Identifique quais volumes você deseja fazer backup na página Selecionar volumes.

6 Restaure seus dados conforme necessário

Na Lista de cópias de segurança, selecione um volume, selecione uma cópia de segurança e, em seguida, restaure os dados da cópia de segurança para um novo volume.



Requisitos

Leia os requisitos a seguir para garantir que você tenha uma configuração com suporte antes de iniciar o backup de volumes no storage Azure Blob.

Versões de ONTAP compatíveis

Cloud Volumes ONTAP 9,7 e posterior.

Regiões Azure compatíveis

O backup na nuvem é compatível com todas as regiões do Azure "Onde o Cloud Volumes ONTAP é suportado" .

Requisitos de licença

Para o licenciamento do Backup to Cloud PAYGO, é necessária uma assinatura pelo Azure Marketplace antes de ativar o Backup to Cloud. A cobrança do Backup to Cloud é feita por meio dessa assinatura. "Pode subscrever a partir da página Detalhes credenciais do assistente do ambiente de trabalho".

Para o licenciamento BYOL do backup para a nuvem, você precisa do número de série da NetApp que permita usar o serviço durante a duração e a capacidade da licença. "Adicionar e atualizar sua licença do Backup BYOL"Consulte .

E você precisa ter uma assinatura do Microsoft Azure para o espaço de armazenamento onde seus backups estarão localizados.

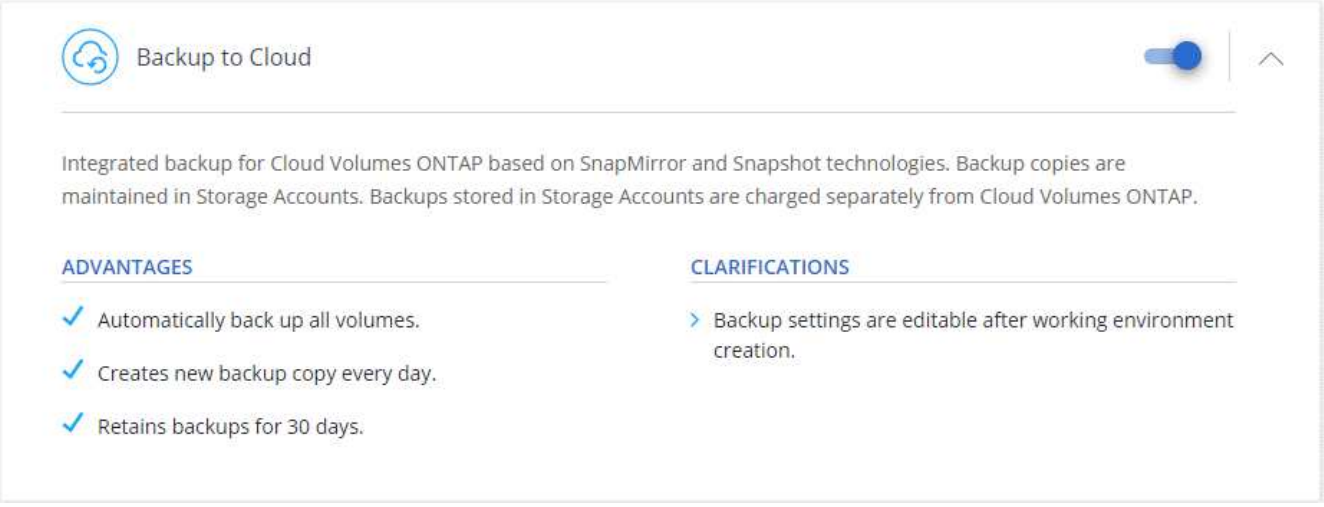
Habilitando o backup para a nuvem em um novo sistema

O backup para a nuvem é habilitado por padrão no assistente de ambiente de trabalho. Certifique-se de que mantém a opção ativada.

Se você quiser escolher o nome do grupo de recursos, **Disable** Backup to Cloud ao implantar o Cloud Volumes ONTAP. Siga as etapas para habilitando o backup na nuvem em um sistema existentehabilitar o backup na nuvem e escolher o grupo de recursos.

Passos

1. Clique em **Create Cloud Volumes ONTAP**.
2. Selecione o Microsoft Azure como fornecedor de nuvem e, em seguida, escolha um único nó ou sistema de HA.
3. Preencha a página Detalhes e credenciais e certifique-se de que existe uma subscrição do Azure Marketplace.
4. Na página Serviços, deixe o serviço ativado e clique em **continuar**.



5. Complete as páginas no assistente para implantar o sistema.

Resultado

O backup na nuvem está ativado no sistema, faz backup de volumes todos os dias e mantém as cópias de backup mais recentes de 30.

O que se segue?

"Você pode gerenciar backups alterando o agendamento de backup, restaurando volumes e muito mais".

Habilitando o backup para a nuvem em um sistema existente

Habilite o backup na nuvem a qualquer momento diretamente do ambiente de trabalho.

Passos

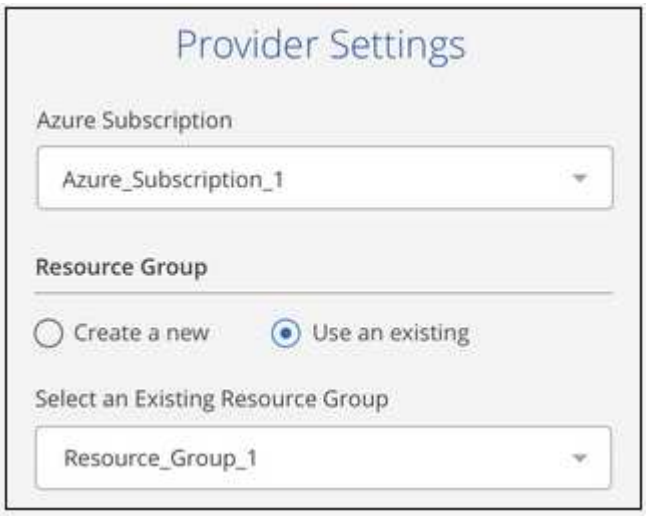
1. Selecione o ambiente de trabalho e clique em **Activate** ao lado do serviço Backup to Cloud no painel direito.

2. Selecione os detalhes do fornecedor:

   a. A assinatura do Azure usada para armazenar os backups.

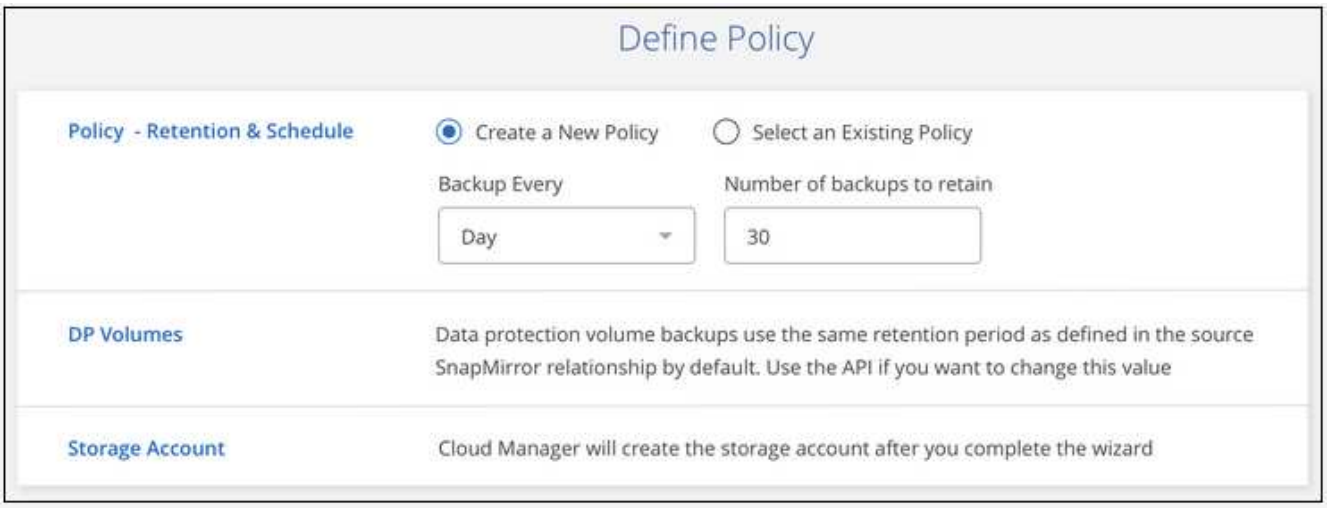
   b. O grupo de recursos - você pode criar um novo grupo de recursos ou selecionar e um grupo de recursos existente.

   c. E, em seguida, clique em **continuar**.



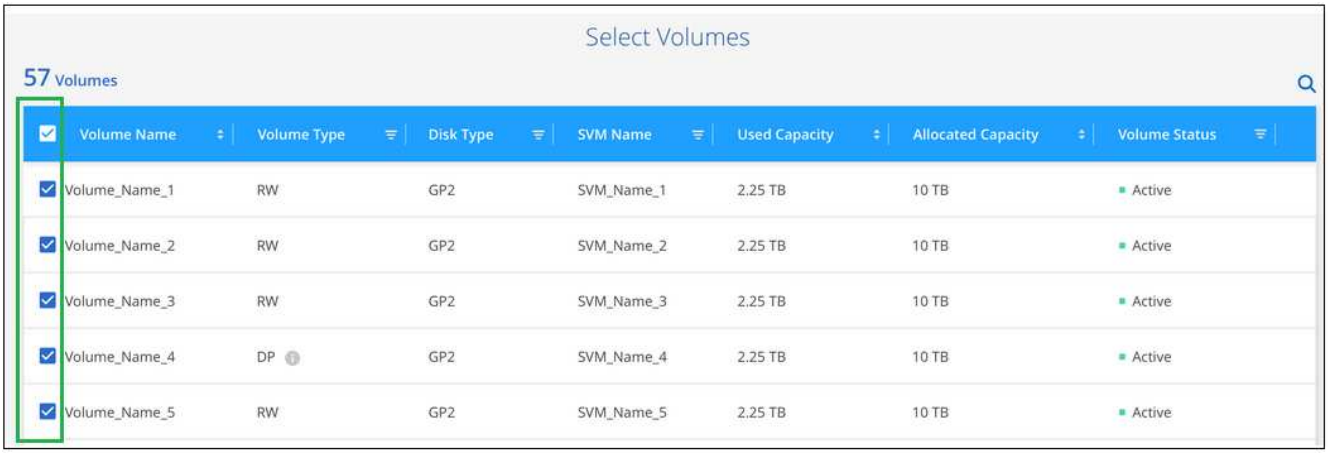
   Observe que você não pode alterar a assinatura ou o grupo de recursos após o início dos serviços.

3. Na página *Definir política*, selecione o agendamento de backup e o valor de retenção e clique em **continuar**.



"a lista de políticas existentes"Consulte .

4. Selecione os volumes que deseja fazer backup e clique em **Ativar**.



Resultado

O backup na nuvem começa a fazer os backups iniciais de cada volume selecionado.

O que se segue?

"Você pode gerenciar backups alterando o agendamento de backup, restaurando volumes e muito mais".

Fazer backup de dados de um sistema ONTAP no local para a nuvem

Conclua algumas etapas para começar a fazer backup de dados do seu sistema ONTAP local para storage de objetos de baixo custo na nuvem.

Início rápido

Comece rapidamente seguindo estas etapas ou role para baixo até as seções restantes para obter detalhes completos.

Verifique o suporte para sua configuração

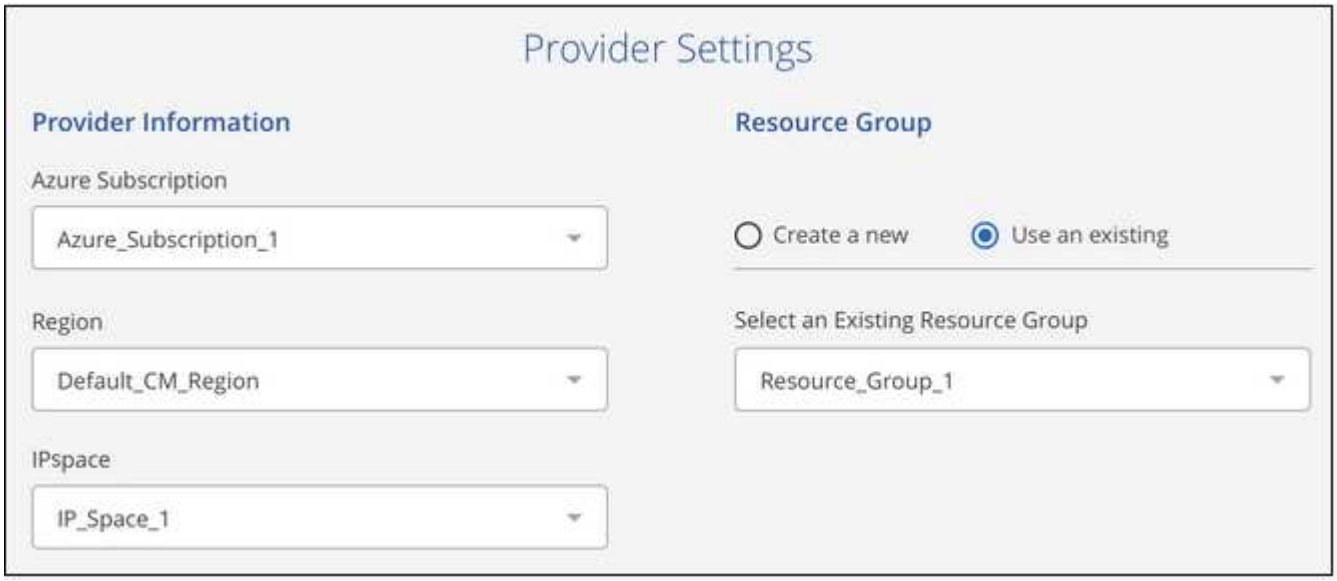
- Você descobriu o cluster no local e o adicionou a um ambiente de trabalho no Cloud Manager. "Descobrindo clusters do ONTAP"Consulte para obter detalhes.
- Você está executando o ONTAP 9.7P5 ou posterior no cluster.
- Você tem uma assinatura válida do provedor de nuvem para o espaço de armazenamento onde seus backups serão localizados.
- Você se inscreveu no "Oferta de backup do Cloud Manager Marketplace", ou comprou "e ativado" uma licença BYOL de backup para nuvem da NetApp.

Habilite o backup na nuvem no sistema

Selecione o ambiente de trabalho e clique em **Activate** ao lado do serviço Backup to Cloud no painel direito e, em seguida, siga o assistente de configuração.

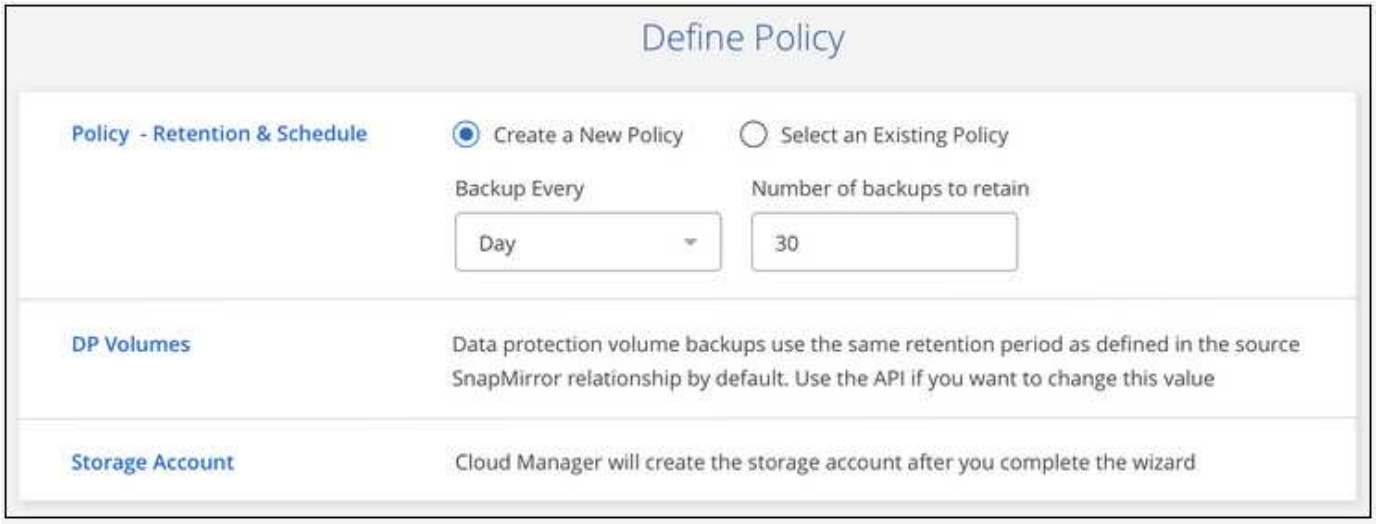
Selecione o provedor de nuvem e insira os detalhes do provedor

Selecione o fornecedor e, em seguida, selecione a subscrição do fornecedor, a região e o grupo de recursos. Você também precisa especificar o espaço de IPspace no cluster do ONTAP onde os volumes residem.



Defina a política de cópia de segurança

A política padrão faz backup de volumes todos os dias e retém as 30 cópias de backup mais recentes de cada volume. Altere para backups semanais ou mensais ou selecione uma das políticas definidas pelo sistema que oferecem mais opções.

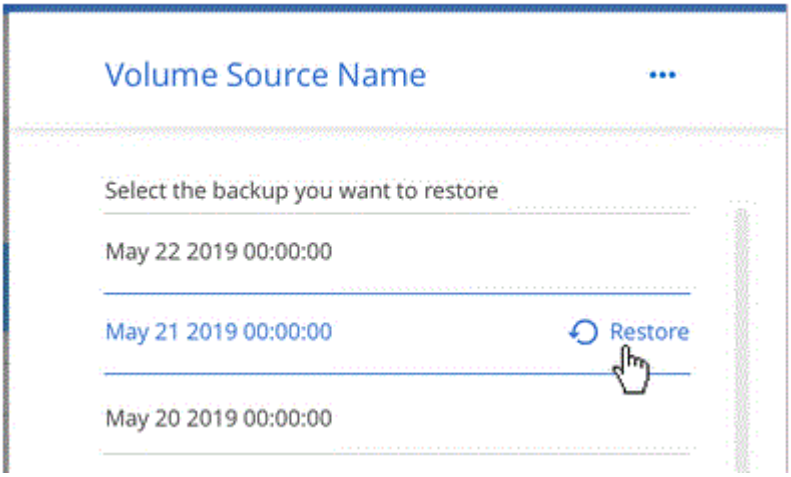


5 Selecione os volumes que deseja fazer backup

Identifique quais volumes você deseja fazer backup do cluster.

6 Restaure seus dados conforme necessário

Na Lista de backup, selecione um volume, selecione um backup e restaure os dados do backup para um novo volume em um sistema Cloud Volumes ONTAP que esteja usando o mesmo provedor de nuvem.



Requisitos

Leia os requisitos a seguir para garantir que você tenha uma configuração com suporte antes de iniciar o backup de volumes no armazenamento Blob do Azure.

Versões de ONTAP compatíveis

ONTAP 9.7P5 e posterior.

Requisitos de rede de cluster

É necessário um LIF entre clusters em cada nó do ONTAP que hospeda os volumes que você deseja fazer backup. O LIF deve estar associado ao *IPspace* que o ONTAP deve usar para se conetar ao armazenamento de objetos. O SVM Admin deve residir no IPspace. "Saiba mais sobre IPspaces".

Ao configurar o backup na nuvem, você será solicitado a usar o IPspace. Você deve escolher o espaço IPspace ao qual cada LIF está associado. Esse pode ser o espaço IPspace "padrão" ou um espaço IPspace personalizado que você criou.

Regiões Azure compatíveis

O backup na nuvem é compatível com todas as regiões do Azure "onde o cloud volumes é compatível" .

Requisitos de licença

Para o licenciamento do Backup to Cloud PAYGO, é necessária uma assinatura do "Oferta de backup do Azure Marketplace Cloud Manager" antes de ativar o Backup to Cloud. A cobrança do Backup to Cloud é feita por meio dessa assinatura.

Para o licenciamento BYOL do backup para a nuvem, você precisa do número de série da NetApp que permita usar o serviço durante a duração e a capacidade da licença. "Adicionar e atualizar sua licença do Backup BYOL"Consulte .

E você precisa ter uma assinatura do Microsoft Azure para o espaço de armazenamento onde seus backups estarão localizados.

Habilitando o backup na nuvem

Habilite o backup na nuvem a qualquer momento diretamente do ambiente de trabalho.

Passos

1. Selecione o ambiente de trabalho e clique em **Activate** ao lado do serviço Backup to Cloud no painel direito.

2. Selecione o fornecedor e, em seguida, introduza os detalhes do fornecedor:

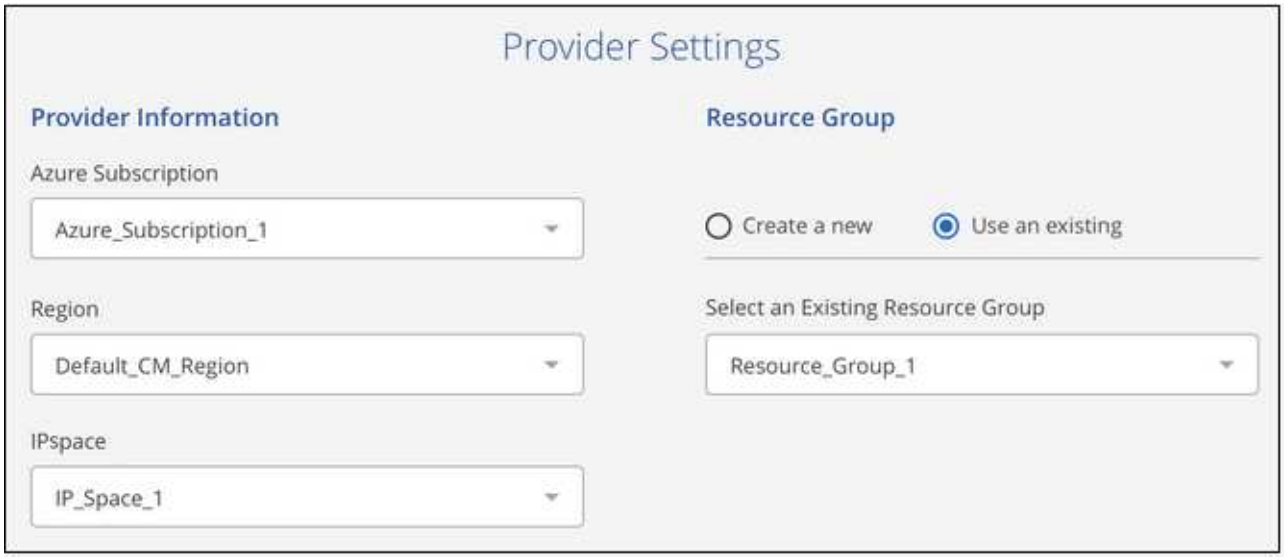
   a. A assinatura do Azure usada para armazenar os backups.

   b. A região do Azure.

   c. O grupo de recursos - você pode criar um novo grupo de recursos ou selecionar e um grupo de recursos existente.

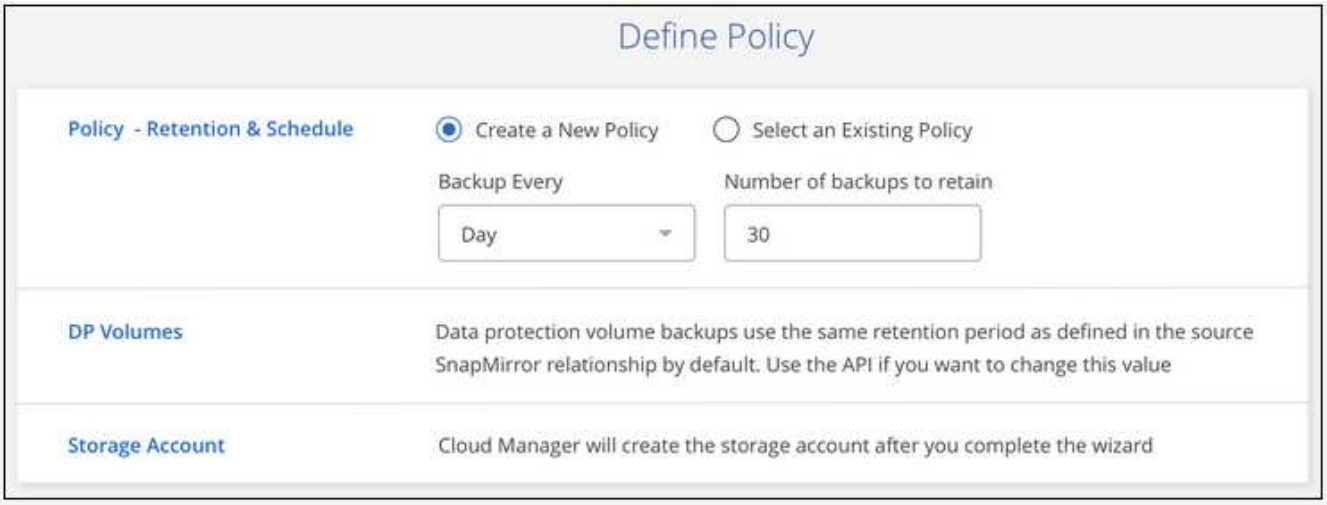
   d. O espaço de IPspace no cluster do ONTAP onde residem os volumes que você deseja fazer backup.

   e. E, em seguida, clique em **continuar**.



Observe que você não pode alterar a assinatura ou o grupo de recursos após o início dos serviços.

3. Na página *Definir política*, selecione o agendamento de backup e o valor de retenção e clique em **continuar**.



"a lista de políticas existentes"Consulte .

4. Selecione os volumes que deseja fazer backup e clique em **Ativar**.

Resultado

O backup na nuvem começa a fazer os backups iniciais de cada volume selecionado.

O que se segue?

"Você pode gerenciar backups alterando o agendamento de backup, restaurando volumes e muito mais".

Gerenciamento de backups para sistemas Cloud Volumes ONTAP e ONTAP locais

Gerencie backups para sistemas Cloud Volumes ONTAP e ONTAP locais alterando o agendamento de backup, restaurando volumes, excluindo backups e muito mais.

Alteração da retenção de agendamento e backup

A política padrão faz backup de volumes todos os dias e retém as 30 cópias de backup mais recentes de cada volume. Você pode alterar para backups semanais ou mensais e pode alterar o número de cópias de backup a serem mantidas. Você também pode selecionar uma das políticas definidas pelo sistema que fornece backups programados para 3 meses, 1 ano e 7 anos.

A alteração da política de backup afeta apenas novos volumes criados após a alteração da programação. Isso não afeta a programação de nenhum volume existente.

Passos

1. Selecione o ambiente de trabalho.
2. Clique e selecione **Backup Settings**.

3. Na página *Backup Settings*, clique ••• em para o ambiente de trabalho e selecione **Modify Backup Policy**.

4. Na página *Modificar política de backup*, altere a retenção de agendamento e backup e clique em **Salvar**.

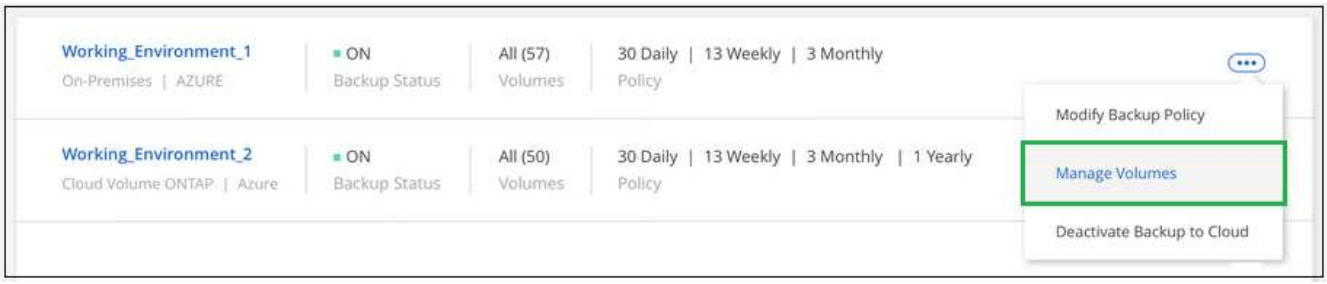
Iniciar e parar backups de volumes

Você pode parar de fazer backup de um volume se não precisar de cópias de backup desse volume e não quiser pagar pelo custo para armazenar os backups. Você também pode adicionar um novo volume à lista de backup se ele não estiver sendo feito o backup no momento.

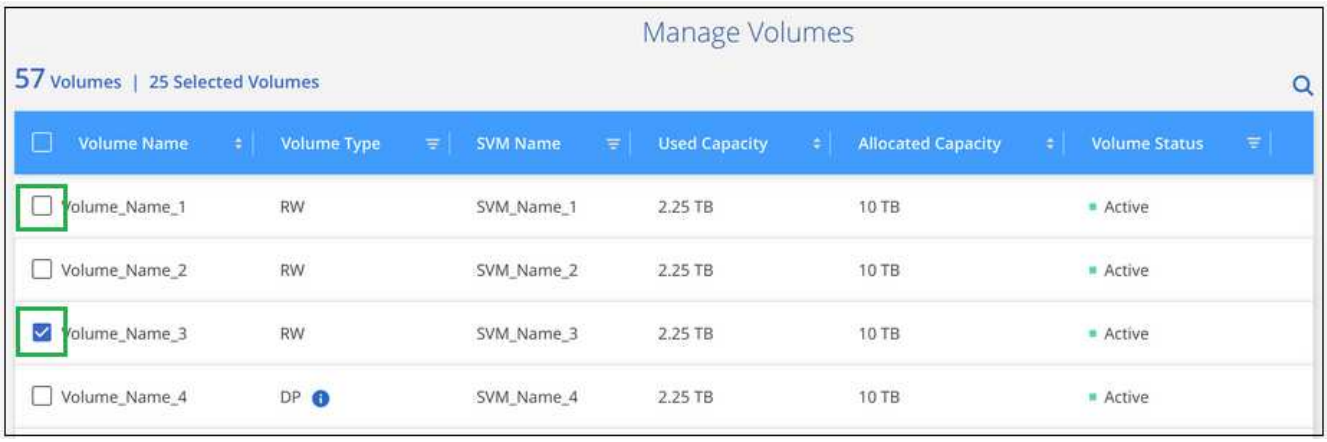
Passos

1. Selecione o ambiente de trabalho.
2. Clique ⋮ e selecione **Backup Settings**.

3. Na página *Configurações de backup*, clique ••• em para o ambiente de trabalho e selecione **Gerenciar volumes**.



4. Marque a caixa de seleção para volumes que deseja iniciar o backup e desmarque a caixa de seleção para volumes que deseja interromper o backup.



Observação: ao impedir que um volume seja feito backup, você continuará sendo cobrado pelo provedor de nuvem pelos custos de armazenamento de objetos pela capacidade que os backups usam, a menos que você exclua os backups.

Restaurar um volume a partir de uma cópia de segurança

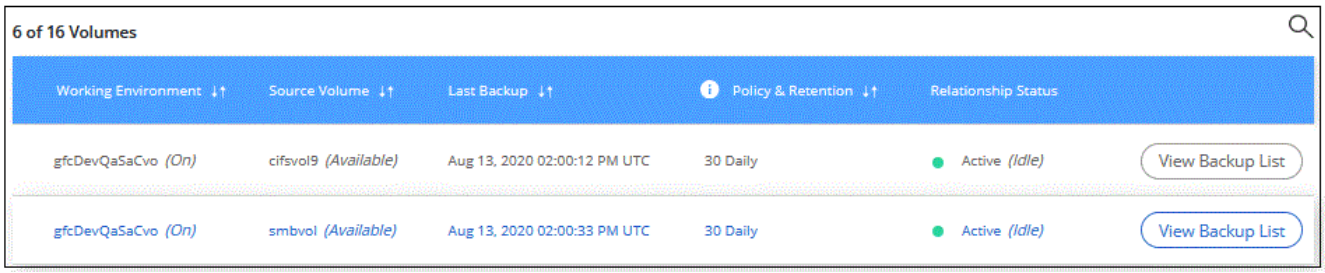
Quando você restaura dados de um backup, o Cloud Manager cria um volume *new* usando os dados do backup. Você pode restaurar os dados para um volume no mesmo ambiente de trabalho ou para um ambiente de trabalho diferente localizado na mesma conta de nuvem que o ambiente de trabalho de origem. Como o backup não contém nenhum instantâneo, o volume recém-restaurado também não.

Os backups criados a partir de sistemas ONTAP no local podem ser restaurados apenas para sistemas Cloud Volumes ONTAP que usam o mesmo fornecedor de nuvem que reside no backup.

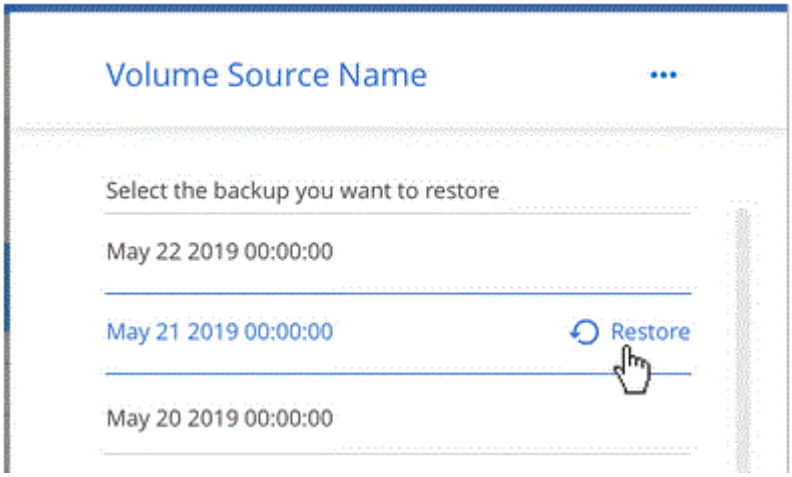
Passos

1. Selecione o ambiente de trabalho.
2. Clique e selecione **Ver backups**.

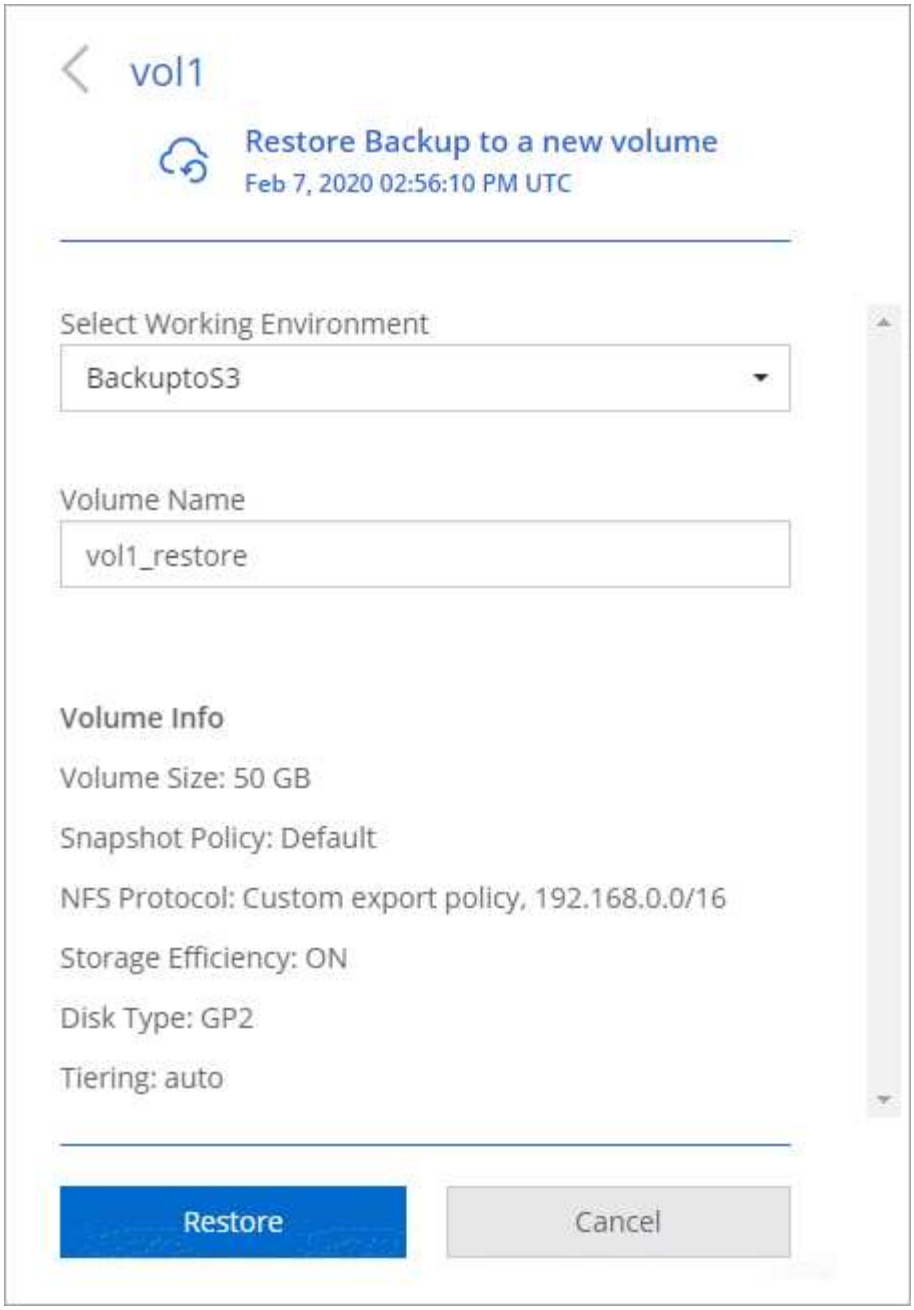
3. Selecione a linha para o volume que deseja restaurar e clique em **Exibir lista de backup**.



4. Localize o backup que você deseja restaurar e clique no ícone **Restaurar**.



5. Preencha a página *Restore Backup to new volume*:
   a. Selecione o ambiente de trabalho para o qual pretende restaurar o volume.
   b. Introduza um nome para o volume.
   c. Clique em **Restaurar**.



Resultado

O Cloud Manager cria um novo volume com base no backup selecionado. Você pode "gerencie esse novo volume"como necessário.

Eliminar cópias de segurança

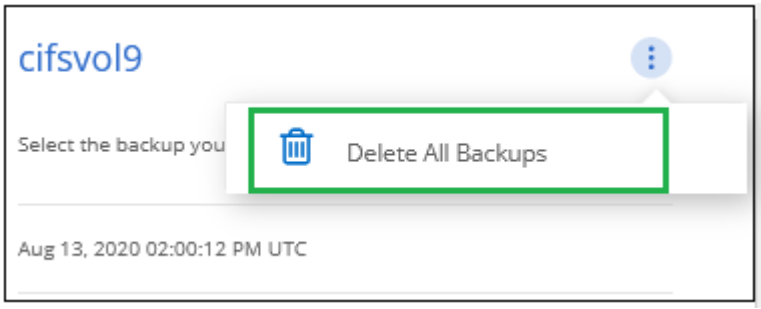
O Backup to Cloud permite que você exclua *todos* backups de um volume específico. Você não pode excluir *individuais* backups.

Você pode fazer isso se não precisar mais dos backups ou se você excluir o volume de origem e quiser remover todos os backups.

Se você pretende excluir um sistema Cloud Volumes ONTAP ou ONTAP local que tenha backups, exclua os backups **antes** de excluir o sistema. O Backup to Cloud não exclui backups automaticamente quando você exclui um sistema e não há suporte atual na IU para excluir os backups depois que o sistema for excluído.

Passos

1. Na parte superior do Cloud Manager, clique em **Backup**.
2. Na lista de volumes, localize o volume e clique em **Exibir lista de backup**.
3. Clique ••• e selecione **Excluir todos os backups**.



4. Na caixa de diálogo de confirmação, clique em **Excluir**.

Desativação do backup na nuvem

A desativação do Backup na nuvem para um ambiente de trabalho desativa os backups de cada volume no sistema e também desativa a capacidade de restaurar um volume. Quaisquer backups existentes não serão excluídos.

Observe que você continuará sendo cobrado pelo seu provedor de nuvem pelos custos de storage de objetos pela capacidade que seus backups usam, a menos que você exclua os backups.

Passos

1. Selecione o ambiente de trabalho.
2. Clique ⋮ e selecione **Backup Settings**.

3. Na página *Backup Settings*, clique ••• em para o ambiente de trabalho e selecione **Deactivate Backup to Cloud**.

4. Na caixa de diálogo de confirmação, clique em **Desativar**.

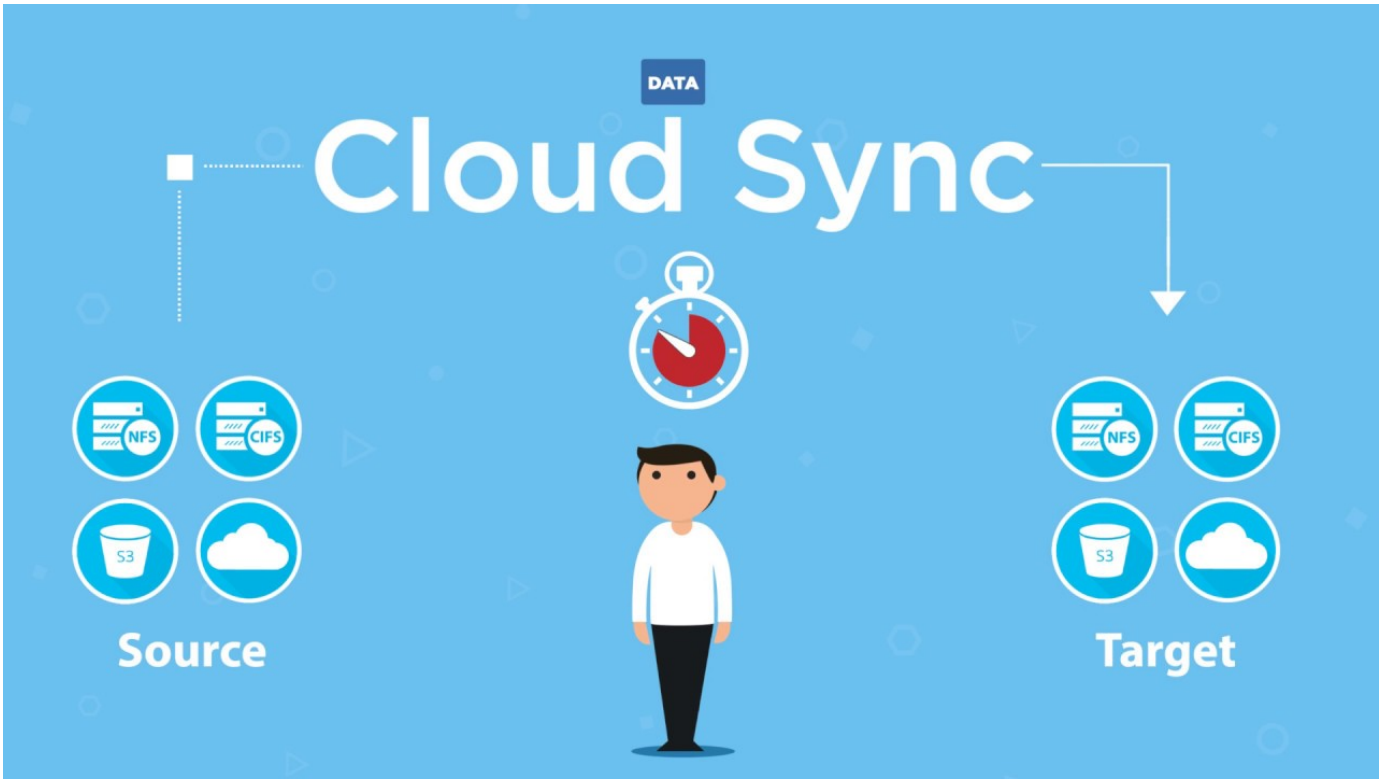
Copiar e sincronizar dados

Visão geral do Cloud Sync

O serviço NetApp Cloud Sync oferece uma maneira simples, segura e automatizada de migrar seus dados para qualquer destino, na nuvem ou no local. Seja um conjunto de dados nas baseado em arquivo (NFS ou SMB), formato de objeto Amazon Simple Storage Service (S3), um dispositivo NetApp StorageGRID ou qualquer outro armazenamento de objetos de fornecedor de nuvem, o Cloud Sync pode convertê-lo e movê-lo para você.

Caraterísticas

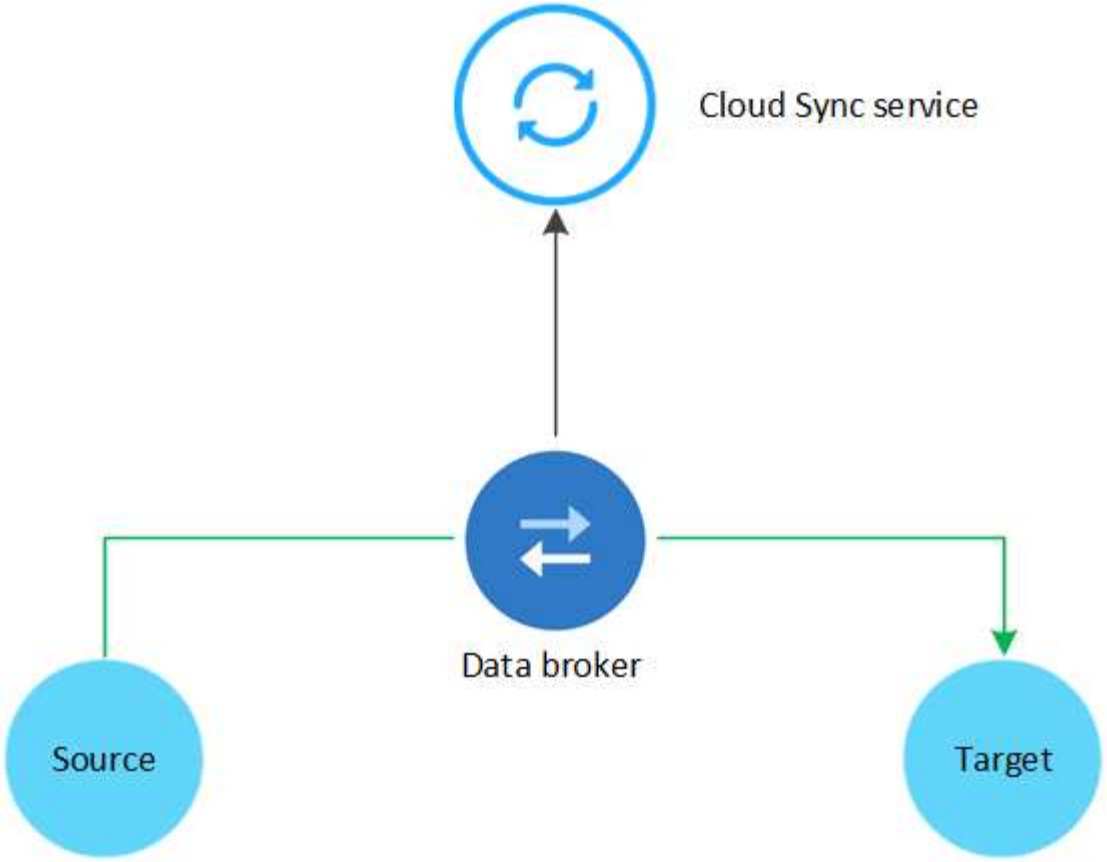
Assista ao vídeo a seguir para uma visão geral do Cloud Sync:



Como o Cloud Sync funciona

O Cloud Sync é uma plataforma de software como serviço (SaaS) que consiste em um agente de dados, uma interface baseada em nuvem disponível pelo Cloud Manager e uma fonte e destino.

A imagem a seguir mostra a relação entre os componentes do Cloud Sync:



O software de corretor de dados NetApp sincroniza dados de uma origem para um destino (isso é chamado de *relação de sincronização*). Você pode executar o agente de dados na AWS, Azure, Google Cloud Platform ou no local. O corretor de dados precisa de uma conexão de saída de Internet pela porta 443 para que possa se comunicar com o serviço Cloud Sync e entrar em Contato com alguns outros serviços e repositórios. "Exibir a lista de endpoints".

Após a cópia inicial, o serviço sincroniza todos os dados alterados com base na programação definida.

Tipos de armazenamento suportados

O Cloud Sync é compatível com os seguintes tipos de storage:

- Qualquer servidor NFS
- Qualquer servidor SMB
- AWS EFS
- AWS S3
- Blob do Azure
- Azure NetApp Files
- Cloud Volumes Service
- Cloud Volumes ONTAP
- Google Cloud Storage
- IBM Cloud Object Storage
- Cluster ONTAP on-premises

- Storage ONTAP S3
- StorageGRID

"Reveja as relações de sincronização suportadas".

Custo

Existem dois tipos de custos associados ao uso do Cloud Sync: Taxas de recursos e taxas de serviço.

Cobranças de recursos

As cobranças de recursos estão relacionadas aos custos de computação e storage para executar o agente de dados na nuvem.

Taxas de serviço

Há duas maneiras de pagar pelas relações de sincronização após o término da avaliação gratuita de 14 dias. A primeira opção é se inscrever na AWS ou no Azure, o que permite que você pague por hora ou anualmente. A segunda opção é comprar licenças diretamente da NetApp. Leia as seções a seguir para obter mais detalhes.

Subscrição do mercado

A assinatura do serviço Cloud Sync da AWS ou Azure permite que você pague por uma taxa por hora ou pague anualmente. "Você pode se inscrever na AWS ou no Azure", dependendo de onde você deseja ser cobrado.

Assinaturas por hora

Com uma assinatura paga conforme o uso por hora, o serviço Cloud Sync cobra por hora com base no número de relacionamentos de sincronização criados.

- "Ver preços no Azure"
- "Veja a definição de preço para pagamento conforme o uso na AWS"

Assinaturas anuais

Uma assinatura anual fornece uma licença para 20 relacionamentos de sincronização que você paga antecipadamente. Se você passar acima de 20 relacionamentos de sincronização e se inscreveu através do Azure, você paga pelas relações adicionais por hora.

"Veja os preços anuais na AWS"

Licenças da NetApp

Outra forma de pagar antecipadamente pelas relações de sincronização é comprando licenças diretamente da NetApp. Cada licença permite criar até 20 relações de sincronização.

Você pode usar essas licenças com uma assinatura da AWS ou do Azure. Por exemplo, se você tiver 25 relacionamentos de sincronização, poderá pagar pelas primeiras 20 relações de sincronização usando uma licença e pagar conforme o uso da AWS ou do Azure com as 5 relações de sincronização restantes.

"Saiba como comprar licenças e adicioná-las ao Cloud Sync".

Termos da licença

Os clientes que comprarem uma licença bring Your own License (BYOL) para o serviço Cloud Sync devem estar cientes das limitações associadas ao direito de licença.

- Os clientes têm o direito de utilizar a licença BYOL por um prazo não superior a um ano a partir da data de entrega.
- Os clientes têm o direito de utilizar a licença BYOL para estabelecer e não exceder um total de 20 conexões individuais entre uma fonte e um destino (cada uma uma uma "relação de sincronização").
- O direito de um cliente expira na conclusão do prazo de licença de um ano, independentemente de o Cliente ter atingido a limitação de relação de sincronização de 20.
- No caso de o Cliente optar por renovar a sua licença, as relações de sincronização não utilizadas associadas à concessão de licença anterior NÃO serão transferidas para a renovação da licença.

Privacidade de dados

O NetApp não tem acesso a quaisquer credenciais que você fornecer ao usar o serviço Cloud Sync. As credenciais são armazenadas diretamente na máquina do data broker, que reside na sua rede.

Dependendo da configuração escolhida, o Cloud Sync poderá solicitar credenciais ao criar uma nova relação. Por exemplo, ao configurar um relacionamento que inclua um servidor SMB ou ao implantar o agente de dados na AWS.

Essas credenciais são sempre salvas diretamente no próprio corretor de dados. O agente de dados reside em uma máquina em sua rede, seja no local ou na sua conta na nuvem. As credenciais nunca são disponibilizadas ao NetApp.

As credenciais são criptografadas localmente na máquina do corretor de dados usando o HashiCorp Vault.

Limitações

- O Cloud Sync não é suportado na China.
- Além da China, o corretor de dados Cloud Sync não é suportado nas seguintes regiões:
  - AWS GovCloud (EUA)
  - Azure US Gov
  - Azure US DoD

Comece agora

Início rápido para Cloud Sync

A introdução ao serviço Cloud Sync inclui alguns passos.

Prepare sua fonte e destino

Verifique se sua origem e destino são suportados e configurados. O requisito mais importante é verificar a conetividade entre o agente de dados e os locais de origem e destino. "Saiba mais".

Prepare um local para o agente de dados do NetApp

O software de corretor de dados NetApp sincroniza dados de uma origem para um destino (isso é chamado de *relação de sincronização*). Você pode executar o agente de dados na AWS, Azure, Google Cloud Platform ou no local. O corretor de dados precisa de uma conexão de saída de Internet pela porta 443 para que possa se comunicar com o serviço Cloud Sync e entrar em Contato com alguns outros serviços e repositórios. "Exibir a lista de endpoints".

O Cloud Sync orienta você pelo processo de instalação quando você cria uma relação de sincronização, momento em que você pode implantar o agente de dados na nuvem ou baixar um script de instalação para seu próprio host Linux.

- "Revise a instalação da AWS"
- "Revise a instalação do Azure"
- "Revise a instalação da GCP"
- "Revise a instalação do host Linux"

Crie sua primeira relação de sincronização

Faça login no "Cloud Manager", clique em **Sincronizar** e arraste e solte suas seleções para a origem e destino. Siga as instruções para concluir a configuração. "Saiba mais".

Pague pelos seus relacionamentos de sincronização depois que a avaliação gratuita terminar

Inscreva-se na AWS ou Azure para pagar conforme o uso ou pagar anualmente. Ou compre licenças diretamente da NetApp. Basta ir para a página Configurações de Licença no Cloud Sync para configurá-lo. "Saiba mais".

Preparando a fonte e o alvo

Prepare-se para sincronizar dados verificando se sua origem e destino são suportados e configurados.

Relações de sincronização suportadas

O Cloud Sync permite sincronizar dados de uma origem para um destino (isso é chamado de *relação de sincronização*). Você deve entender os relacionamentos suportados antes de começar.

Localização da origem	Locais de destino suportados
AWS EFS	• AWS EFS • AWS S3 • Blob do Azure • Azure NetApp Files (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Servidor NFS • Cluster ONTAP on-premises • StorageGRID
AWS S3	• AWS EFS • AWS S3 • Blob do Azure • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • IBM Cloud Object Storage • Google Cloud Storage • Servidor NFS • Cluster ONTAP on-premises • SMB Server • StorageGRID

Localização da origem	Locais de destino suportados
Blob do Azure	• AWS EFS • AWS S3 • Blob do Azure • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • IBM Cloud Object Storage • Servidor NFS • Cluster ONTAP on-premises • SMB Server • StorageGRID
Azure NetApp Files (NFS)	• AWS EFS • AWS S3 • Blob do Azure • Azure NetApp Files (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Servidor NFS • Cluster ONTAP on-premises • StorageGRID
Azure NetApp Files (SMB)	• AWS S3 • Blob do Azure • Azure NetApp Files (SMB) • Cloud Volumes ONTAP (SMB) • Cloud Volumes Service (SMB) • Google Cloud Storage • IBM Cloud Object Storage • Cluster ONTAP on-premises • SMB Server • StorageGRID

Localização da origem	Locais de destino suportados
Cloud Volumes ONTAP (NFS)	• AWS EFS • AWS S3 • Blob do Azure • Azure NetApp Files (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Servidor NFS • Cluster ONTAP on-premises • StorageGRID
Cloud Volumes ONTAP (SMB)	• AWS S3 • Blob do Azure • Azure NetApp Files (SMB) • Cloud Volumes ONTAP (SMB) • Cloud Volumes Service (SMB) • Google Cloud Storage • IBM Cloud Object Storage • Cluster ONTAP on-premises • SMB Server • StorageGRID
Cloud Volumes Service (NFS)	• AWS EFS • AWS S3 • Blob do Azure • Azure NetApp Files (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Servidor NFS • Cluster ONTAP on-premises • StorageGRID

Localização da origem	Locais de destino suportados
Cloud Volumes Service (SMB)	• AWS S3 • Blob do Azure • Azure NetApp Files (SMB) • Cloud Volumes ONTAP (SMB) • Cloud Volumes Service (SMB) • Google Cloud Storage • IBM Cloud Object Storage • Cluster ONTAP on-premises • SMB Server • StorageGRID
Google Cloud Storage	• AWS EFS • AWS S3 • Blob do Azure • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • IBM Cloud Object Storage • Servidor NFS • Cluster ONTAP on-premises • SMB Server • StorageGRID
IBM Cloud Object Storage	• AWS EFS • AWS S3 • Blob do Azure • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • IBM Cloud Object Storage • Servidor NFS • Cluster ONTAP on-premises • SMB Server • StorageGRID

Localização da origem	Locais de destino suportados
Servidor NFS	• AWS EFS • AWS S3 • Blob do Azure • Azure NetApp Files (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Servidor NFS • Cluster ONTAP on-premises • StorageGRID
Cluster ONTAP on-premise (NFS)	• AWS EFS • AWS S3 • Blob do Azure • Azure NetApp Files (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Servidor NFS • Cluster ONTAP on-premises • StorageGRID
Cluster ONTAP on-premise (SMB)	• AWS S3 • Blob do Azure • Azure NetApp Files (SMB) • Cloud Volumes ONTAP (SMB) • Cloud Volumes Service (SMB) • Google Cloud Storage • IBM Cloud Object Storage • Cluster ONTAP on-premises • SMB Server • StorageGRID
Storage ONTAP S3	• StorageGRID

Localização da origem	Locais de destino suportados
Servidor SMB	• AWS S3 • Blob do Azure • Azure NetApp Files (SMB) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Cluster ONTAP on-premises • SMB Server • StorageGRID
StorageGRID	• AWS EFS • AWS S3 • Blob do Azure • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • IBM Cloud Object Storage • Google Cloud Storage • Servidor NFS • Cluster ONTAP on-premises • Storage ONTAP S3 • SMB Server • StorageGRID

Notas:

1. Você pode escolher uma categoria de storage específica do Azure Blob quando um contêiner de Blob é o destino:
    - Armazenamento a quente
    - Armazenamento frio
2. você pode escolher uma classe de armazenamento S3 específica quando o AWS S3 é o destino:
    - Standard (esta é a classe padrão)
    - Disposição em camadas inteligente
    - Acesso padrão-infrequente
    - Uma zona de acesso pouco frequente
    - Glacier

- Glacier Deep Archive

Rede para a origem e o destino

- A origem e o destino devem ter uma conexão de rede com o corretor de dados.

  Por exemplo, se um servidor NFS estiver no data center e o agente de dados estiver na AWS, você precisará de uma conexão de rede (VPN ou Direct Connect) da rede para a VPC.

- A NetApp recomenda configurar o agente de origem, destino e dados para usar um serviço de protocolo de tempo de rede (NTP). A diferença de tempo entre os três componentes não deve exceder 5 minutos.

Requisitos de origem e destino

Verifique se sua origem e seus destinos atendem aos seguintes requisitos.

requisitos de bucket do AWS S3

Certifique-se de que seu bucket do AWS S3 atenda aos seguintes requisitos.

Localizações de corretores de dados compatíveis para AWS S3

As relações de sincronização que incluem o storage S3 exigem que um agente de dados seja implantado na AWS ou no local. Em ambos os casos, o Cloud Sync solicita que você associe o agente de dados a uma conta da AWS durante a instalação.

- "Saiba como implantar o agente de dados da AWS"
- "Saiba como instalar o corretor de dados em um host Linux"

Regiões AWS compatíveis

Todas as regiões são suportadas, exceto as regiões China e GovCloud (EUA).

Permissões necessárias para buckets do S3 em outras contas da AWS

Ao configurar um relacionamento de sincronização, você pode especificar um bucket do S3 que reside em uma conta da AWS que não está associada ao agente de dados.

"As permissões incluídas neste arquivo JSON" Deve ser aplicado a esse bucket do S3 para que o agente de dados possa acessá-lo. Essas permissões permitem que o agente de dados copie dados de e para o bucket e liste os objetos no bucket.

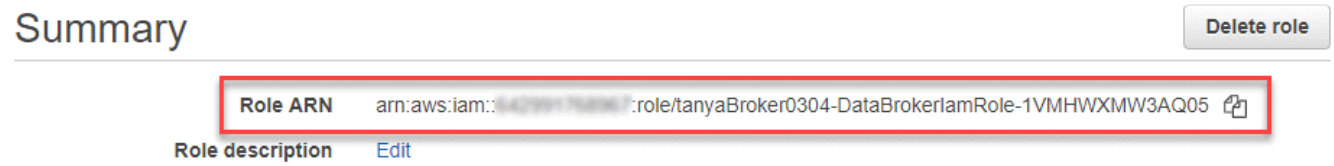
Observe o seguinte sobre as permissões incluídas no arquivo JSON:

1. *<BucketName>* é o nome do bucket que reside na conta da AWS que não está associado ao corretor de dados.
2. *<RoleARN>* deve ser substituído por um dos seguintes:

   - Se o corretor de dados foi instalado manualmente em um host Linux, *RoleARN* deve ser o ARN do usuário da AWS para o qual você forneceu credenciais da AWS ao implantar o corretor de dados.
   - Se o corretor de dados foi implantado na AWS usando o modelo CloudFormation, *RoleARN* deve ser o ARN da função IAM criada pelo modelo.

     Você pode encontrar a função ARN indo para o console EC2, selecionando a instância do data broker

e clicando na função IAM na guia Descrição. Você deve então ver a página Resumo no console do IAM que contém a função ARN.



requisitos de armazenamento de Blobs do Azure

Certifique-se de que seu storage Azure Blob atenda aos requisitos a seguir.

Localizações de corretores de dados compatíveis para Azure Blob

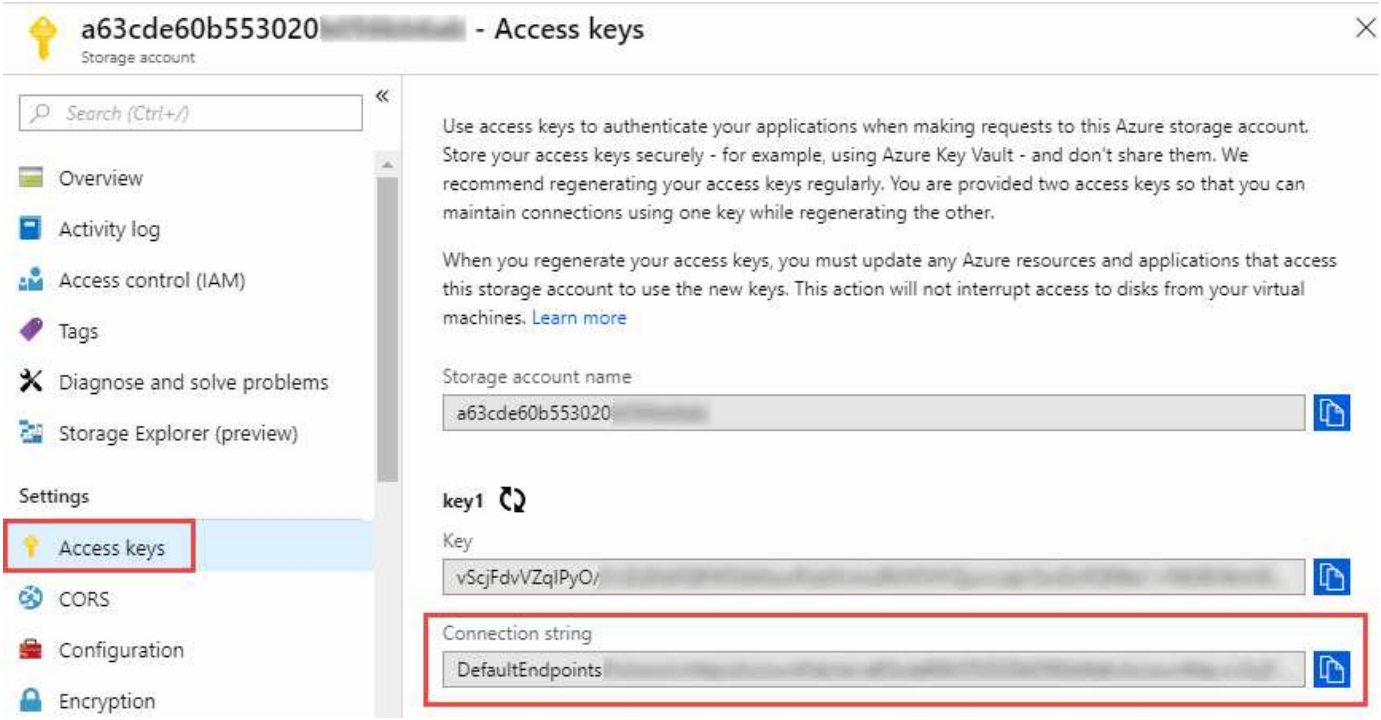
O agente de dados pode residir em qualquer local quando uma relação de sincronização inclui o armazenamento Azure Blob.

Regiões Azure compatíveis

Todas as regiões são suportadas, exceto as regiões China, US Gov e US DoD.

Cadeia de conexão necessária para relacionamentos que incluem Azure Blob e NFS/SMB

Ao criar uma relação de sincronização entre um contêiner de Blob do Azure e um servidor NFS ou SMB, você precisa fornecer à Cloud Sync a cadeia de conexão de conta de storage:

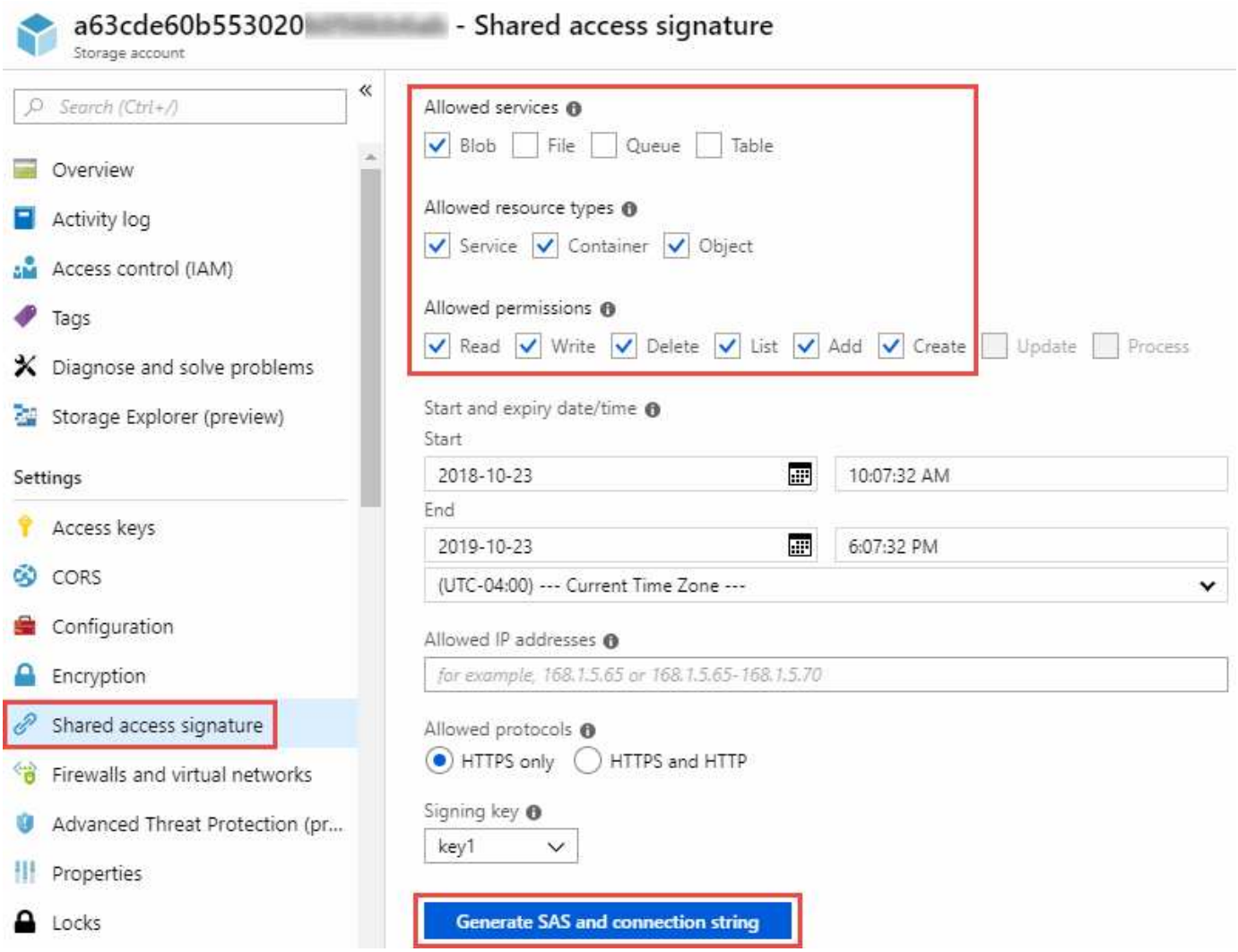


Se você quiser sincronizar dados entre dois contentores Blob do Azure, a cadeia de conexão deve incluir um "assinatura de acesso compartilhado" (SAS). Você também tem a opção de usar um SAS ao sincronizar entre um contêiner Blob e um servidor NFS ou SMB.

O SAS deve permitir acesso ao serviço Blob e a todos os tipos de recursos (Serviço, contêiner e Objeto). O

SAS também deve incluir as seguintes permissões:

- Para o contentor Blob de origem: Leitura e Lista
- Para o contentor Blob de destino: Leitura, gravação, Lista, Adicionar e criar



Requisito Azure NetApp Files

Use o nível de serviço Premium ou Ultra ao sincronizar dados com ou a partir do Azure NetApp Files. Você pode ter falhas e problemas de desempenho se o nível de serviço de disco for padrão.

Consulte um arquiteto de soluções se precisar de ajuda para determinar o nível de serviço certo. O tamanho do volume e a camada de volume determinam a taxa de transferência que você pode obter.

"Saiba mais sobre os níveis de serviço e a taxa de transferência do Azure NetApp Files".

Requisitos de bucket do Google Cloud Storage

Certifique-se de que seu bucket do Google Cloud Storage atenda aos seguintes requisitos.

Localizações de corretores de dados compatíveis com o Google Cloud Storage

Relacionamentos de sincronização que incluem o Google Cloud Storage exigem que um agente de dados seja implantado no GCP ou no local. O Cloud Sync orienta você pelo processo de instalação do data broker quando você cria uma relação de sincronização.

- "Saiba como implantar o agente de dados da GCP"
- "Saiba como instalar o corretor de dados em um host Linux"

Regiões GCP compatíveis

Todas as regiões são suportadas.

Requisitos do servidor NFS

- O servidor NFS pode ser um sistema NetApp ou um sistema que não seja NetApp.
- O servidor de arquivos deve permitir que o host do data broker acesse as exportações.
- As versões de NFS 3, 4,0, 4,1 e 4,2 são compatíveis.

  A versão desejada deve estar ativada no servidor.

- Se você quiser sincronizar dados NFS de um sistema ONTAP, verifique se o acesso à lista de exportação NFS de um SVM está ativado (vserver nfs modificar -vserver *svm_name* -showmount habilitado).

  A configuração padrão para showmount é *enabled* começando com ONTAP 9.2.

Requisitos de storage do ONTAP S3

O ONTAP 9.7 oferece suporte ao Amazon Simple Storage Service (Amazon S3) como uma prévia pública. "Saiba mais sobre o suporte do ONTAP para o Amazon S3".

Ao configurar uma relação de sincronização que inclua o armazenamento ONTAP S3, você precisará fornecer o seguinte:

- O endereço IP do LIF conetado ao ONTAP S3
- A chave de acesso e a chave secreta que o ONTAP está configurado para usar

Requisitos de servidor SMB

- O servidor SMB pode ser um sistema NetApp ou um sistema que não seja NetApp.
- O servidor de arquivos deve permitir que o host do data broker acesse as exportações.
- As versões SMB 1,0, 2,0, 2,1, 3,0 e 3,11 são suportadas.
- Conceda ao grupo "Administradores" permissões "Controle total" para as pastas de origem e destino.

  Se você não conceder essa permissão, o corretor de dados pode não ter permissões suficientes para obter as ACLs em um arquivo ou diretório. Se isso ocorrer, você receberá o seguinte erro: "Erro getxattr 95"

Limitação SMB para diretórios e arquivos ocultos

Uma limitação SMB afeta diretórios e arquivos ocultos ao sincronizar dados entre servidores SMB. Se algum dos diretórios ou arquivos no servidor SMB de origem estiver oculto pelo Windows, o atributo oculto não será copiado para o servidor SMB de destino.

Comportamento de sincronização SMB devido a limitação de insensibilidade de caso

O protocolo SMB é insensível a maiúsculas e minúsculas, o que significa que as letras maiúsculas e minúsculas são tratadas como sendo as mesmas. Esse comportamento pode resultar em arquivos sobrescritos e erros de cópia de diretório, se uma relação de sincronização incluir um servidor SMB e os dados já existirem no destino.

Por exemplo, digamos que há um arquivo chamado "a" na origem e um arquivo chamado "A" no destino. Quando o Cloud Sync copia o arquivo chamado "a" para o destino, o arquivo "A" é substituído pelo arquivo "a" da origem.

No caso dos diretórios, digamos que há um diretório chamado "b" na fonte e um diretório chamado "B" no destino. Quando o Cloud Sync tenta copiar o diretório chamado "b" para o destino, o Cloud Sync recebe um erro que diz que o diretório já existe. Como resultado, o Cloud Sync sempre falha em copiar o diretório chamado "B."

A melhor maneira de evitar essa limitação é garantir que você sincronize dados para um diretório vazio.

Permissões para um destino SnapMirror

Se a origem de um relacionamento de sincronização for um destino SnapMirror (que é somente leitura), as permissões "leitura/lista" são suficientes para sincronizar dados da origem para um destino.

Visão geral de rede para Cloud Sync

A rede para Cloud Sync inclui conetividade entre o agente de dados e os locais de origem e destino, e uma conexão de saída à Internet do agente de dados através da porta 443.

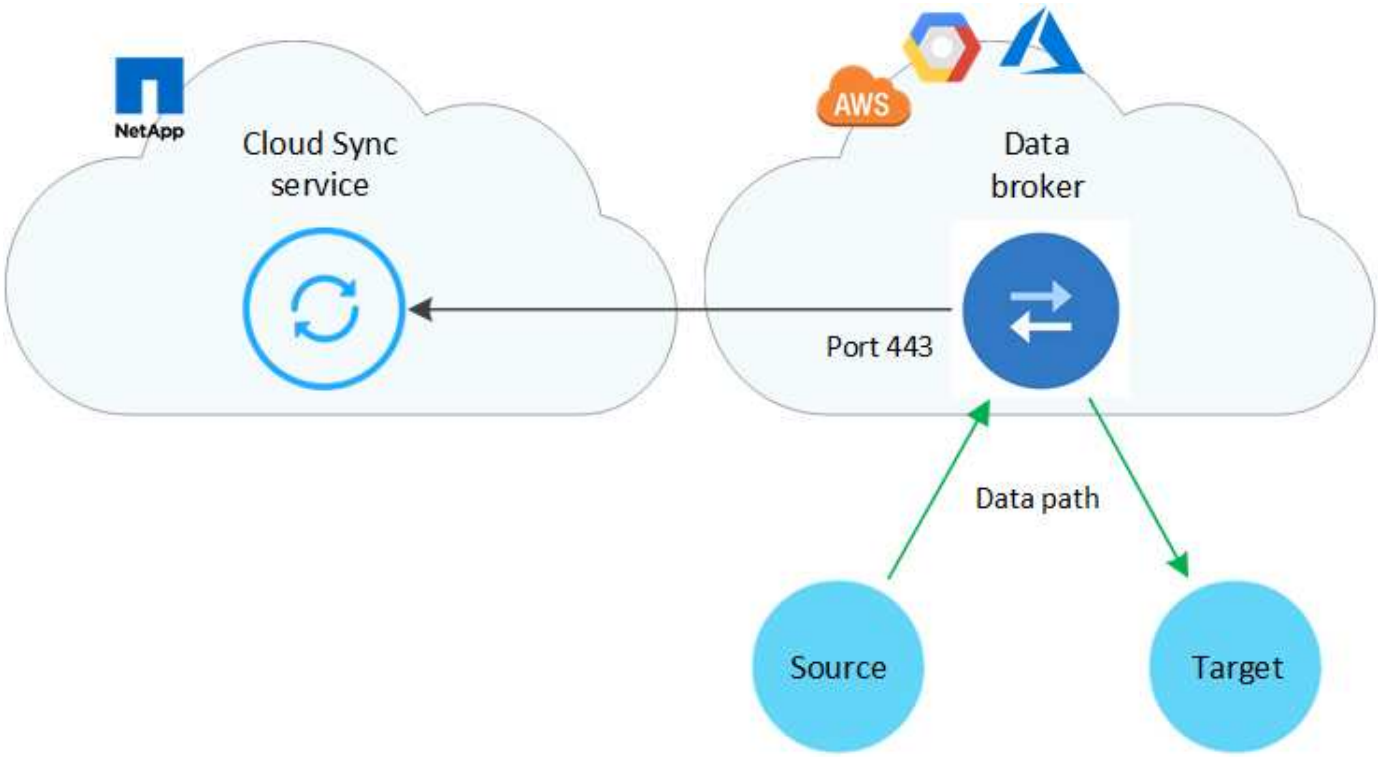
Localização do agente de dados

É possível instalar o agente de dados na nuvem ou no local.

Agente de dados na nuvem

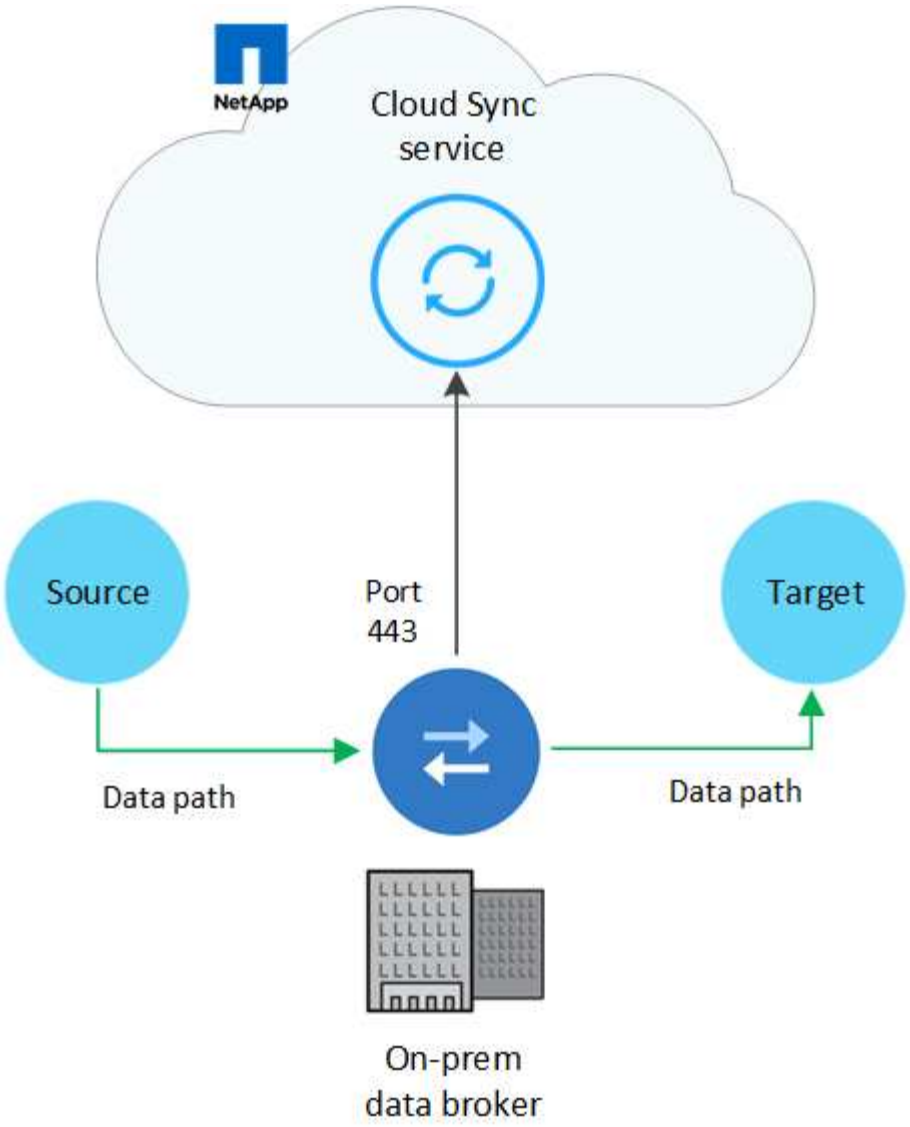
A imagem a seguir mostra o agente de dados em execução na nuvem, na AWS, GCP ou Azure. A origem e o destino podem estar em qualquer local, desde que haja uma conexão com o corretor de dados. Por exemplo, você pode ter uma conexão VPN do seu data center para o seu provedor de nuvem.

Quando o Cloud Sync implanta o agente de dados na AWS, Azure ou GCP, ele cria um grupo de segurança que ativa a comunicação de saída necessária.



Agente de dados no local

A imagem a seguir mostra o agente de dados em execução no local, em um data center. Novamente, a fonte e o alvo podem estar em qualquer local, desde que haja uma conexão com o corretor de dados.



Requisitos de rede

- A origem e o destino devem ter uma conexão de rede com o corretor de dados.

  Por exemplo, se um servidor NFS estiver no data center e o agente de dados estiver na AWS, você precisará de uma conexão de rede (VPN ou Direct Connect) da rede para a VPC.

- O corretor de dados precisa de uma conexão de saída de Internet para que possa pesquisar o serviço Cloud Sync para tarefas na porta 443.
- A NetApp recomenda configurar o agente de origem, destino e dados para usar um serviço de protocolo de tempo de rede (NTP). A diferença de tempo entre os três componentes não deve exceder 5 minutos.

Endpoints de rede

O corretor de dados NetApp requer acesso de saída à Internet pela porta 443 para se comunicar com o serviço Cloud Sync e entrar em Contato com alguns outros serviços e repositórios. Seu navegador da Web local também requer acesso a endpoints para determinadas ações. Se você precisar limitar a conetividade de saída, consulte a seguinte lista de endpoints ao configurar seu firewall para tráfego de saída.

Pontos de extremidade do agente de dados

O corretor de dados entra em Contato com os seguintes pontos finais:

Endpoints	Finalidade
olcentgbl.trafficmanager.net:443	Para entrar em Contato com um repositório para atualizar pacotes CentOS para o host do data broker. Esse endpoint é contatado somente se você instalar manualmente o data broker em um host CentOS.
rpm.nodesource.com:443 registry.npmjs.org:443 nodejs.org:443	Para contatar repositórios para atualizar o Node.js, npm e outros pacotes de 3rd partes usados no desenvolvimento.
tgz.pm2.io:443	Para acessar um repositório para atualizar o PM2, que é um pacote de 3rd partes usado para monitorar o Cloud Sync.
sqs.us-east-1.amazonaws.com:443 kinesis.us-east-1.amazonaws.com:443	Para entrar em Contato com os serviços da AWS que o Cloud Sync usa para operações (enfileirando arquivos, registrando ações e fornecendo atualizações para o agente de dados).
s3.*region*.amazonaws.com:443 por exemplo: s3.us-east-2.amazonaws.com:443 "Consulte a documentação da AWS para obter uma lista de endpoints do S3"	Para entrar em Contato com o Amazon S3 quando um relacionamento de sincronização incluir um bucket do S3.
cf.cloudsync.NetApp.com:443 repo.cloudsync.NetApp.com:443	Para contactar o serviço Cloud Sync.
support.NetApp.com:443	Para entrar em Contato com o suporte da NetApp ao usar uma licença BYOL para relacionamentos de sincronização.
fedoraproject.org:443	Para instalar o 7z na máquina virtual do corretor de dados durante a instalação e atualizações. O 7z é necessário para enviar mensagens AutoSupport para o suporte técnico da NetApp.

Endpoints do navegador da Web

O seu navegador da Web precisa de acesso ao seguinte ponto final para transferir registos para fins de resolução de problemas:

logs.cloudsync.NetApp.com:443

Como instalar um corretor de dados

Instalar o agente de dados na AWS

Quando você cria um relacionamento de sincronização, escolha a opção AWS Data Broker para implantar o software de corretor de dados em uma nova instância do EC2 em uma VPC. O Cloud Sync orienta você pelo processo de instalação, mas os requisitos e etapas são repetidos nesta página para ajudá-lo a se preparar para a instalação.

Você também tem a opção de instalar o agente de dados em um host Linux existente na nuvem ou no local. "Saiba mais".

Regiões AWS compatíveis

Todas as regiões são suportadas, exceto as regiões China e GovCloud (EUA).

Requisitos de rede

- O corretor de dados precisa de uma conexão de saída de Internet para que possa pesquisar o serviço Cloud Sync para tarefas na porta 443.

  Quando o Cloud Sync implanta o agente de dados na AWS, ele cria um grupo de segurança que permite a comunicação de saída necessária. Observe que você pode configurar o agente de dados para usar um servidor proxy durante o processo de instalação.

  Se precisar limitar a conetividade de saída, "a lista de endpoints que o corretor de dados entra em contato"consulte .

- A NetApp recomenda configurar o agente de origem, destino e dados para usar um serviço de protocolo de tempo de rede (NTP). A diferença de tempo entre os três componentes não deve exceder 5 minutos.

Permissões necessárias para implantar o agente de dados na AWS

A conta de usuário da AWS que você usa para implantar o agente de dados deve ter as permissões incluídas no "Esta política fornecida pela NetApp".

requisitos para usar sua própria função do IAM com o agente de dados da AWS

Quando o Cloud Sync implanta o agente de dados, ele cria uma função do IAM para a instância do agente de dados. Você pode implantar o agente de dados usando sua própria função do IAM, se preferir. Você pode usar essa opção se sua organização tiver políticas de segurança rígidas.

A função do IAM deve atender aos seguintes requisitos:

- O serviço EC2 deve ter permissão para assumir a função IAM como uma entidade confiável.
- "As permissões definidas neste arquivo JSON" Deve ser anexado à função do IAM para que o corretor de dados possa funcionar corretamente.

Siga as etapas abaixo para especificar a função do IAM ao implantar o corretor de dados.

Instalar o agente de dados

Você pode instalar um agente de dados na AWS ao criar um relacionamento de sincronização.

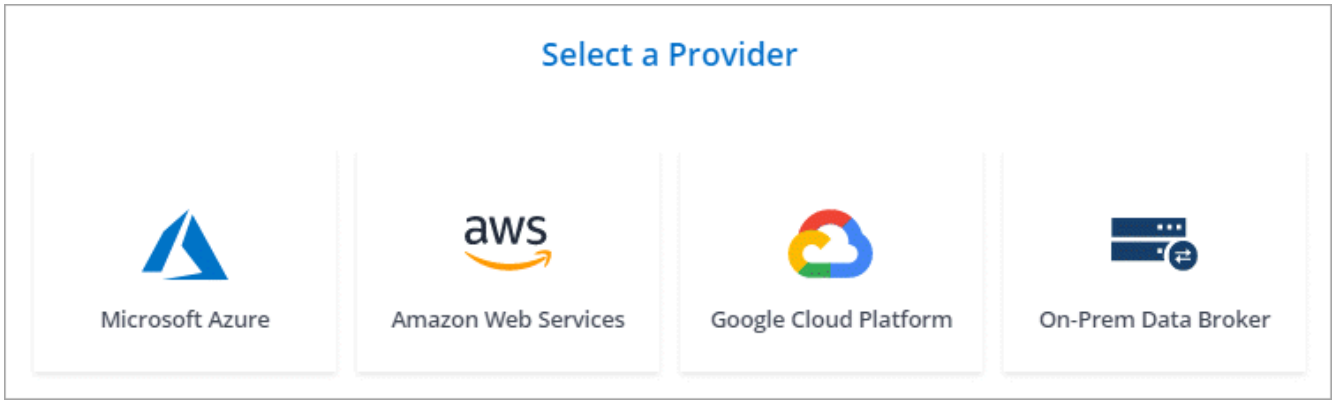
Passos

1. Clique em **criar nova sincronização**.
2. Na página **Definir relação de sincronização**, escolha uma fonte e destino e clique em **continuar**.

   Conclua as etapas até chegar à página **Data Broker**.

3. Na página **Data Broker**, clique em **Create Data Broker** e selecione **Amazon Web Services**.

   Se você já tem um corretor de dados, você precisará clicar no  ícone primeiro.



4. Digite um nome para o corretor de dados e clique em **continuar**.
5. Insira uma chave de acesso da AWS para que o Cloud Sync possa criar o agente de dados na AWS em seu nome.

   As chaves não são salvas ou usadas para quaisquer outros fins.

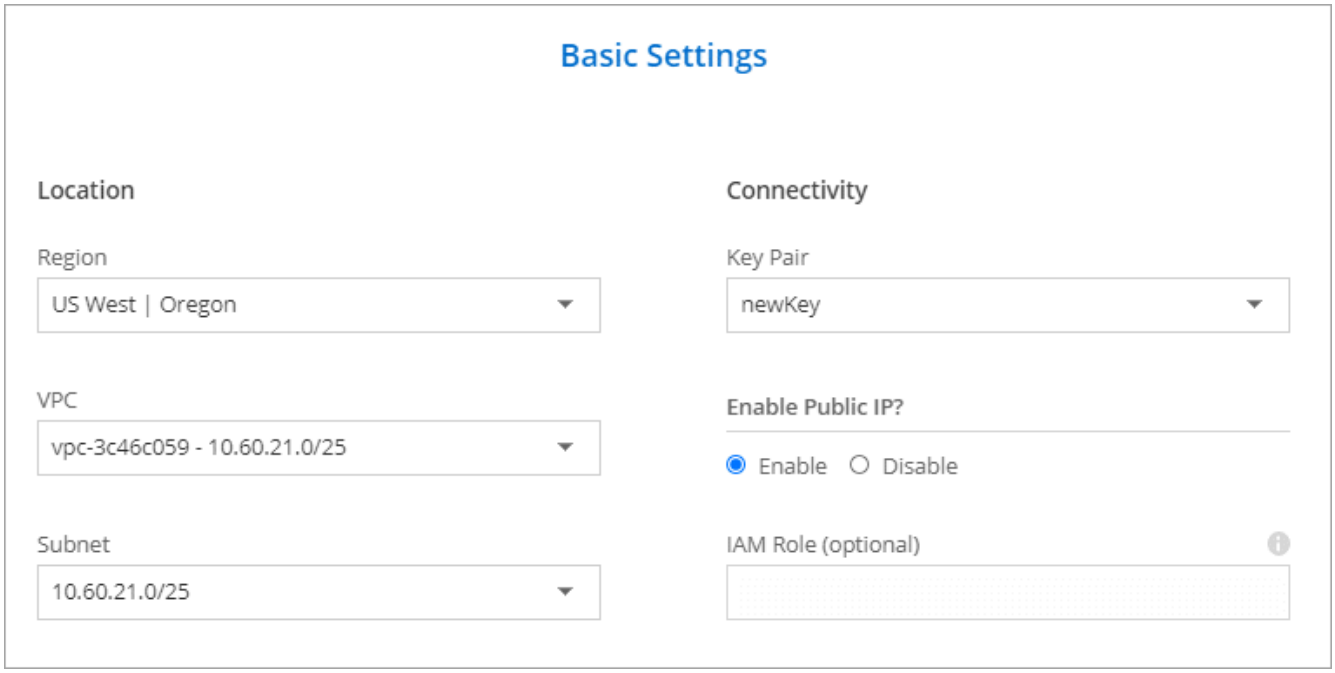
   Se você preferir não fornecer chaves de acesso, clique no link na parte inferior da página para usar um modelo do CloudFormation. Ao usar essa opção, você não precisa fornecer credenciais porque está fazendo login diretamente na AWS.

   o vídeo a seguir mostra como iniciar a instância do data broker usando um modelo do CloudFormation:

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

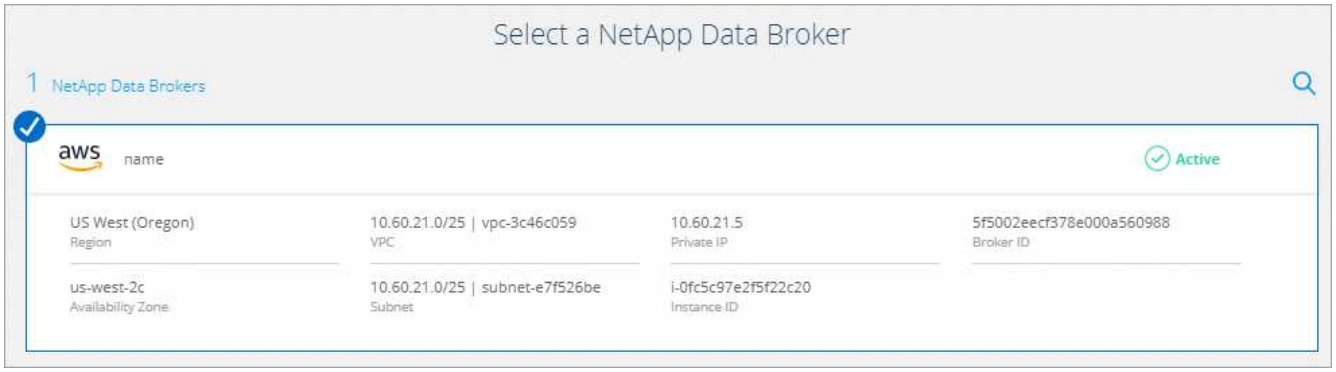
6. Se você inseriu uma chave de acesso da AWS, selecione um local para a instância, selecione um par de chaves, escolha se deseja habilitar um endereço IP público e, em seguida, selecione uma função do IAM existente ou deixe o campo em branco para que o Cloud Sync crie a função para você.

   Se você escolher sua própria função do IAM, você precisará fornecer as permissões necessárias.



7. Depois que o corretor de dados estiver disponível, clique em **continuar** no Cloud Sync.

A imagem a seguir mostra uma instância implantada com sucesso na AWS:



8. Complete as páginas no assistente para criar a nova relação de sincronização.

Resultado

Você implantou um agente de dados na AWS e criou uma nova relação de sincronização. Você pode usar esse corretor de dados com relações de sincronização adicionais.

Instalar o corretor de dados no Azure

Ao criar uma relação de sincronização, escolha a opção Agente de dados do Azure para implantar o software de corretor de dados em uma nova máquina virtual em uma VNet. O Cloud Sync orienta você pelo processo de instalação, mas os requisitos e etapas são repetidos nesta página para ajudá-lo a se preparar para a instalação.

Você também tem a opção de instalar o agente de dados em um host Linux existente na nuvem ou no local. "Saiba mais".

Regiões Azure compatíveis

Todas as regiões são suportadas, exceto as regiões China, US Gov e US DoD.

Requisitos de rede

- O corretor de dados precisa de uma conexão de saída de Internet para que possa pesquisar o serviço Cloud Sync para tarefas na porta 443.

  Quando o Cloud Sync implanta o agente de dados no Azure, ele cria um grupo de segurança que permite a comunicação de saída necessária.

  Se precisar limitar a conetividade de saída, "a lista de endpoints que o corretor de dados entra em contato"consulte .

- A NetApp recomenda configurar o agente de origem, destino e dados para usar um serviço de protocolo de tempo de rede (NTP). A diferença de tempo entre os três componentes não deve exceder 5 minutos.

Método de autenticação

Ao implantar o corretor de dados, você precisará escolher um método de autenticação: Uma senha ou um par de chaves SSH público-privadas.

Para obter ajuda sobre a criação de um par de chaves, "Documentação do Azure: Crie e use um par de

chaves SSH público-privada para VMs Linux no Azure" consulte .

Instalar o agente de dados

Você pode instalar um corretor de dados no Azure quando criar uma relação de sincronização.

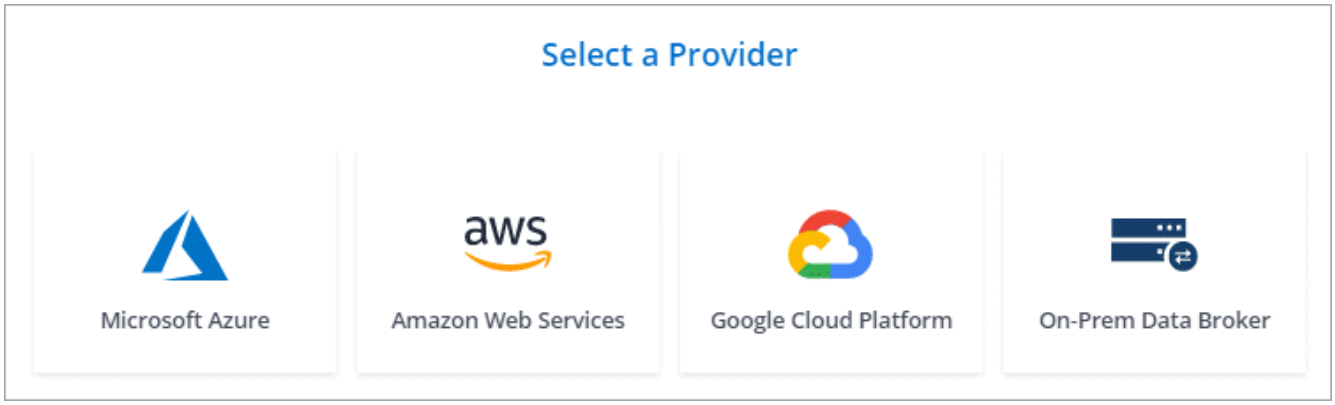
Passos

1. Clique em **criar nova sincronização**.
2. Na página **Definir relação de sincronização**, escolha uma fonte e destino e clique em **continuar**.

   Complete as páginas até chegar à página **Data Broker**.

3. Na página **Data Broker**, clique em **Create Data Broker** e selecione **Microsoft Azure**.

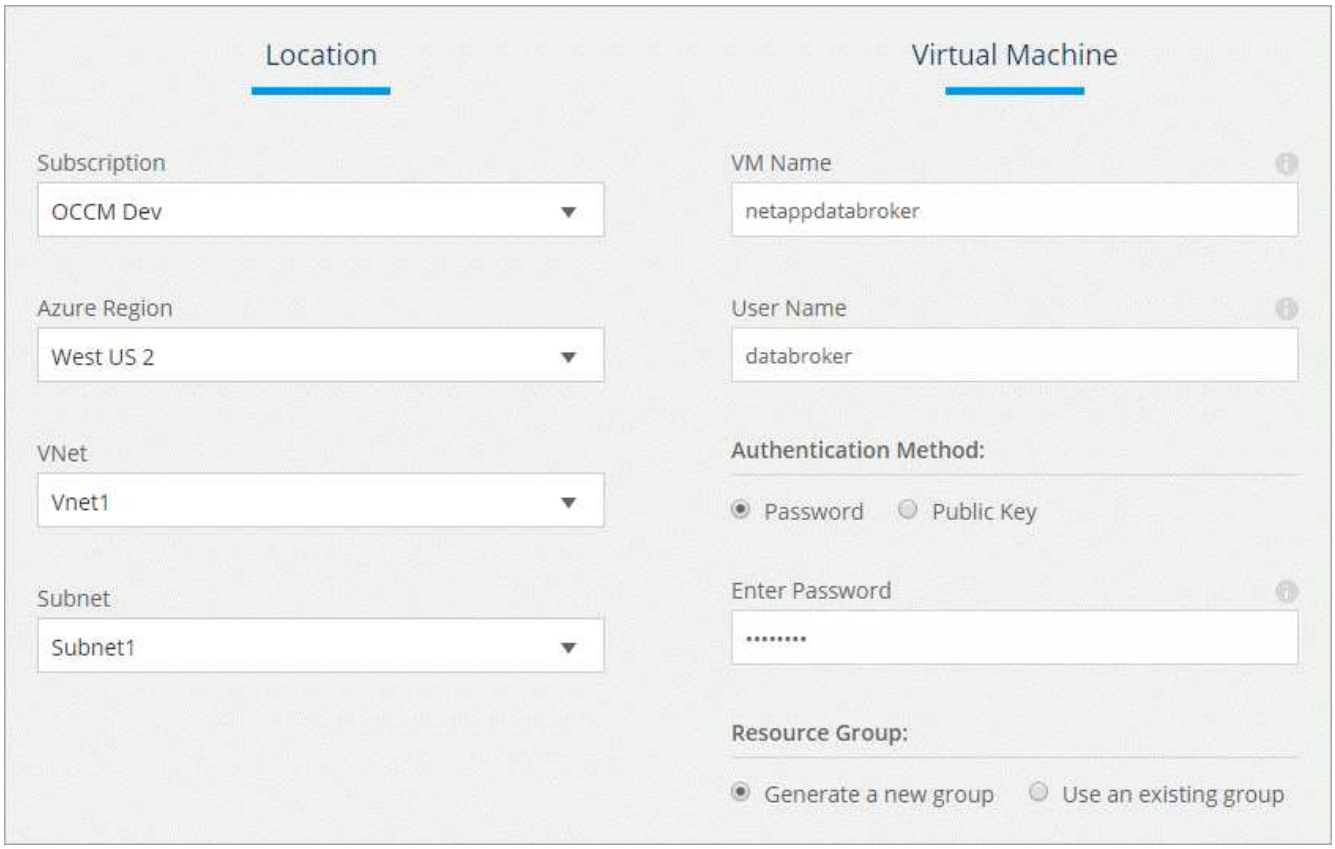
   Se você já tem um corretor de dados, você precisará clicar no ícone primeiro.



4. Digite um nome para o corretor de dados e clique em **continuar**.
5. Se lhe for solicitado, inicie sessão na sua conta Microsoft. Se você não for solicitado, clique em **entrar no Azure**.

   O formulário é de propriedade e hospedado pela Microsoft. Suas credenciais não são fornecidas ao NetApp.

6. Escolha um local para o corretor de dados e insira detalhes básicos sobre a máquina virtual.



7. Clique em **continuar** e mantenha a página aberta até que a implantação esteja concluída.

   O processo pode levar até 7 minutos.

8. No Cloud Sync, clique em **continuar** quando o corretor de dados estiver disponível.
9. Complete as páginas no assistente para criar a nova relação de sincronização.

Resultado

Você implantou um agente de dados no Azure e criou uma nova relação de sincronização. Você pode usar esse corretor de dados com relações de sincronização adicionais.

Recebendo uma mensagem sobre a necessidade de consentimento do administrador?

Se a Microsoft notificar você de que a aprovação de administrador é necessária porque o Cloud Sync precisa de permissão para acessar recursos em sua organização em seu nome, então você tem duas opções:

1. Peça ao administrador do AD para fornecer a você a seguinte permissão:

   No Azure, aceda a **Centros de administração > Azure AD > utilizadores e grupos > Definições de utilizador** e ative **os utilizadores podem autorizar as aplicações a acederem aos dados da empresa em seu nome**.

2. Peça ao administrador do AD para consentir em seu nome para **CloudSync-AzureDataBrokerCreator** usando o seguinte URL (este é o endpoint de consentimento do administrador):

   https://login.microsoftonline.com/{FILL HERE YOUR TENANT ID/v2,0/adminconsent?client_id_8e4ca3a-bafa-4831-97cc-5a38923cab85&redirect_uri_https://cloudsync.NetApp.com&scope-https://management.azure.com/user_impersonationhttps://graph.microsoft.com/User.Read

   Como mostrado na URL, o URL do nosso aplicativo é https://cloudsync.NetApp.com e o ID do cliente do aplicativo é 8ee4ca3a-bafa-4831-97cc-5a38923cab85.

Instalar o agente de dados no Google Cloud Platform

Quando você cria um relacionamento de sincronização, escolha a opção Data Broker do GCP para implantar o software de agente de dados em uma nova instância de máquina virtual em uma VPC. O Cloud Sync orienta você pelo processo de instalação, mas os requisitos e etapas são repetidos nesta página para ajudá-lo a se preparar para a instalação.

Você também tem a opção de instalar o agente de dados em um host Linux existente na nuvem ou no local. "Saiba mais".

Regiões GCP compatíveis

Todas as regiões são suportadas.

Requisitos de rede

- O corretor de dados precisa de uma conexão de saída de Internet para que possa pesquisar o serviço Cloud Sync para tarefas na porta 443.

  Quando o Cloud Sync implanta o agente de dados no GCP, ele cria um grupo de segurança que ativa a comunicação de saída necessária.

  Se precisar limitar a conetividade de saída, "a lista de endpoints que o corretor de dados entra em contato"consulte .

- A NetApp recomenda configurar o agente de origem, destino e dados para usar um serviço de protocolo de tempo de rede (NTP). A diferença de tempo entre os três componentes não deve exceder 5 minutos.

Permissões necessárias para implantar o agente de dados na GCP

Certifique-se de que o usuário do GCP que implanta o agente de dados tenha as seguintes permissões:

```
- compute.networks.list
- compute.regions.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.operations.get
- iam.serviceAccounts.list
```

Permissões necessárias para a conta de serviço

Ao implantar o agente de dados, você precisa selecionar uma conta de serviço que tenha as seguintes permissões:

```
- logging.logEntries.create
- resourcemanager.projects.get
- storage.buckets.get
- storage.buckets.list
- storage.objects.*
```

Instalar o agente de dados

É possível instalar um agente de dados no GCP ao criar um relacionamento de sincronização.

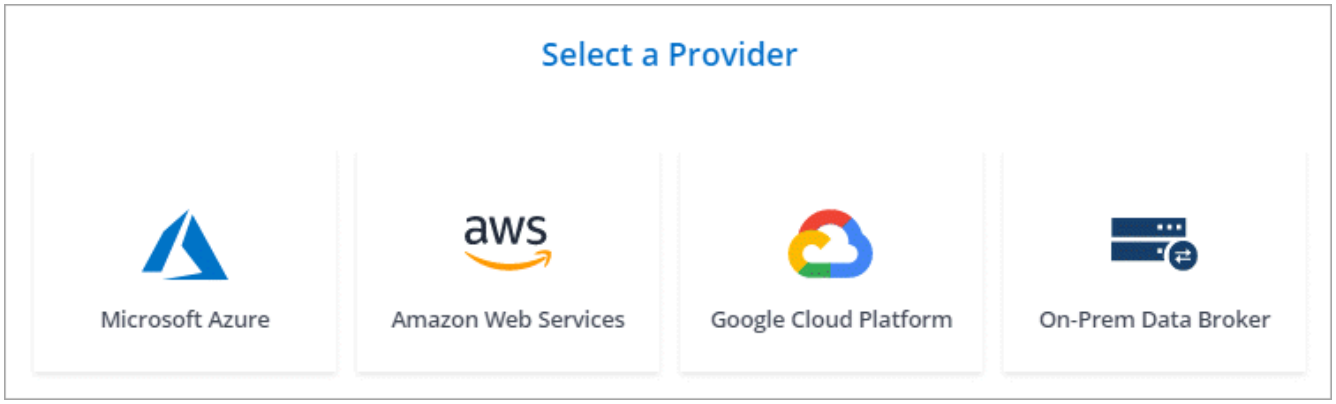
Passos

1. Clique em **criar nova sincronização**.
2. Na página **Definir relação de sincronização**, escolha uma fonte e destino e clique em **continuar**.

   Conclua as etapas até chegar à página **Data Broker**.

3. Na página **Data Broker**, clique em **Create Data Broker** e selecione **Google Cloud Platform**.

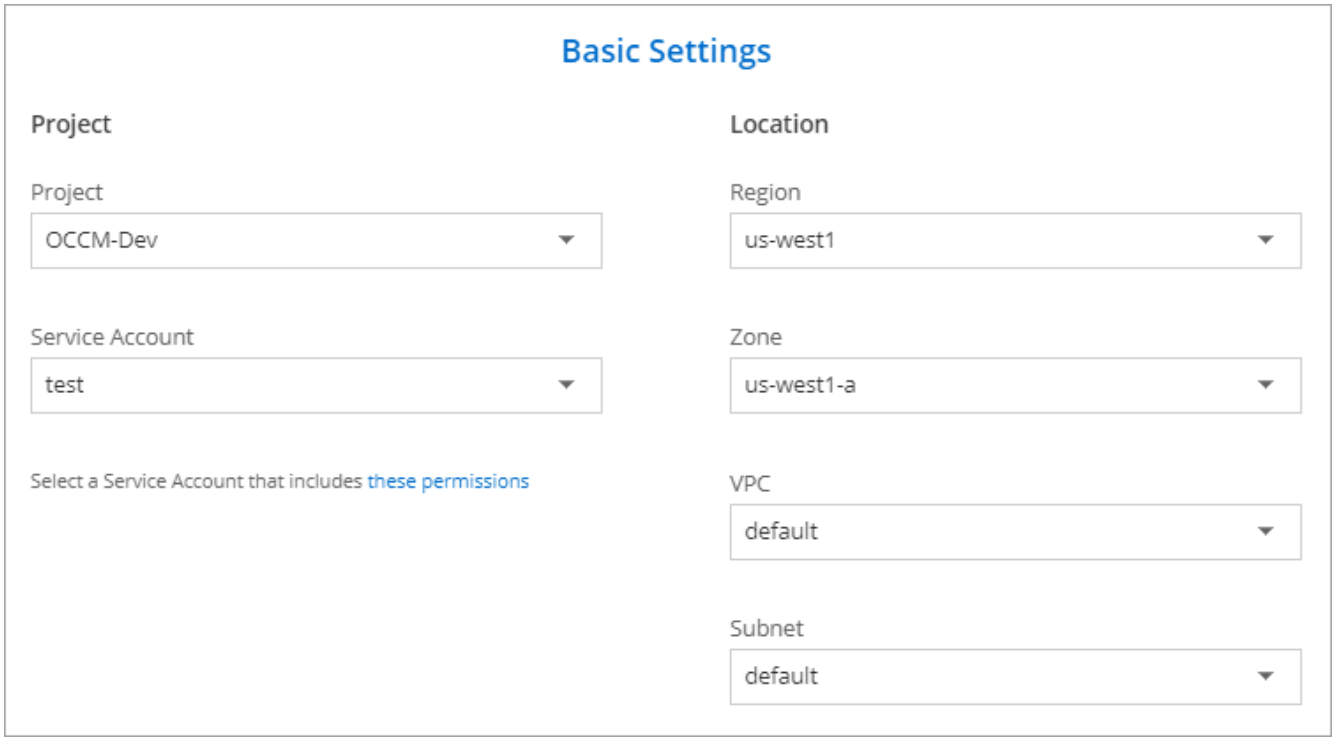
   Se você já tem um corretor de dados, você precisará clicar no  ícone primeiro.



4. Digite um nome para o corretor de dados e clique em **continuar**.
5. Se você for solicitado, faça login com sua conta do Google.

   O formulário é de propriedade e hospedado pelo Google. Suas credenciais não são fornecidas ao NetApp.

6. Selecione uma conta de projeto e serviço e escolha um local para o corretor de dados.



7. Quando o corretor de dados estiver disponível, clique em **continuar** no Cloud Sync.

   A instância leva aproximadamente 5 a 10 minutos para implantar. Você pode monitorar o andamento do serviço Cloud Sync, que é atualizado automaticamente quando a instância está disponível.

8. Complete as páginas no assistente para criar a nova relação de sincronização.

Resultado

Você implantou um agente de dados no GCP e criou uma nova relação de sincronização. Você pode usar esse corretor de dados com relações de sincronização adicionais.

Instalar o corretor de dados em um host Linux

Quando você cria uma relação de sincronização, escolha a opção Data Broker local para instalar o software Data Broker em um host Linux local ou em um host Linux existente na nuvem. O Cloud Sync orienta você pelo processo de instalação, mas os requisitos e etapas são repetidos nesta página para ajudá-lo a se preparar para a instalação.

Requisitos de host do Linux

- **Sistema operacional**:
  - CentOS 7,0, 7,7 e 8,0
  - Red Hat Enterprise Linux 7,7 e 8,0
  - Ubuntu Server 18,04 LTS
  - SUSE Linux Enterprise Server 15 SP1

    O comando `yum update all` deve ser executado no host antes de instalar o corretor de dados.

  Um sistema Red Hat Enterprise Linux deve ser registrado no Red Hat Subscription Management. Se não estiver registado, o sistema não poderá aceder aos repositórios para atualizar o software de 3rd partes necessário durante a instalação.
- **RAM**: 16 GB
- * CPU*: 4 núcleos
- * Espaço livre em disco *: 10 GB
- **SELinux**: Recomendamos que você desative "SELinux" no host.

  O SELinux aplica uma política que bloqueia atualizações de software de corretor de dados e pode impedir que o corretor de dados entre em Contato com os endpoints necessários para a operação normal.
- * OpenSSL*: OpenSSL deve ser instalado no host Linux.

Requisitos de rede

- O host Linux deve ter uma conexão com a origem e o destino.
- O servidor de arquivos deve permitir que o host Linux acesse as exportações.
- A porta 443 deve estar aberta no host Linux para tráfego de saída para a AWS (o agente de dados se comunica constantemente com o serviço Amazon SQS).
- A NetApp recomenda configurar o agente de origem, destino e dados para usar um serviço de protocolo de tempo de rede (NTP). A diferença de tempo entre os três componentes não deve exceder 5 minutos.

Habilitando o acesso à AWS

Se você planeja usar o agente de dados com um relacionamento de sincronização que inclui um bucket do S3, então você deve preparar o host Linux para o AWS Access. Ao instalar o agente de dados, você precisará fornecer chaves da AWS para um usuário da AWS que tenha acesso programático e permissões específicas.

Passos

1. Crie uma política do IAM usando "Esta política fornecida pela NetApp"o . "Veja as instruções da AWS".

2. Crie um usuário do IAM que tenha acesso programático. "Veja as instruções da AWS".

   Certifique-se de copiar as chaves da AWS porque você precisa especificá-las ao instalar o software de data broker.

Habilitando o acesso ao Google Cloud

Se você planeja usar o agente de dados com uma relação de sincronização que inclua um bucket do Google Cloud Storage, prepare o host Linux para acesso ao GCP. Ao instalar o corretor de dados, você precisará fornecer uma chave para uma conta de serviço que tenha permissões específicas.

Passos

1. Crie uma conta de serviço do GCP que tenha permissões de Administrador de armazenamento, se você ainda não tiver uma.
2. Crie uma chave de conta de serviço salva no formato JSON. "Veja as instruções da GCP".

   O arquivo deve conter pelo menos as seguintes propriedades: "Project_id", "private_key" e "client_email"

   Quando você cria uma chave, o arquivo é gerado e baixado para sua máquina.

3. Salve o arquivo JSON no host Linux.

Habilitando o acesso ao Microsoft Azure

O acesso ao Azure é definido por relacionamento fornecendo uma conta de armazenamento e uma cadeia de conexão no assistente de relacionamento de sincronização.

Instalar o agente de dados

Você pode instalar um corretor de dados em um host Linux quando você cria uma relação de sincronização.

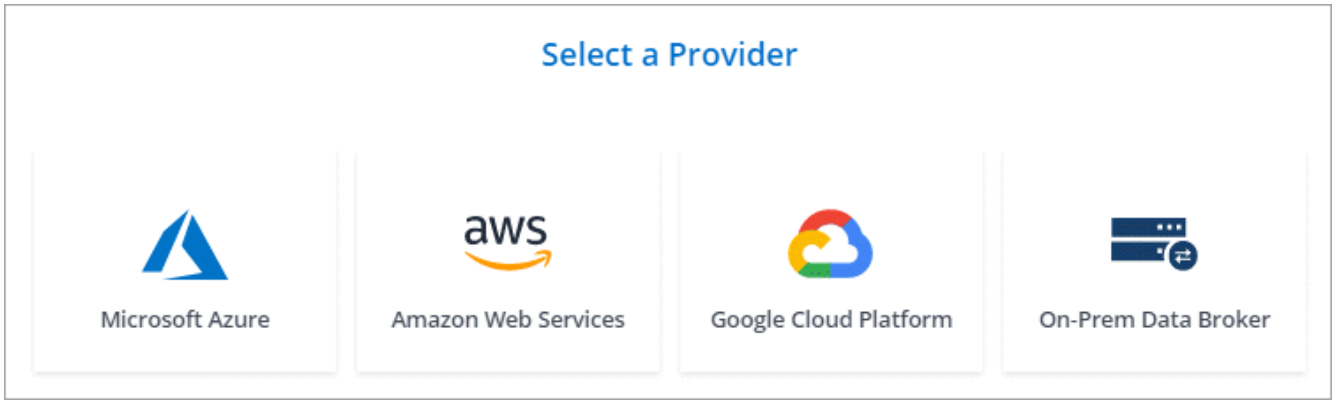
Passos

1. Clique em **criar nova sincronização**.
2. Na página **Definir relação de sincronização**, escolha uma fonte e destino e clique em **continuar**.

   Conclua as etapas até chegar à página **Data Broker**.

3. Na página **Data Broker**, clique em **Create Data Broker** e selecione **On-Prem Data Broker**.

   Se você já tem um corretor de dados, você precisará clicar no ícone primeiro.



Mesmo que a opção seja rotulada ***on-Prem* Data Broker**, ela se aplica a um host Linux em suas instalações ou na nuvem.

4. Digite um nome para o corretor de dados e clique em **continuar**.

   A página de instruções é carregada em breve. Você precisará seguir estas instruções - elas incluem um link exclusivo para baixar o instalador.

5. Na página de instruções:
   a. Selecione se deseja habilitar o acesso a **AWS**, **Google Cloud** ou ambos.
   b. Selecione uma opção de instalação: **No proxy**, **Use proxy Server** ou **Use proxy Server with Authentication**.
   c. Use os comandos para baixar e instalar o corretor de dados.

      As etapas a seguir fornecem detalhes sobre cada opção de instalação possível. Siga a página de instruções para obter o comando exato com base na opção de instalação.

   d. Faça o download do instalador:
      - Sem proxy:

        ```
        curl <URI> -o data_broker_installer.sh
        ```

      - Use o servidor proxy:

        ```
        curl <URI> -o data_broker_installer.sh -x <proxy_host>:<proxy_port>
        ```

      - Use o servidor proxy com autenticação:

        ```
        curl <URI> -o data_broker_installer.sh -x
        <proxy_username>:<proxy_password>@<proxy_host>:<proxy_port>
        ```

        URI

        O Cloud Sync exibe o URI do arquivo de instalação na página de instruções, que é carregado quando você segue os prompts para implantar o Data Broker local. Esse URI não é repetido aqui porque o link é gerado dinamicamente e pode ser usado apenas uma vez. Siga estes passos para obter o URI do Cloud Sync.

   e. Mude para superusuário, torne o instalador executável e instale o software:

Cada comando listado abaixo inclui parâmetros para o AWS Access e o GCP Access. Siga a página de instruções para obter o comando exato com base na opção de instalação.

- Sem configuração de proxy:

```
sudo -s
chmod +x data_broker_installer.sh
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
<absolute_path_to_the_json_file>
```

- Configuração do proxy:

```
sudo -s
chmod +x data_broker_installer.sh
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
<absolute_path_to_the_json_file> -h <proxy_host> -p <proxy_port>
```

- Configuração de proxy com autenticação:

```
sudo -s
chmod +x data_broker_installer.sh
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
<absolute_path_to_the_json_file> -h <proxy_host> -p <proxy_port> -u
<proxy_username> -w <proxy_password>
```

Chaves da AWS

Estas são as chaves para o usuário que você deve ter preparado seguindo estes passos. As chaves da AWS são armazenadas no agente de dados, que é executado em sua rede local ou na nuvem. O NetApp não usa as chaves fora do corretor de dados.

Ficheiro JSON

Este é o arquivo JSON que contém uma chave de conta de serviço que você deve ter preparado seguindo estes passos.

6. Quando o corretor de dados estiver disponível, clique em **continuar** no Cloud Sync.
7. Complete as páginas no assistente para criar a nova relação de sincronização.

Criando uma relação de sincronização

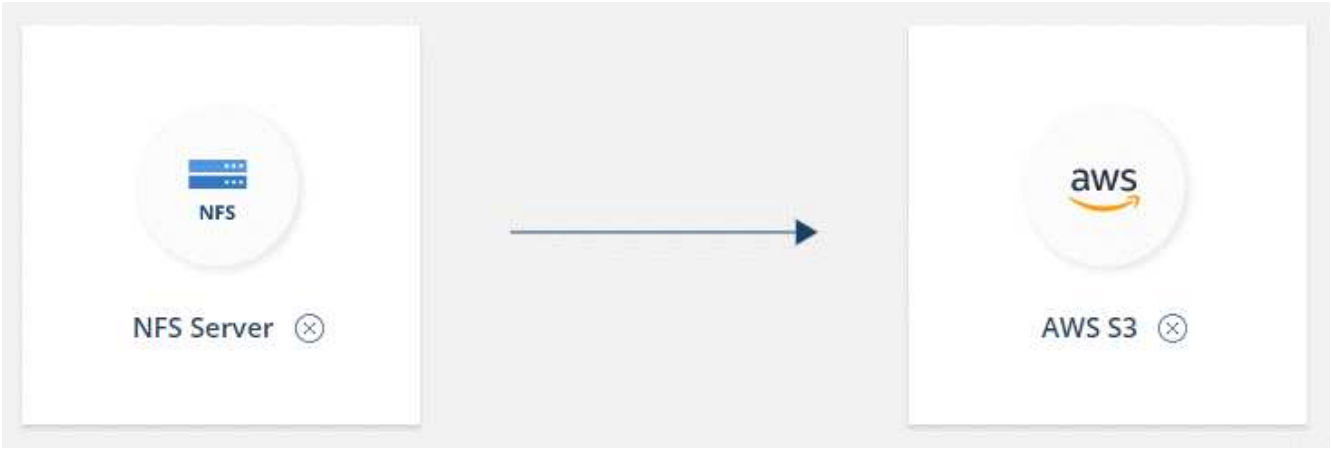
Quando você cria uma relação de sincronização, o serviço Cloud Sync copia arquivos da origem para o destino. Após a cópia inicial, o serviço sincroniza todos os dados alterados a cada 24 horas.

As etapas abaixo fornecem um exemplo que mostra como configurar uma relação de sincronização de um servidor NFS para um bucket do S3.

Passos

1. No Cloud Manager, clique em **Sync**.
2. Na página **Definir relação de sincronização**, escolha uma fonte e destino.

As etapas a seguir fornecem um exemplo de como criar uma relação de sincronização de um servidor NFS para um bucket do S3.

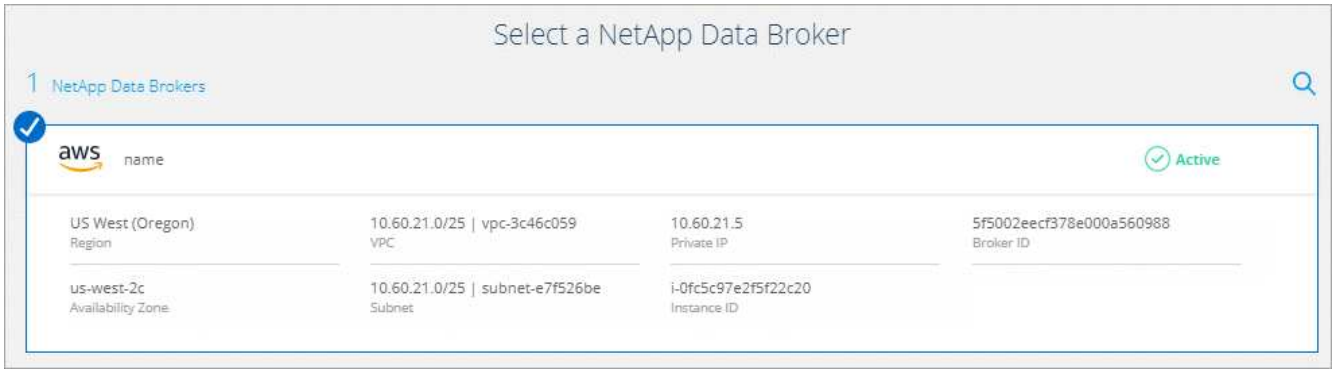


3. Na página **servidor NFS**, insira o endereço IP ou o nome de domínio totalmente qualificado do servidor NFS que você deseja sincronizar com a AWS.
4. Na página **Data Broker**, siga as instruções para criar uma máquina virtual de agente de dados na AWS, Azure ou Google Cloud Platform, ou para instalar o software de corretor de dados em um host Linux existente.

   Para obter mais detalhes, consulte as seguintes páginas:

   - "Instalar o agente de dados na AWS"
   - "Instalar o corretor de dados no Azure"
   - "Instalar o agente de dados no GCP"
   - "Instalar o corretor de dados em um host Linux"
5. Depois de instalar o corretor de dados, clique em **continuar**.

   A imagem a seguir mostra um corretor de dados implantado com sucesso na AWS:

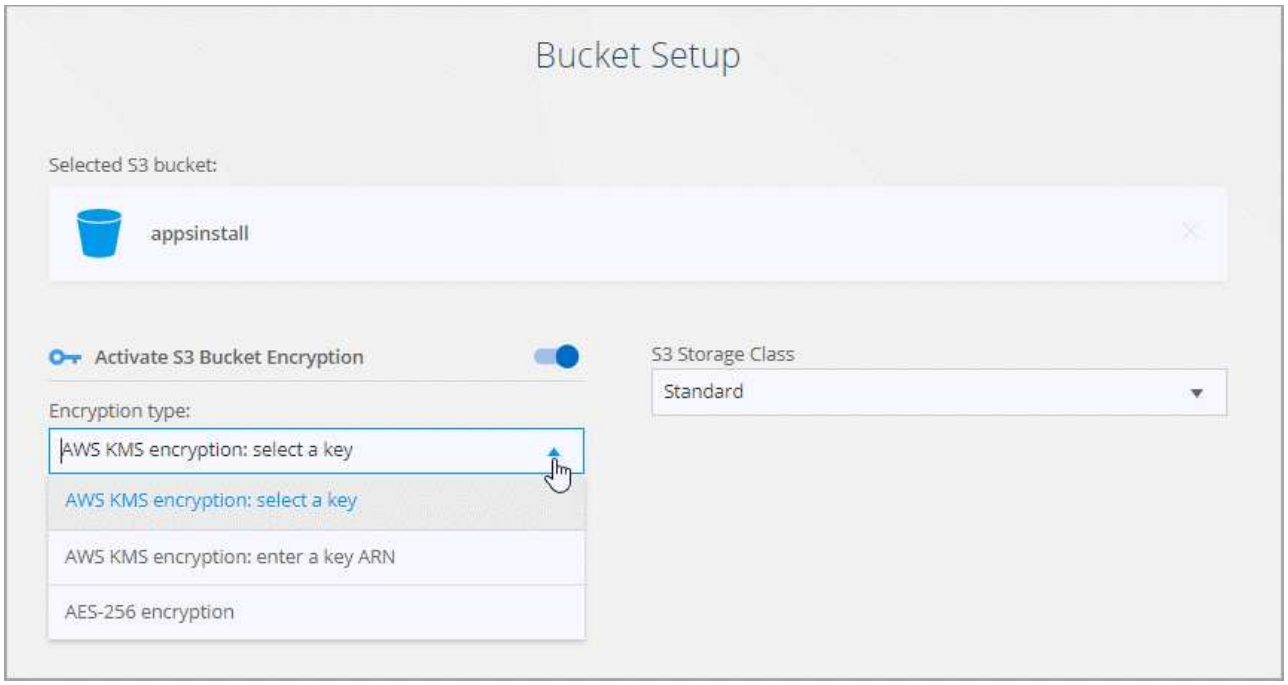


6. na página **diretórios**, selecione um diretório ou subdiretório de nível superior.

Se o Cloud Sync não conseguir recuperar as exportações, clique em **Adicionar exportação manualmente** e insira o nome de uma exportação NFS.

Se você quiser sincronizar mais de um diretório no servidor NFS, então você deve criar relações de sincronização adicionais depois que terminar.

7. Na página **AWS S3 Bucket**, selecione um bucket:
   - Faça uma pesquisa detalhada para selecionar uma pasta existente dentro do intervalo ou para selecionar uma nova pasta criada dentro do intervalo.
   - Clique em **Adicionar à lista** para selecionar um bucket do S3 que não esteja associado à sua conta da AWS. "Permissões específicas devem ser aplicadas ao bucket do S3".
8. Na página **Bucket Setup**, configure o bucket:
   - Escolha se deseja ativar a criptografia de bucket S3 e, em seguida, selecione uma chave AWS KMS, insira o ARN de uma chave KMS ou selecione criptografia AES-256.
   - Selecione uma classe de armazenamento S3. "Veja as classes de armazenamento suportadas".



9. Na página **Configurações**, defina como os arquivos de origem e as pastas são sincronizados e mantidos no local de destino:

Programação

Escolha uma programação recorrente para futuras sincronizações ou desative a programação de sincronização. Você pode agendar uma relação para sincronizar dados a cada 1 minutos.

Tenta novamente

Defina o número de vezes que o Cloud Sync deve tentar sincronizar um arquivo antes de ignorá-lo.

Ficheiros modificados recentemente

Escolha excluir arquivos que foram modificados recentemente antes da sincronização programada.

Eliminar ficheiros na origem

Escolha excluir arquivos do local de origem depois que o Cloud Sync copiar os arquivos para o local de destino. Essa opção inclui o risco de perda de dados porque os arquivos de origem são excluídos após serem copiados.

Se você ativar essa opção, também precisará alterar um parâmetro no arquivo local.json no corretor de dados. Abra o arquivo e altere o parâmetro chamado *workers.transferrer.delete-on-source* para **true**.

Excluir arquivos no destino

Escolha excluir arquivos do local de destino, se eles foram excluídos da origem. O padrão é nunca excluir arquivos do local de destino.

Marcação de objetos

Quando o AWS S3 é o destino em uma relação de sincronização, o Cloud Sync marca objetos S3 com metadados relevantes para a operação de sincronização. Você pode desativar a marcação de objetos S3, se não for desejado em seu ambiente. Não há impactos no Cloud Sync se você desabilitar a marcação: O Cloud Sync apenas armazena os metadados de sincronização de uma maneira diferente.

Tipos de ficheiros

Defina os tipos de arquivo a serem incluídos em cada sincronização: Arquivos, diretórios e links simbólicos.

Excluir extensões de arquivos

Especifique extensões de arquivo para excluir da sincronização digitando a extensão do arquivo e pressionando **Enter**. Por exemplo, digite *log* ou *.log* para excluir arquivos *.log. Não é necessário um separador para várias extensões. O vídeo a seguir fornece uma breve demonstração:

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

Tamanho do ficheiro

Escolha sincronizar todos os arquivos, independentemente do seu tamanho ou apenas arquivos que estão em um intervalo de tamanho específico.

Data de modificação

Escolha todos os arquivos independentemente da data da última modificação, arquivos modificados após uma data específica, antes de uma data específica ou entre um intervalo de tempo.

10. Na página **Tags de relacionamento**, insira até 9 tags de relacionamento e clique em **continuar**.

    O serviço Cloud Sync atribui as tags a cada objeto que ele sincroniza com o bucket do S3.

11. Revise os detalhes da relação de sincronização e clique em **criar relacionamento**.

Resultado

O Cloud Sync inicia a sincronização de dados entre a origem e o destino.

Pagando por relacionamentos de sincronização após o término da avaliação gratuita

Há duas maneiras de pagar pelas relações de sincronização após o término da avaliação gratuita de 14 dias. A primeira opção é se inscrever na AWS ou no Azure para pagar conforme o uso ou pagar anualmente. A segunda opção é comprar licenças diretamente da NetApp.

Você pode usar licenças do NetApp com uma assinatura da AWS ou do Azure. Por exemplo, se você tiver 25 relacionamentos de sincronização, poderá pagar pelas primeiras 20 relações de sincronização usando uma licença e pagar conforme o uso da AWS ou do Azure com as 5 relações de sincronização restantes.

"Saiba mais sobre como as licenças funcionam".

E se eu não pagar imediatamente após o fim da minha avaliação gratuita? 8217

Você não será capaz de criar relacionamentos adicionais. Relacionamentos existentes não são excluídos, mas você não pode fazer alterações a eles até que você assine ou insira uma licença.

assinatura da AWS

A AWS permite que você pague conforme o uso ou pague anualmente.

Passos para pagar conforme o uso

1. Clique em **Sync > Licensing**.
2. Selecione **AWS**
3. Clique em **Subscribe** e, em seguida, clique em **Continue**.
4. Inscreva-se no AWS Marketplace e faça login novamente no serviço Cloud Sync para concluir o Registro.

   O vídeo a seguir mostra o processo:

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

Passos para pagar anualmente

1. "Vá para a página do AWS Marketplace".
2. Clique em **continuar para assinar**.
3. Selecione suas opções de contrato e clique em **criar contrato**.

subscrição do Azure

O Azure permite que você pague conforme o uso ou pague anualmente.

O que você vai precisar

Uma conta de usuário do Azure que tenha permissões de Colaborador ou proprietário na assinatura relevante.

Passos

1. Clique em **Sync > Licensing**.
2. Selecione **Azure**.
3. Clique em **Subscribe** e, em seguida, clique em **Continue**.
4. No portal do Azure, clique em **criar**, selecione suas opções e clique em **Inscrever-se**.

   Selecione **mensal** para pagar por hora, ou **anual** para pagar por um ano antes.

5. Quando a implementação estiver concluída, clique no nome do recurso SaaS no pop-up de notificação.
6. Clique em **Configurar conta** para retornar ao Cloud Sync.

   O vídeo a seguir mostra o processo:

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

comprando licenças da NetApp e adicionando-as ao Cloud Sync

Para pagar antecipadamente pelas relações de sincronização, você deve comprar uma ou mais licenças e adicioná-las ao serviço Cloud Sync.

Passos

1. Compre uma licença por mailto:ng-cloudsync-Contact at NetApp.com?subject:Cloud%20Sync%20Service%20-%20BYOL%20License%20Purchase%20Request[contactar o NetApp].
2. No Cloud Manager, clique em **Sync > Licensing**.
3. Clique em **Adicionar licença** e adicione a licença.

Tutoriais

Cópia de ACLs entre compartilhamentos SMB

O Cloud Sync pode copiar listas de controle de acesso (ACLs) entre um compartilhamento SMB de origem e um compartilhamento SMB de destino. Se necessário, você pode preservar manualmente as ACLs usando robocopy.

Opções

- Configure o Cloud Sync para copiar ACLs automaticamente
- Copie manualmente as ACLs

Configurando o Cloud Sync para copiar ACLs entre servidores SMB

Copie ACLs entre servidores SMB habilitando uma configuração quando você cria um relacionamento ou depois de criar um relacionamento.

Observe que esse recurso está disponível para novas relações de sincronização criadas após a versão de 23 de fevereiro de 2020. Se você quiser usar esse recurso com relacionamentos existentes criados antes dessa data, precisará recriar o relacionamento.

O que você vai precisar

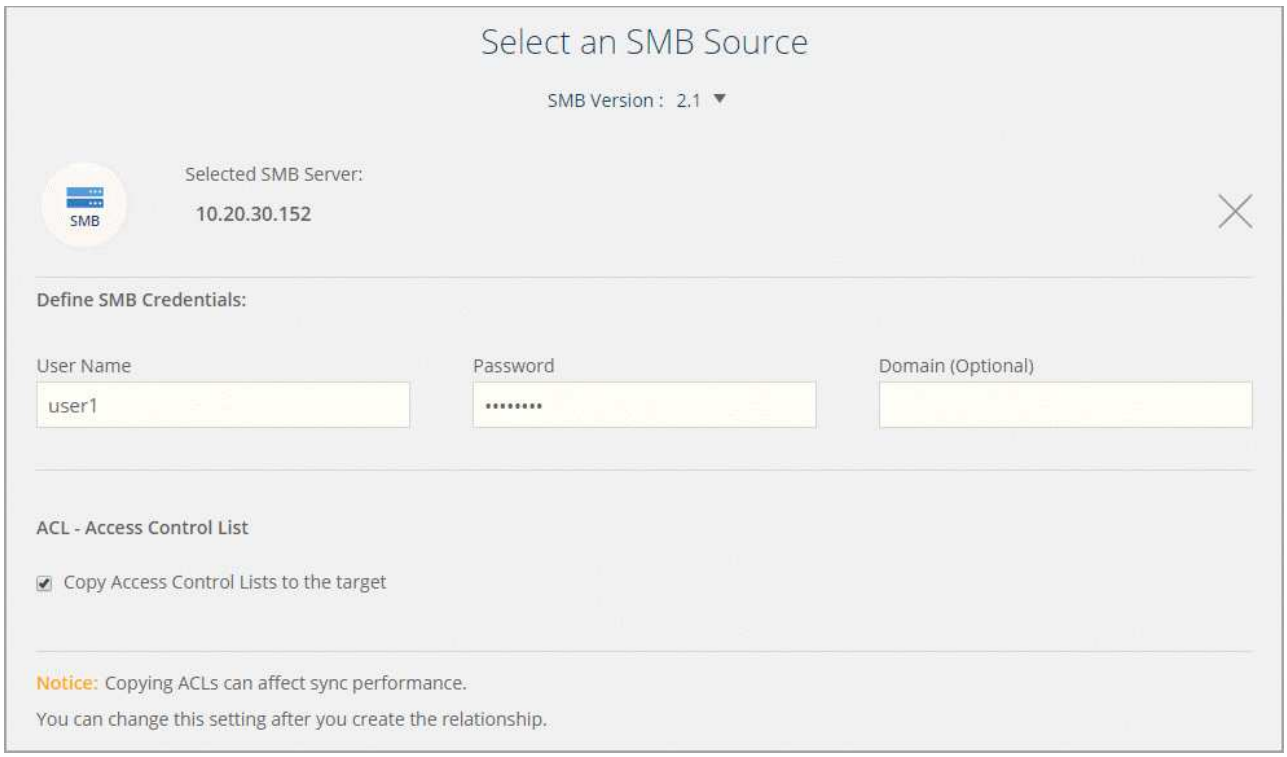
- Uma nova relação de sincronização ou uma relação de sincronização existente criada após a versão de 23 de fevereiro de 2020.
- Qualquer tipo de corretor de dados.

  Esse recurso funciona com *qualquer* tipo de agente de dados: AWS, Azure, Google Cloud Platform ou agente de dados local. O agente de dados local pode executar "qualquer sistema operacional suportado"o .

Passos para um novo relacionamento

1. No Cloud Sync, clique em **criar nova sincronização**.
2. Arraste e solte **servidor SMB** para a origem e destino e clique em **continuar**.
3. Na página **servidor SMB**:
   a. Introduza um novo servidor SMB ou selecione um servidor existente e clique em **continuar**.
   b. Insira credenciais para o servidor SMB.

c. Selecione **Copiar listas de controle de acesso para o destino** e clique em **continuar**.



4. Siga as instruções restantes para criar a relação de sincronização.

Etapas para um relacionamento existente

1. Passe o Mouse sobre a relação de sincronização e clique no menu de ação.
2. Clique em **Configurações**.
3. Selecione **Copiar listas de controle de acesso para o destino**.
4. Clique em **Salvar configurações**.

Resultado

Ao sincronizar dados, o Cloud Sync preserva as ACLs entre os compartilhamentos SMB de origem e destino.

Copiar manualmente ACLs

Você pode preservar manualmente ACLs entre compartilhamentos SMB usando o comando Windows robocopy.

Passos

1. Identifique um host do Windows que tenha acesso total a ambos os compartilhamentos SMB.
2. Se qualquer um dos endpoints exigir autenticação, use o comando **uso líquido** para se conetar aos endpoints a partir do host do Windows.

   Você deve executar esta etapa antes de usar o robocopy.

3. A partir do Cloud Sync, crie uma nova relação entre os compartilhamentos SMB de origem e destino ou sincronize um relacionamento existente.
4. Após a conclusão da sincronização de dados, execute o seguinte comando a partir do host do Windows para sincronizar as ACLs e a propriedade:

```
robocopy /E /COPY:SOU /secfix [source] [target] /w:0 /r:0 /XD ~snapshots
/UNILOG:"[logfilepath]
```

Tanto *source* quanto *target* devem ser especificados usando o formato UNC. Por exemplo: <server>/<share>/<path>

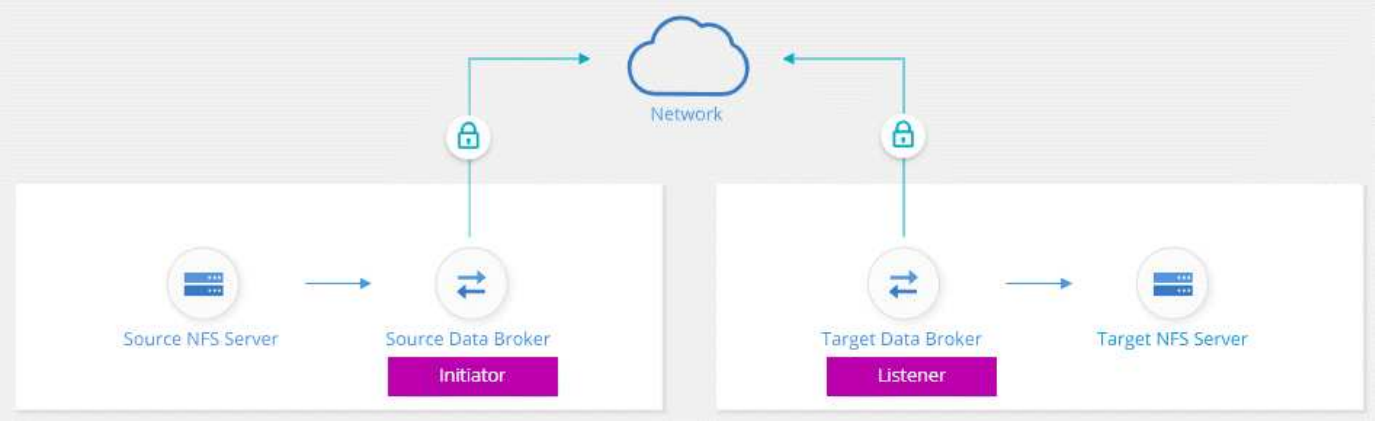
Sincronização de dados NFS com a criptografia de dados em trânsito

Se sua empresa tiver políticas de segurança rígidas, você poderá sincronizar dados NFS com a criptografia de dados em trânsito. Esse recurso é compatível de um servidor NFS para outro servidor NFS e de Azure NetApp Files para Azure NetApp Files.

Por exemplo, você pode querer sincronizar dados entre dois servidores NFS que estão em redes diferentes. Ou talvez seja necessário transferir dados com segurança no Azure NetApp Files entre sub-redes ou regiões.

Como funciona a criptografia de dados em trânsito

A criptografia de dados em trânsito criptografa os dados NFS quando eles são enviados pela rede entre dois corretores de dados. A imagem a seguir mostra uma relação entre dois servidores NFS e dois data brokers:



Um corretor de dados funciona como *iniciador*. Quando é hora de sincronizar dados, ele envia uma solicitação de conexão para o outro corretor de dados, que é o *listener*. Esse corretor de dados escuta solicitações na porta 443. Você pode usar uma porta diferente, se necessário, mas certifique-se de verificar se a porta não está em uso por outro serviço.

Por exemplo, se você sincronizar dados de um servidor NFS no local para um servidor NFS baseado na nuvem, poderá escolher qual agente de dados escuta as solicitações de conexão e quais as envia.

Veja como funciona a criptografia em trânsito:

1. Depois de criar a relação de sincronização, o iniciador inicia uma conexão criptografada com o outro corretor de dados.
2. O corretor de dados de origem criptografa os dados da fonte usando TLS 1,3.
3. Em seguida, ele envia os dados pela rede para o agente de dados de destino.
4. O corretor de dados de destino descriptografa os dados antes de enviá-los para o destino.
5. Após a cópia inicial, o serviço sincroniza todos os dados alterados a cada 24 horas. Se houver dados para sincronizar, o processo começa com o iniciador abrindo uma conexão criptografada com o outro corretor

de dados.

Se preferir sincronizar dados com mais frequência, "você pode alterar a programação depois de criar o relacionamento".

Versões de NFS compatíveis

- Para servidores NFS, a criptografia de dados em trânsito é compatível com NFS versões 3, 4,0, 4,1 e 4,2.
- Para Azure NetApp Files, a criptografia de dados em trânsito é compatível com NFS versões 3 e 4,1.

O que você precisará para começar

Certifique-se de que tem o seguinte:

- Dois servidores NFS que atendem "requisitos de origem e destino" ou Azure NetApp Files em duas sub-redes ou regiões.
- Os endereços IP ou nomes de domínio totalmente qualificados dos servidores.
- Locais de rede para dois corretores de dados.

  Você pode selecionar um corretor de dados existente, mas ele deve funcionar como o iniciador. O corretor de dados do ouvinte deve ser um *new* corretor de dados.

  Se você ainda não implantou um agente de dados, revise os requisitos do agente de dados. Como você tem políticas de segurança rígidas, certifique-se de rever os requisitos de rede, que incluem tráfego de saída da porta 443 e o "endpoints da internet" que o agente de dados contacta.

  - "Revise a instalação da AWS"
  - "Revise a instalação do Azure"
  - "Revise a instalação da GCP"
  - "Revise a instalação do host Linux"

Sincronização de dados NFS com a criptografia de dados em trânsito

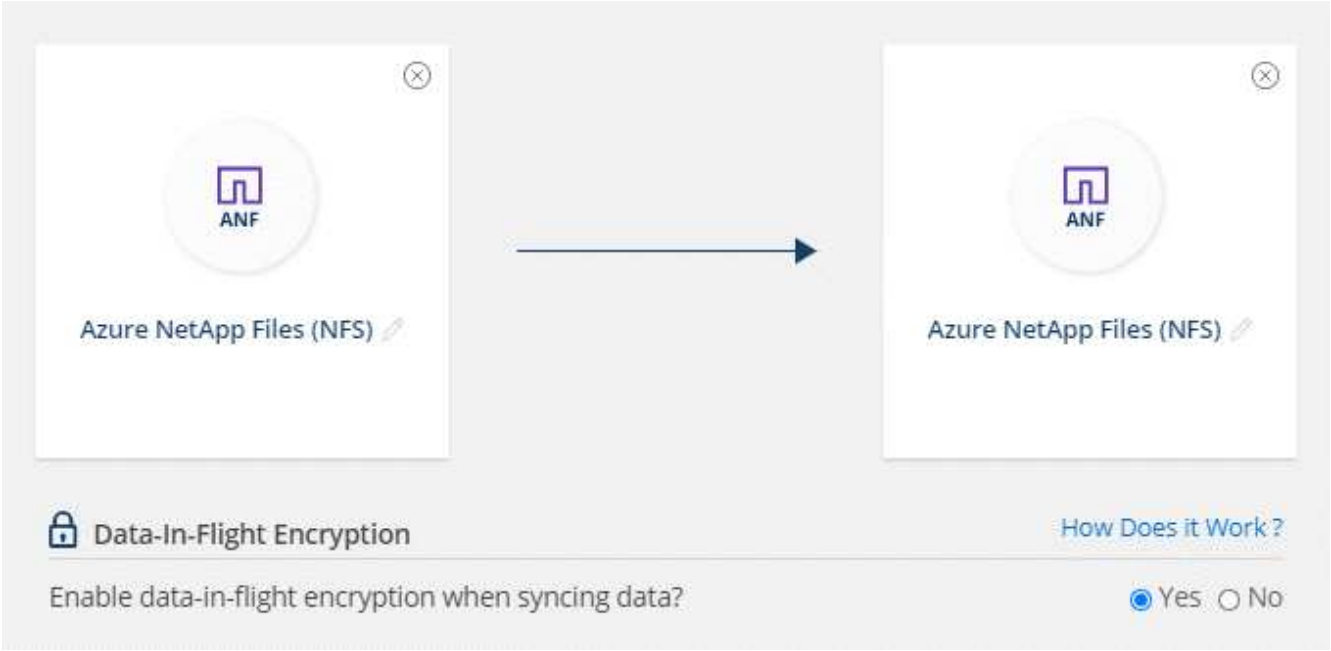
Crie uma nova relação de sincronização entre dois servidores NFS ou entre Azure NetApp Files, ative a opção de criptografia em trânsito e siga as instruções.

Passos

1. Clique em **criar nova sincronização**.
2. Arraste e solte **servidor NFS** para os locais de origem e destino ou **Azure NetApp Files** para os locais de origem e destino e selecione **Sim** para ativar a criptografia de dados em trânsito.

   A imagem a seguir mostra o que você selecionaria para sincronizar dados entre dois servidores NFS:

A imagem a seguir mostra o que você selecionaria para sincronizar dados entre o Azure NetApp Files:



3. Siga as instruções para criar a relação:

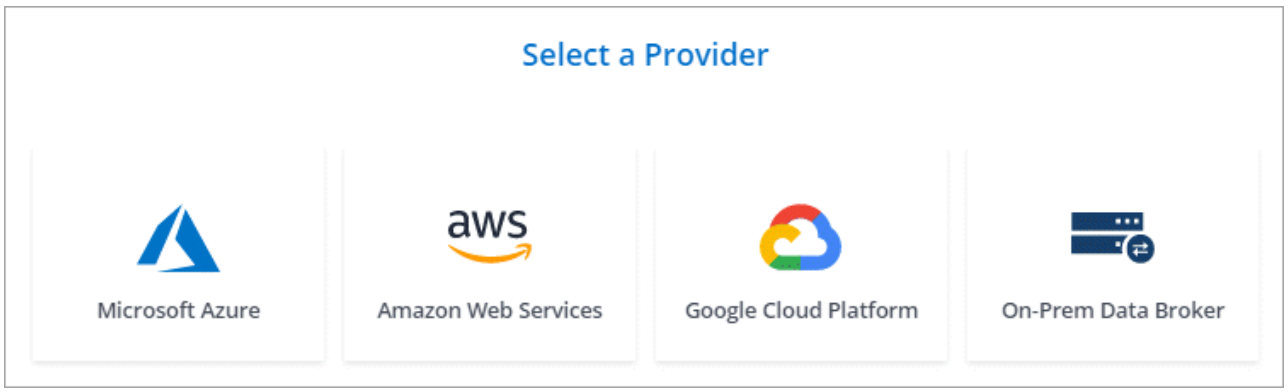
   a. **Servidor NFS/Azure NetApp Files**: Escolha a versão NFS e especifique uma nova fonte NFS ou selecione um servidor existente.

   b. **Definir funcionalidade do Data Broker**: Defina qual agente de dados *escuta* para solicitações de conexão em uma porta e qual *inicia* a conexão. Faça sua escolha com base em seus requisitos de rede.

   c. **Data Broker**: Siga as instruções para adicionar um novo corretor de dados de origem ou selecionar um corretor de dados existente.

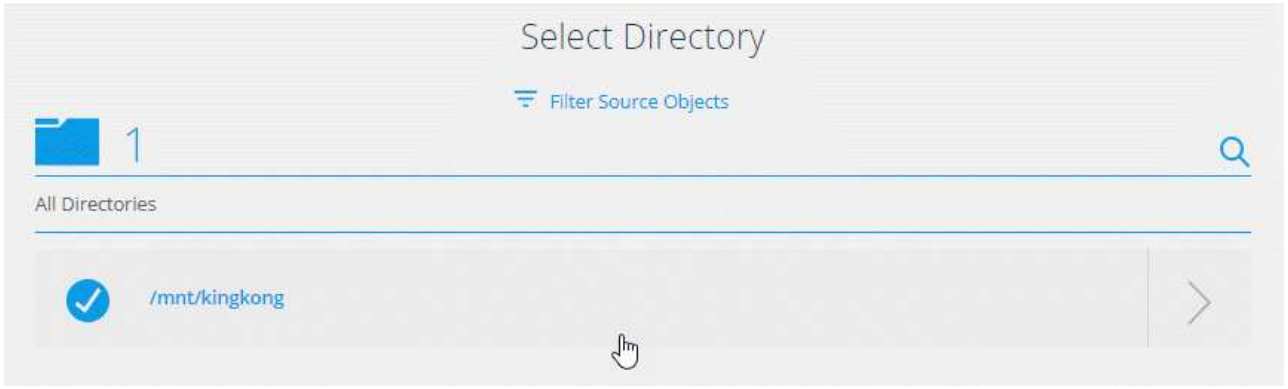
      Se o corretor de dados de origem age como o ouvinte, então ele deve ser um novo corretor de dados.

Se você precisar de um novo corretor de dados, o Cloud Sync solicitará as instruções de instalação. Você pode implantar o agente de dados na nuvem ou baixar um script de instalação para seu próprio host Linux.



d. **Diretórios**: Escolha os diretórios que você deseja sincronizar selecionando todos os diretórios, ou pesquisando e selecionando um subdiretório.

   Clique em **Filtrar objetos de origem** para modificar as configurações que definem como os arquivos de origem e as pastas são sincronizados e mantidos no local de destino.

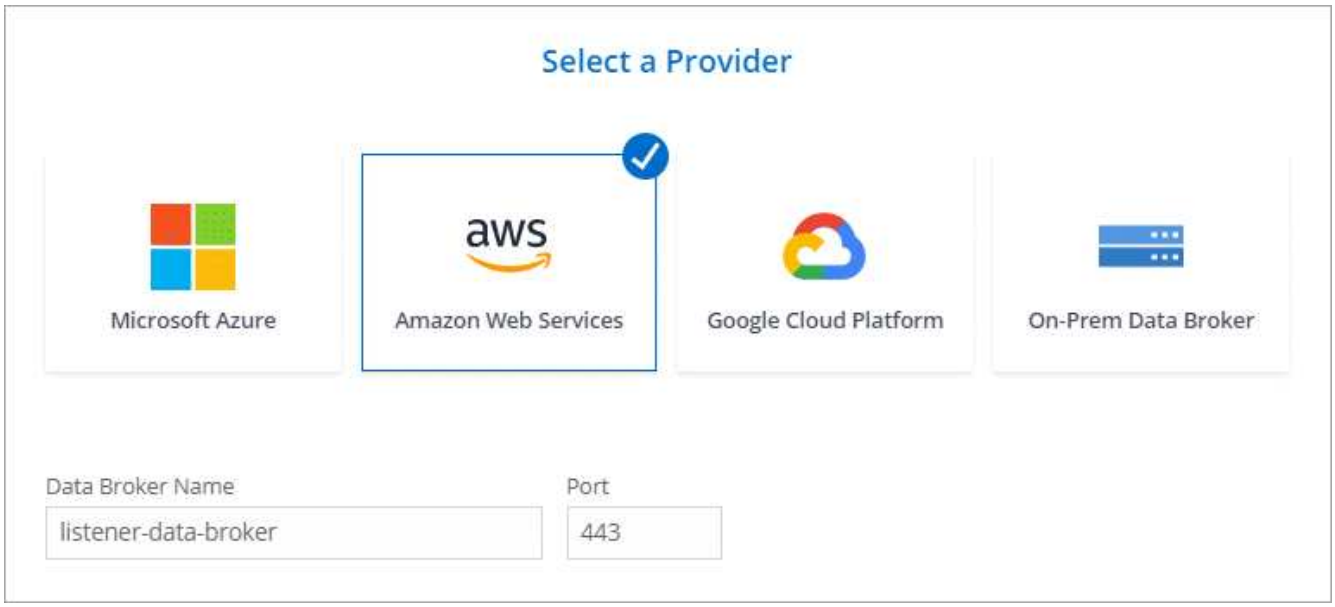


e. **Servidor NFS de destino/Azure NetApp Files de destino**: Escolha a versão NFS e insira um novo destino NFS ou selecione um servidor existente.

f. **Target Data Broker**: Siga as instruções para adicionar um novo corretor de dados de origem ou selecionar um corretor de dados existente.

   Se o corretor de dados de destino age como ouvinte, então ele deve ser um novo corretor de dados.

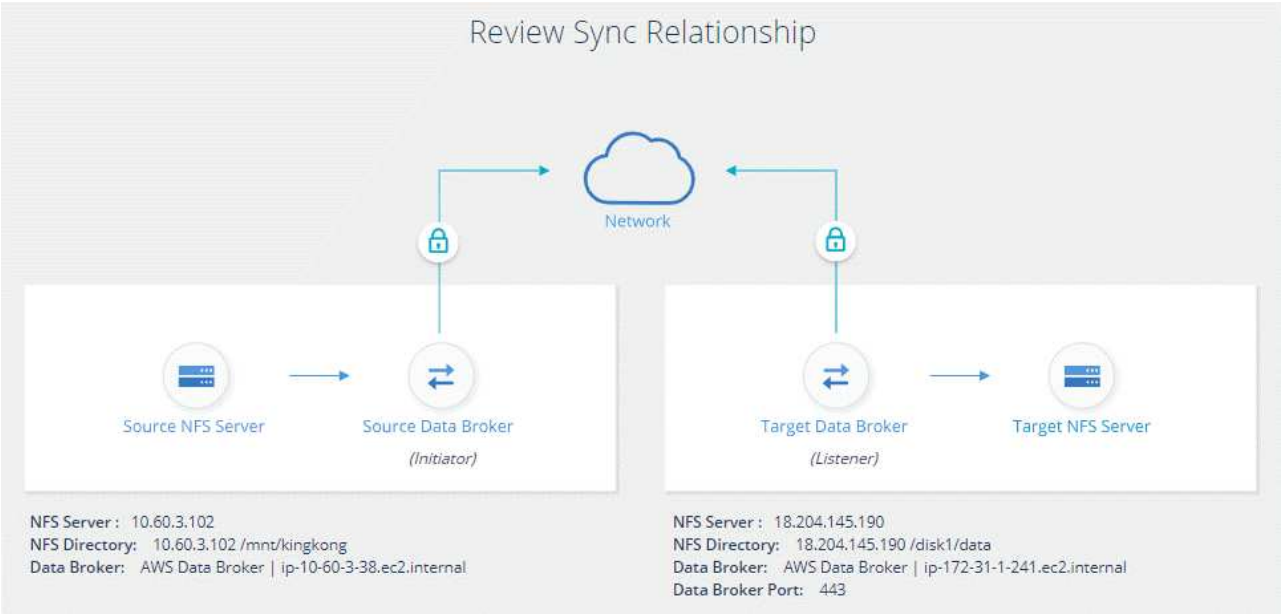
   Aqui está um exemplo do prompt quando o corretor de dados de destino funciona como ouvinte. Observe a opção de especificar a porta.



a. **Diretórios de destino**: Selecione um diretório de nível superior ou faça uma pesquisa para selecionar um subdiretório existente ou criar uma nova pasta dentro de uma exportação.

b. **Configurações**: Defina como os arquivos de origem e as pastas são sincronizados e mantidos no local de destino.

c. **Revisão**: Revise os detalhes da relação de sincronização e clique em **criar relacionamento**.



Resultado

O Cloud Sync começa a criar a nova relação de sincronização. Quando terminar, clique em **Exibir no Dashboard** para ver detalhes sobre o novo relacionamento.

Gerenciando relacionamentos de sincronização

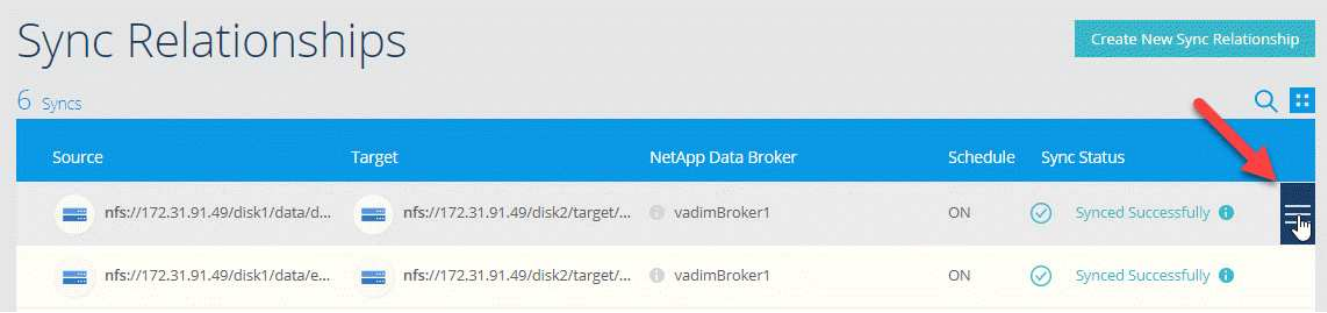
Você pode gerenciar relacionamentos de sincronização a qualquer momento sincronizando dados imediatamente, alterando horários e muito mais.

Realizar uma sincronização de dados imediata

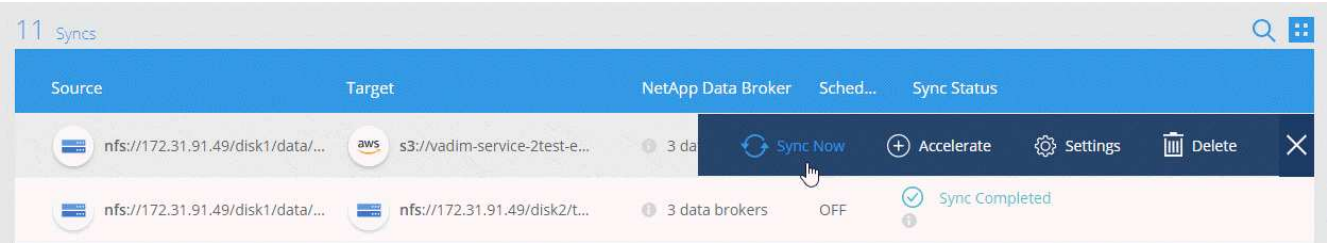
Em vez de esperar pela próxima sincronização agendada, você pode pressionar um botão para sincronizar imediatamente os dados entre a origem e o destino.

Passos

1. No **Painel de sincronização**, passe o Mouse sobre a relação de sincronização e clique no menu de ação.



2. Clique em **Sincronizar agora** e, em seguida, clique em **Sincronizar** para confirmar.



Resultado

O Cloud Sync inicia o processo de sincronização de dados para a relação.

Acelerando o desempenho de sincronização

Acelere o desempenho de uma relação de sincronização adicionando um agente de dados adicional ao relacionamento. O corretor de dados adicional deve ser um corretor de dados *new*.

Como isso funciona

Se os corretores de dados existentes no relacionamento forem usados em outras relações de sincronização, o Cloud Sync também adicionará automaticamente o novo corretor de dados a essas relações.

Por exemplo, digamos que você tenha três relacionamentos:

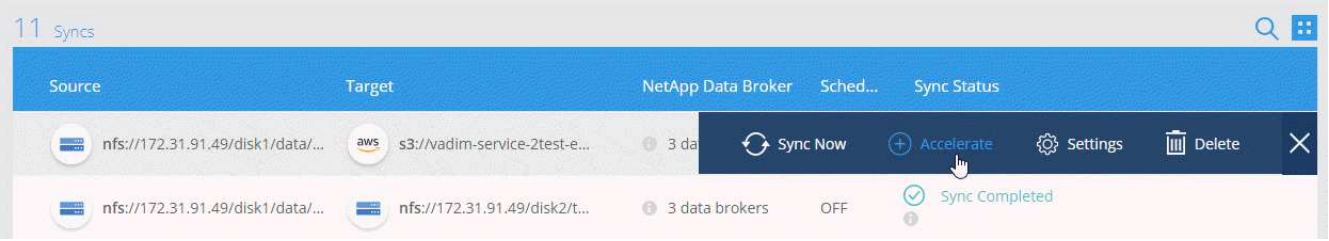
- O relacionamento 1 usa o agente de dados A.
- O relacionamento 2 usa o corretor de dados B
- O relacionamento 3 usa o agente de dados A.

Você quer acelerar o desempenho do relacionamento 1 para adicionar um novo agente de dados a esse relacionamento (agente de dados C). Como o corretor de dados A também é usado no relacionamento 3, o novo corretor de dados também é automaticamente adicionado ao relacionamento 3.

Passos

1. Certifique-se de que pelo menos um dos corretores de dados existentes no relacionamento esteja on-line.

2. Passe o Mouse sobre a relação de sincronização e clique no menu de ação.
3. Clique em **Accelerate**.



4. Siga as instruções para criar um novo corretor de dados.

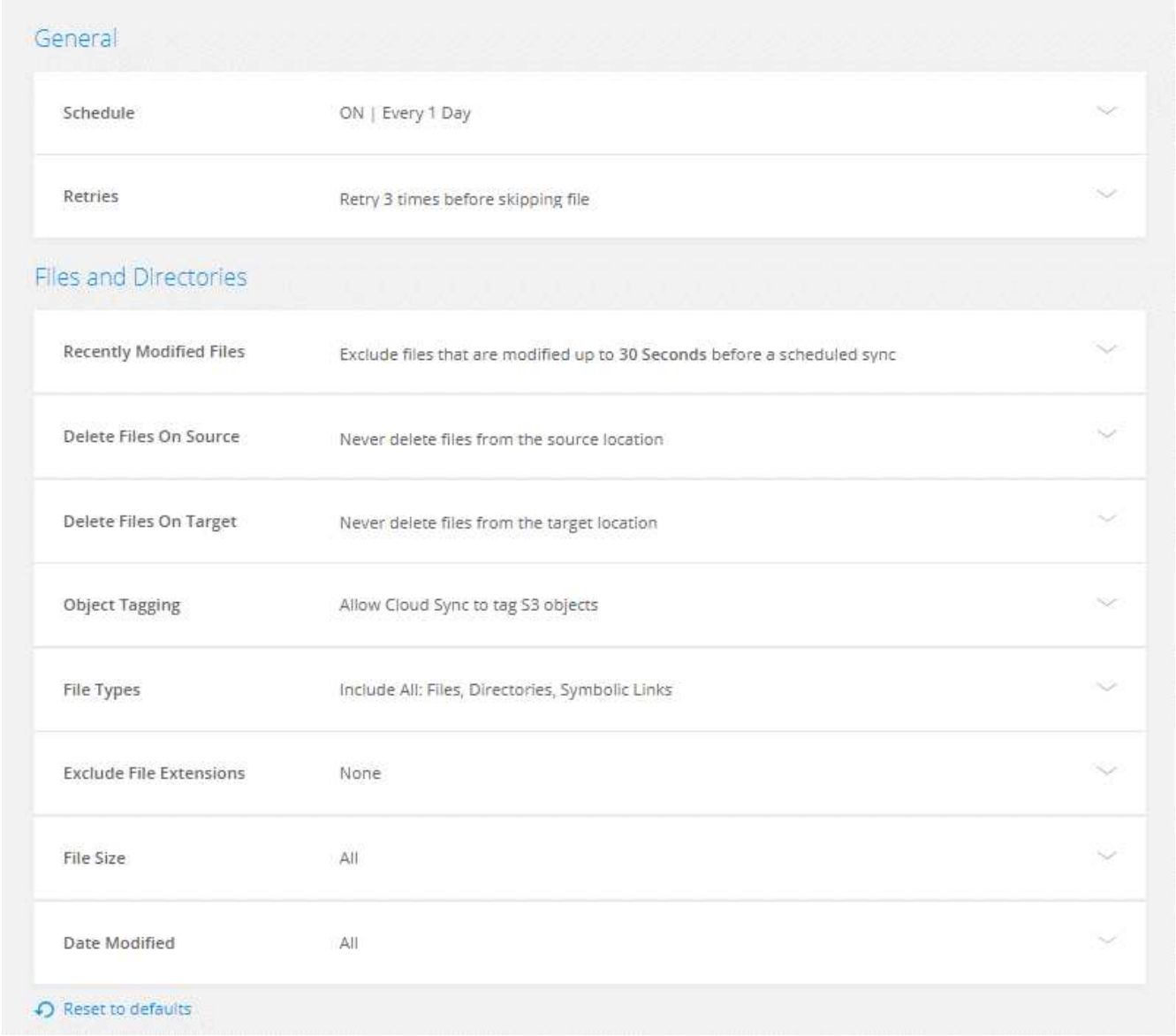
Resultado

O Cloud Sync adiciona o novo agente de dados às relações de sincronização. O desempenho da próxima sincronização de dados deve ser acelerado.

Alterar as definições de uma relação de sincronização

Modifique as configurações que definem como os arquivos de origem e as pastas são sincronizados e mantidos no local de destino.

1. Passe o Mouse sobre a relação de sincronização e clique no menu de ação.
2. Clique em **Configurações**.
3. Modifique qualquer uma das definições.



aqui está uma breve descrição de cada configuração:

Programação

Escolha uma programação recorrente para futuras sincronizações ou desative a programação de sincronização. Você pode agendar uma relação para sincronizar dados a cada 1 minutos.

Tenta novamente

Defina o número de vezes que o Cloud Sync deve tentar sincronizar um arquivo antes de ignorá-lo.

Ficheiros modificados recentemente

Escolha excluir arquivos que foram modificados recentemente antes da sincronização programada.

Eliminar ficheiros na origem

Escolha excluir arquivos do local de origem depois que o Cloud Sync copiar os arquivos para o local de destino. Essa opção inclui o risco de perda de dados porque os arquivos de origem são excluídos após serem copiados.

Se você ativar essa opção, também precisará alterar um parâmetro no arquivo local.json no corretor de dados. Abra o arquivo e altere o parâmetro chamado *workers.transferrer.delete-on-source* para **true**.

Excluir arquivos no destino

Escolha excluir arquivos do local de destino, se eles foram excluídos da origem. O padrão é nunca excluir arquivos do local de destino.

Marcação de objetos

Quando o AWS S3 é o destino em uma relação de sincronização, o Cloud Sync marca objetos S3 com metadados relevantes para a operação de sincronização. Você pode desativar a marcação de objetos S3, se não for desejado em seu ambiente. Não há impactos no Cloud Sync se você desabilitar a marcação: O Cloud Sync apenas armazena os metadados de sincronização de uma maneira diferente.

Tipos de ficheiros

Defina os tipos de arquivo a serem incluídos em cada sincronização: Arquivos, diretórios e links simbólicos.

Excluir extensões de arquivos

Especifique extensões de arquivo para excluir da sincronização digitando a extensão do arquivo e pressionando **Enter**. Por exemplo, digite *log* ou *.log* para excluir arquivos *.log. Não é necessário um separador para várias extensões. O vídeo a seguir fornece uma breve demonstração:

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

Tamanho do ficheiro

Escolha sincronizar todos os arquivos, independentemente do seu tamanho ou apenas arquivos que estão em um intervalo de tamanho específico.

Data de modificação

Escolha todos os arquivos independentemente da data da última modificação, arquivos modificados após uma data específica, antes de uma data específica ou entre um intervalo de tempo.

Copiar listas de controlo de acesso para o destino

Escolha copiar listas de controle de acesso (ACLs) entre compartilhamentos SMB de origem e compartilhamentos SMB de destino. Observe que essa opção só está disponível para relacionamentos de sincronização criados após a versão de 23 de fevereiro de 2020.

4. Clique em **Salvar configurações**.

Resultado

O Cloud Sync modifica a relação de sincronização com as novas configurações.

Excluindo relacionamentos

Você pode excluir uma relação de sincronização, se não precisar mais sincronizar dados entre a origem e o destino. Esta ação não exclui a instância do corretor de dados e não exclui dados do destino.

Passos

1. Passe o Mouse sobre a relação de sincronização e clique no menu de ação.
2. Clique em **Delete** e, em seguida, clique em **Delete** novamente para confirmar.

Resultado

O Cloud Sync exclui a relação de sincronização.

APIs da Cloud Sync

Os recursos do Cloud Sync disponíveis pela IU da Web também estão disponíveis por meio de APIs RESTful.

Como começar

Para começar a usar as APIs do Cloud Sync, você precisa obter um token de usuário e seu ID de conta do Cloud Central. Você precisará adicionar o token e o ID da conta ao cabeçalho de autorização ao fazer chamadas de API.

Passos

1. Obtenha um token de usuário do NetApp Cloud Central.

```
POST https://netapp-cloud-account.auth0.com/oauth/token
Header: Content-Type: application/json
Body:
{
                "username": "<user_email>",
                "scope": "profile",
                "audience": "https://api.cloud.netapp.com",
                "client_id": "UaVhOIXMWQs5i1WdDxauXe5Mqkb34NJQ",
                "grant_type": "password",
                "password": "<user_password>"
}
```

2. Obtenha seu ID de conta do Cloud Central.

```
GET https://cloudsync.netapp.com/api/accounts
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
```

Esta API retornará uma resposta como a seguinte:

```
[
  {
    "accountId": "account-JeL97Ry3",
    "name": "Test"
  }
]
```

3. Adicione o token de usuário e o ID da conta no cabeçalho de autorização de cada chamada de API.

Exemplo

O exemplo a seguir mostra uma chamada de API para criar um corretor de dados no Microsoft Azure. Você simplesmente substituiria o <user_token> e o <accountId> pelo token e ID obtidos nas etapas anteriores.

```
POST https://cloudsync.netapp.com/api/data-brokers
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
Body: { "name": "databroker1", "type": "AZURE" }
```

O que devo fazer quando o token expirar?

O token de usuário do NetApp tem uma data de expiração. Para atualizar o token, você precisa chamar a API da etapa 1 novamente.

A resposta da API inclui um campo "expires_in" que indica quando o token expira.

Referência da API

A documentação para cada API do Cloud Sync está disponível no "Centro de nuvem da NetApp".

Usando APIs de lista

As APIs de lista são APIs assíncronas, portanto, o resultado não retorna imediatamente (por exemplo: `GET /data-brokers/{id}/list-nfs-export-folders` E `GET /data-brokers/{id}/list-s3-buckets`). A única resposta do servidor é o status HTTP 202. Para obter o resultado real, você deve usar a `GET /messages/client` API.

Passos

1. Chame a API de lista que você deseja usar.
2. Use a `GET /messages/client` API para exibir o resultado da operação.
3. Use a mesma API anexando-a com o ID que você acabou de receber: `GET http://cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>`

   Observe que o ID muda sempre que você chamar a `GET /messages/client` API.

Exemplo

Quando você chama a `list-s3-buckets` API, um resultado não é retornado imediatamente:

```
GET http://cloudsync.netapp.com/api/data-brokers/<data-broker-id>/list-s3-buckets
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

O resultado é o código de status HTTP 202, o que significa que a mensagem foi aceita, mas ainda não foi processada.

Para obter o resultado da operação, você precisa usar a seguinte API:

```
GET http://cloudsync.netapp.com/api/messages/client
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

O resultado é uma matriz com um objeto que inclui um campo de ID. O campo ID representa a última mensagem enviada pelo servidor. Por exemplo:

```
[
    {
        "header": {
            "requestId": "init",
            "clientId": "init",
            "agentId": "init"
        },
        "payload": {
            "init": {}
        },
        "id": "5801"
    }
]
```

Agora você faria a seguinte chamada de API usando o ID que acabou de receber:

```
GET http://cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

O resultado é uma matriz de mensagens. Dentro de cada mensagem há um objeto payload, que consiste no nome da operação (como chave) e seu resultado (como valor). Por exemplo:

```
[
    {
        "payload": {
            "list-s3-buckets": [
                {
                    "tags": [
                        {
                            "Value": "100$",
                            "Key": "price"
                        }
                    ],
                    "region": {
                        "displayName": "US West (Oregon)",
                        "name": "us-west-2"
                    },
                    "name": "small"
                }
            ]
        },
        "header": {
            "requestId": "f687ac55-2f0c-40e3-9fa6-57fb8c4094a3",
            "clientId": "5beb032f548e6e35f4ed1ba9",
            "agentId": "5bed61f4489fb04e34a9aac6"
        },
        "id": "5802"
    }
]
```


Perguntas frequentes técnicas do Cloud Sync

Esta FAQ pode ajudar se você está apenas procurando uma resposta rápida para uma pergunta.

Como começar

As perguntas a seguir estão relacionadas a como começar a usar o Cloud Sync.

Como funciona o Cloud Sync?

O Cloud Sync usa o software de corretor de dados NetApp para sincronizar dados de uma origem para um destino (isso é chamado de *relação de sincronização*).

O corretor de dados controla as relações de sincronização entre suas fontes e alvos. Depois de configurar uma relação de sincronização, o Cloud Sync analisa o sistema de origem e o divide em vários fluxos de replicação para enviar para os dados de destino selecionados.

Após a cópia inicial, o serviço sincroniza todos os dados alterados com base na programação definida.

Como funciona o teste gratuito de 14 dias?

A avaliação gratuita de 14 dias começa quando você se inscreve no serviço Cloud Sync. Você não está sujeito a cobranças do NetApp para relacionamentos do Cloud Sync criados por 14 dias. No entanto, todas as cobranças de recursos para qualquer agente de dados que você implantar ainda se aplicam.

Quanto custa o Cloud Sync?

Existem dois tipos de custos associados ao uso do Cloud Sync: Taxas de serviço e taxas de recursos.

Taxas de serviço

Para os preços de pagamento conforme o uso, as taxas de serviço do Cloud Sync são de hora em hora, com base no número de relacionamentos de sincronização criados por você.

- "Veja a definição de preço para pagamento conforme o uso na AWS"
- "Veja os preços anuais na AWS"
- "Ver preços no Azure"

As licenças do Cloud Sync também estão disponíveis através do seu representante da NetApp. Cada licença permite 20 relações de sincronização por 12 meses.

"Saiba mais sobre licenças".

Cobranças de recursos

As cobranças por recursos estão relacionadas aos custos de computação e storage para executar o agente de dados na nuvem.

Como é cobrado o Cloud Sync?

Há duas maneiras de pagar pelas relações de sincronização após o término da avaliação gratuita de 14 dias. A primeira opção é se inscrever na AWS ou no Azure, o que permite que você pague conforme o uso ou pague anualmente. A segunda opção é comprar licenças diretamente da NetApp.

Posso usar o Cloud Sync fora da nuvem?

Sim, você pode usar o Cloud Sync em uma arquitetura que não seja na nuvem. A origem e o destino podem residir no local, assim como o agente de dados.

Observe os seguintes pontos-chave sobre o uso do Cloud Sync fora da nuvem:

- Para sincronização no local, um bucket privado do Amazon S3 está disponível por meio do NetApp StorageGRID.
- O corretor de dados precisa de uma conexão com a Internet para se comunicar com o serviço Cloud Sync.
- Se você não comprar uma licença diretamente da NetApp, precisará de uma conta da AWS ou do Azure para a cobrança do serviço PAYGO Cloud Sync.

Como faço para acessar o Cloud Sync?

O Cloud Sync está disponível no Gerenciador de nuvem na guia **Sincronizar**.

Fontes e alvos suportados

As perguntas a seguir relacionadas à origem e aos destinos que são suportados em um relacionamento de sincronização.

Quais fontes e alvos o Cloud Sync suporta?

O Cloud Sync suporta muitos tipos diferentes de relações de sincronização. "Veja a lista inteira".

Quais versões de NFS e SMB são compatíveis com o Cloud Sync?

O Cloud Sync é compatível com NFS versão 3 e posterior, e SMB versão 1 e posterior.

"Saiba mais sobre os requisitos de sincronização".

Quando o Amazon S3 é o destino, os dados podem ser dispostos em camadas em uma classe de armazenamento S3 específica?

Sim, você pode escolher uma classe de armazenamento S3 específica quando o AWS S3 for o destino:

- Standard (esta é a classe padrão)
- Disposição em camadas inteligente
- Acesso padrão-infrequente
- Uma zona de acesso pouco frequente
- Glacier
- Glacier Deep Archive

E quanto às camadas de storage do Azure Blob?

Você pode escolher uma categoria de storage específica do Azure Blob quando um contêiner de Blob é o destino:

- Armazenamento a quente
- Armazenamento frio

Rede

As perguntas a seguir referem-se aos requisitos de rede para o Cloud Sync.

Quais são os requisitos de rede para o Cloud Sync?

O ambiente do Cloud Sync exige que o agente de dados esteja conetado à origem e ao destino por meio do protocolo selecionado (NFS, SMB, EFS) ou da API de storage de objetos (Amazon S3, Azure Blob, IBM Cloud Object Storage).

Além disso, o corretor de dados precisa de uma conexão de saída de Internet pela porta 443 para que possa se comunicar com o serviço Cloud Sync e entrar em Contato com alguns outros serviços e repositórios.

Para mais detalhes, "rever os requisitos de rede".

Há limitações de rede relacionadas à conetividade do data broker?

Os corretores de dados exigem acesso à Internet. Não oferecemos suporte a um servidor proxy ao implantar o corretor de dados no Azure ou no Google Cloud Platform.

Sincronização de dados

As perguntas a seguir referem-se a como a sincronização de dados funciona.

Com que frequência ocorre a sincronização?

A programação padrão é definida para sincronização diária. Após a sincronização inicial, você pode:

- Modifique a programação de sincronização para o número desejado de dias, horas ou minutos
- Desative a programação de sincronização
- Eliminar a programação de sincronização (nenhum dado será perdido; apenas a relação de sincronização será removida)

Qual é a programação mínima de sincronização?

Você pode agendar uma relação para sincronizar dados a cada 1 minutos.

O corretor de dados tenta novamente quando um arquivo não consegue sincronizar? Ou o tempo limite?

O corretor de dados não expira quando um único arquivo falha na transferência. Em vez disso, o corretor de dados tenta novamente 3 vezes antes de pular o arquivo. O valor de repetição é configurável nas definições de uma relação de sincronização.

"Saiba como alterar as configurações de uma relação de sincronização".

E se eu tiver um conjunto de dados muito grande?

Se um único diretório contém 600.000 arquivos ou mais, mailto:ng-cloudsync-support NetApp.com[Contact US] para que possamos ajudá-lo a configurar o corretor de dados para lidar com a carga útil. Talvez seja necessário adicionar memória adicional à máquina do corretor de dados.

Segurança

As seguintes perguntas relacionadas à segurança.

O Cloud Sync é seguro?

Sim. Toda a conetividade de rede do serviço Cloud Sync é feita usando "Amazon Simple Queue Service (SQS)"o .

Toda a comunicação entre o agente de dados e o Amazon S3, Azure Blob, Google Cloud Storage e IBM Cloud Object Storage é feita por meio do protocolo HTTPS.

Se você estiver usando o Cloud Sync com sistemas locais (de origem ou destino), veja algumas opções de conetividade recomendadas:

- Uma conexão AWS Direct Connect, Azure ExpressRoute ou Google Cloud Interconnect, que não é roteada pela Internet (e só pode se comunicar com as redes de nuvem especificadas)

- Uma conexão VPN entre seu dispositivo de gateway local e suas redes na nuvem
- Para transferência de dados extra segura com buckets do S3, armazenamento de Blobs do Azure ou Google Cloud Storage, é possível estabelecer um endpoint Amazon Private S3, pontos de extremidade de serviço da rede virtual do Azure ou o acesso privado do Google.

Qualquer um desses métodos estabelece uma conexão segura entre seus servidores nas locais e um agente de dados Cloud Sync.

Os dados são criptografados pelo Cloud Sync?

- O Cloud Sync é compatível com criptografia de dados em trânsito entre servidores NFS de origem e destino. "Saiba mais".
- A criptografia não é suportada com SMB.
- Quando um bucket do Amazon S3 é o destino em uma relação de sincronização, você pode escolher se deseja ativar a criptografia de dados usando a criptografia AWS KMS ou AES-256.

Permissões

As perguntas a seguir estão relacionadas às permissões de dados.

As permissões de dados SMB são sincronizadas com o local de destino?

Você pode configurar o Cloud Sync para preservar listas de controle de acesso (ACLs) entre um compartilhamento SMB de origem e um compartilhamento SMB de destino. Ou você mesmo pode copiar manualmente as ACLs. "Saiba como copiar ACLs entre compartilhamentos SMB".

As permissões de dados NFS são sincronizadas com o local de destino?

O Cloud Sync copia automaticamente as permissões NFS entre servidores NFS da seguinte forma:

- NFS versão 3: O Cloud Sync copia as permissões e o proprietário do grupo de usuários.
- NFS versão 4: O Cloud Sync copia as ACLs.

Desempenho

As perguntas a seguir referem-se ao desempenho do Cloud Sync.

O que representa o indicador de progresso de uma relação de sincronização?

A relação de sincronização mostra a taxa de transferência do adaptador de rede do corretor de dados. Se você acelerou o desempenho de sincronização usando vários corretores de dados, a taxa de transferência será a soma de todo o tráfego. Essa taxa de transferência é atualizada a cada 20 segundos.

Estou enfrentando problemas de desempenho. Podemos limitar o número de transferências simultâneas?

O corretor de dados pode sincronizar arquivos 4 de cada vez. Se você tiver arquivos muito grandes (vários TBs cada), pode levar muito tempo para concluir o processo de transferência e o desempenho pode ser afetado.

Limitar o número de transferências simultâneas pode ajudar. Mailto:ng-cloudsync-support NetApp.com[Contacte-nos para obter ajuda].

Por que estou tendo baixo desempenho com o Azure NetApp Files?

Quando você sincroniza dados com ou do Azure NetApp Files, você pode ter falhas e problemas de desempenho se o nível de serviço de disco for padrão.

Altere o nível de serviço para Premium ou Ultra para melhorar o desempenho de sincronização.

"Saiba mais sobre os níveis de serviço e a taxa de transferência do Azure NetApp Files".

Por que estou tendo baixo desempenho com o Cloud Volumes Service para AWS?

Ao sincronizar dados de ou para um volume de nuvem, você pode ter falhas e problemas de desempenho se o nível de performance do volume de nuvem for padrão.

Altere o nível de serviço para Premium ou Extreme para melhorar o desempenho de sincronização.

Quantos corretores de dados são necessários?

Ao criar um novo relacionamento, você começa com um único agente de dados (a menos que você tenha selecionado um agente de dados existente que pertence a um relacionamento de sincronização acelerada). Em muitos casos, um único agente de dados pode atender aos requisitos de desempenho de um relacionamento de sincronização. Se isso não acontecer, você pode acelerar o desempenho de sincronização adicionando corretores de dados adicionais. Mas você deve primeiro verificar outros fatores que podem afetar o desempenho da sincronização.

Vários fatores podem afetar o desempenho da transferência de dados. O desempenho geral da sincronização pode ser afetado devido à largura de banda, latência e topologia da rede, bem como às especificações de VM do agente de dados e ao desempenho do sistema de armazenamento. Por exemplo, um único corretor de dados em um relacionamento de sincronização pode atingir 100 MB/s, enquanto a taxa de transferência de disco no destino pode permitir apenas 64 MB/s. Como resultado, o agente de dados continua tentando copiar os dados, mas o destino não consegue atender ao desempenho do agente de dados.

Portanto, certifique-se de verificar o desempenho de sua rede e a taxa de transferência de disco no destino.

Depois, você pode considerar acelerar o desempenho de sincronização adicionando um agente de dados adicional para compartilhar a carga desse relacionamento. "Saiba como acelerar o desempenho de sincronização".

Eliminar coisas

As perguntas a seguir referem-se à exclusão de relacionamentos de sincronização e dados de fontes e destinos.

O que acontece se eu excluir meu relacionamento com o Cloud Sync?

A exclusão de um relacionamento interrompe todas as futuras sincronizações de dados e encerra o pagamento. Todos os dados sincronizados com o alvo permanecem no estado em que se encontram.

O que acontece se eu excluir algo do meu servidor de origem? É removido do alvo também?

Por padrão, se você tiver uma relação de sincronização ativa, o item excluído no servidor de origem não será excluído do destino durante a próxima sincronização. Mas há uma opção nas configurações de sincronização para cada relacionamento, onde você pode definir que o Cloud Sync excluirá arquivos no local de destino se eles foram excluídos da origem.

"Saiba como alterar as configurações de uma relação de sincronização".

O que acontece se eu excluir algo do meu alvo? É removido da minha fonte também?

Se um item for excluído do destino, ele não será removido da origem. O relacionamento é unidirecional, da origem ao destino. No próximo ciclo de sincronização, o Cloud Sync compara a origem com o destino, identifica que o item está ausente e o Cloud Sync o copia novamente da origem para o destino.

Solução de problemas

"Base de Conhecimento da NetApp: Perguntas frequentes do Cloud Sync: Suporte e solução de problemas"

Mergulho profundo do agente de dados

A seguinte pergunta diz respeito ao corretor de dados.

Você pode explicar a arquitetura do corretor de dados?

Claro. Aqui estão os pontos mais importantes:

- O corretor de dados é um aplicativo node.js executado em um host Linux.
- O Cloud Sync implanta o agente de dados da seguinte forma:
  - AWS: A partir de um modelo do AWS CloudFormation
  - Azure: Do Azure Resource Manager
  - Google: Do Google Cloud Deployment Manager
  - Se você usa seu próprio host Linux, você precisa instalar manualmente o software
- O software de data broker atualiza-se automaticamente para a versão mais recente.
- O corretor de dados usa o AWS SQS como um canal de comunicação confiável e seguro e para controle e monitoramento. SQS também fornece uma camada de persistência.
- Você pode adicionar corretores de dados adicionais a um relacionamento para aumentar a velocidade de transferência e adicionar alta disponibilidade. Há resiliência de serviços se um agente de dados falhar.

Tenha insights sobre a privacidade de dados

Saiba mais sobre o Cloud Compliance

O Cloud Compliance é um serviço de conformidade e privacidade de dados do Cloud Manager que analisa volumes, buckets do Amazon S3 e bancos de dados para identificar os dados pessoais e confidenciais que residem nesses arquivos. Usando tecnologia orientada por inteligência artificial (AI), o Cloud Compliance ajuda as organizações a entender o contexto dos dados e identificar dados confidenciais.

"Saiba mais sobre os casos de uso do Cloud Compliance".

Caraterísticas

O Cloud Compliance fornece várias ferramentas para ajudar você a manter a conformidade. Você pode usar o Cloud Compliance para:

- Identificar informações pessoais identificáveis (PII)
- Identifique um amplo escopo de informações confidenciais conforme exigido pelas regulamentações de privacidade do GDPR, CCPA, PCI e HIPAA
- Responder às solicitações de acesso do titular dos dados (DSAR)

Ambientes de trabalho e fontes de dados compatíveis

O Cloud Compliance pode analisar dados dos seguintes tipos de fontes de dados:

- Cloud Volumes ONTAP na AWS
- Cloud Volumes ONTAP no Azure
- Azure NetApp Files
- Amazon S3
- Bancos de dados que residem em qualquer lugar (não há requisito de que o banco de dados resida em um ambiente de trabalho)

Observação: para o Azure NetApp Files, o Cloud Compliance pode verificar todos os volumes que estão na mesma região que o Cloud Manager.

Custo

- O custo para usar o Cloud Compliance depende da quantidade de dados que você está digitalizando. Em 7th de outubro de 2020, os primeiros 1 TB de dados verificados pelo Cloud Compliance em um espaço de trabalho do Cloud Manager são gratuitos. Isso inclui dados do Cloud Volumes ONTAP volumes, do Azure NetApp Files volumes, buckets do Amazon S3 e esquemas de banco de dados. Uma assinatura do AWS ou Azure Marketplace é necessária para continuar a digitalizar dados após esse ponto. "preços"Consulte para obter detalhes.

  "Saiba como se inscrever".

- A instalação do Cloud Compliance requer a implantação de uma instância de nuvem, o que resulta em cobranças do provedor de nuvem onde ela é implantada. Consulte o tipo de instância que é implantada

para cada provedor de nuvem

- O Cloud Compliance exige que você implante um conetor. Em muitos casos, você já tem um conetor devido a outros serviços e storage que você está usando no Cloud Manager. A instância do conetor resulta em cobranças do provedor de nuvem onde ela é implantada. Consulte "tipo de instância implantada para cada provedor de nuvem".

Custos de transferência de dados

Os custos de transferência de dados dependem da configuração. Se a instância e a fonte de dados do Cloud Compliance estiverem na mesma zona de disponibilidade e região, não haverá custos de transferência de dados. Mas se a fonte de dados, como um cluster Cloud Volumes ONTAP ou um bucket do S3, estiver em uma zona de disponibilidade ou região *diferente*, você será cobrado pelo seu provedor de nuvem pelos custos de transferência de dados. Veja estes links para mais detalhes:

- "AWS: Definição de preço do Amazon EC2"
- "Microsoft Azure: Detalhes de preços de largura de banda"

Como o Cloud Compliance funciona

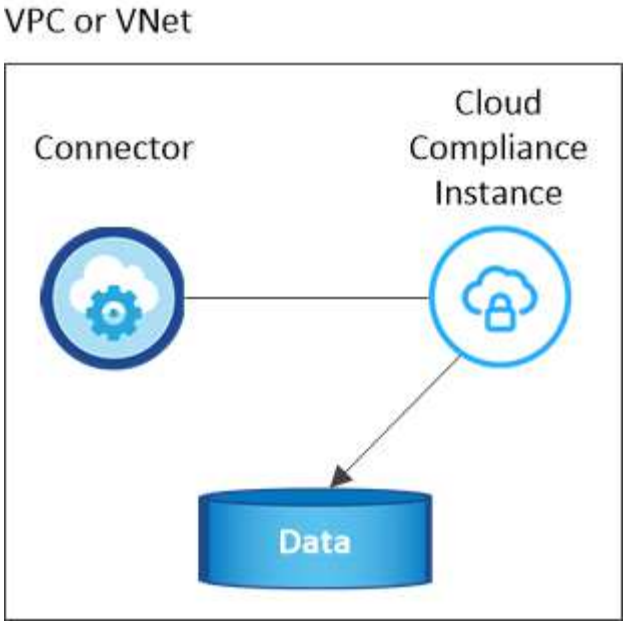
Em um alto nível, o Cloud Compliance funciona assim:

1. Você implanta uma instância de Cloud Compliance no Cloud Manager.
2. Você o habilita em um ou mais ambientes de trabalho ou em seus bancos de dados.
3. O Cloud Compliance verifica os dados usando um processo de aprendizado de AI.
4. No Cloud Manager, você clica em **Compliance** e usa o painel e as ferramentas de relatórios fornecidos para ajudar em seus esforços de conformidade.

A instância do Cloud Compliance

Quando você ativa o Cloud Compliance, o Cloud Manager implanta uma instância de Cloud Compliance na mesma sub-rede que o conetor. "Saiba mais sobre conetores."

Se o conetor for instalado no local, ele implanta a instância de conformidade em nuvem na mesma VPC ou VNet como o primeiro sistema Cloud Volumes ONTAP na solicitação.



Observe o seguinte sobre a instância:

- No Azure, o Cloud Compliance é executado em uma VM Standard_D16s_v3 com um disco de 512 GB.
- Na AWS, o Cloud Compliance é executado em uma instância do m5,4xlarge com um disco GP2 de 500 GB.

  Em regiões onde o m5,4xlarge não está disponível, o Cloud Compliance é executado em uma instância do m4,4xlarge.

  Alterar ou redimensionar o tipo de instância/VM não é suportado. Você precisa usar o tamanho fornecido.

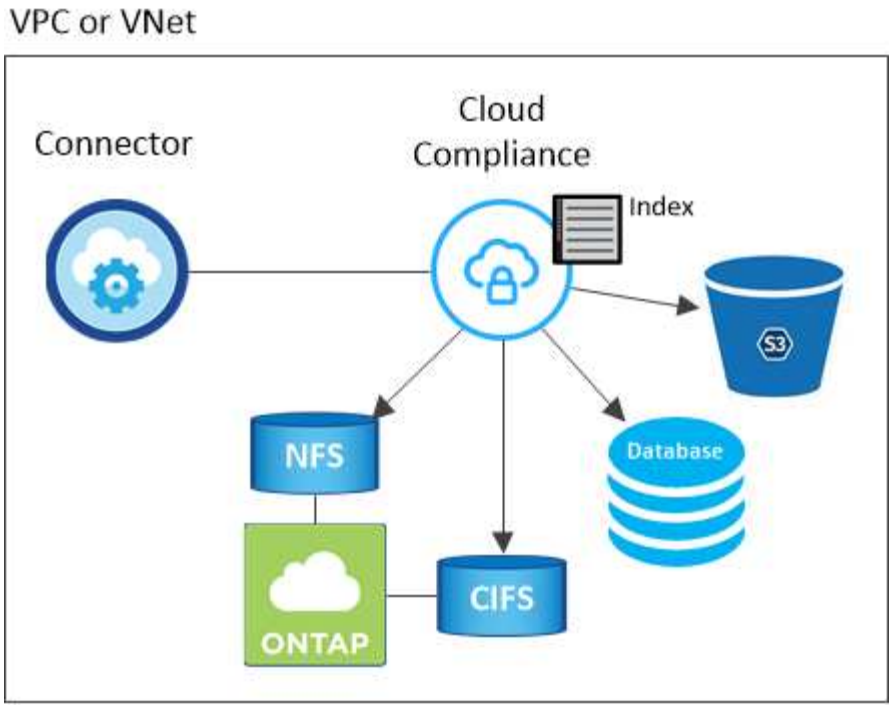
- A instância é chamada *CloudCompliance* com um hash gerado (UUID) concatenado a ela. Por exemplo: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- Somente uma instância do Cloud Compliance é implantada por conetor.
- As atualizações do software de conformidade na nuvem são automatizadas - você não precisa se preocupar com isso.

A instância deve permanecer em execução o tempo todo, porque o Cloud Compliance verifica continuamente os dados.

Como as digitalizações funcionam

Depois de ativar o Cloud Compliance e selecionar os volumes, buckets ou esquemas de banco de dados que você deseja verificar, ele começará imediatamente a verificar os dados para identificar dados pessoais e confidenciais. Ele mapeia seus dados organizacionais, categoriza cada arquivo e identifica e extrai entidades e padrões predefinidos nos dados. O resultado da digitalização é um índice de informações pessoais, informações pessoais confidenciais e categorias de dados.

O Cloud Compliance conecta-se aos dados como qualquer outro cliente, com a montagem de volumes NFS e CIFS. Os volumes NFS são acessados automaticamente como somente leitura, enquanto você precisa fornecer credenciais do active Directory para verificar volumes CIFS.



Após a verificação inicial, o Cloud Compliance verifica continuamente cada volume para detetar alterações incrementais (é por isso que é importante manter a instância em execução).

Pode ativar e desativar as digitalizações nas "nível de volume", em , "nível do balde"e "nível de esquema do banco de dados"em .

Informações indexadas pelo Cloud Compliance

O Cloud Compliance coleta, indexa e atribui categorias a dados não estruturados (arquivos). Os dados indexados pelo Cloud Compliance incluem os seguintes:

Metadados padrão

O Cloud Compliance coleta metadados padrão sobre arquivos: O tipo de arquivo, seu tamanho, datas de criação e modificação, etc.

Dados pessoais

Informações de identificação pessoal, como endereços de e-mail, números de identificação ou números de cartão de crédito. "Saiba mais sobre dados pessoais".

Dados pessoais confidenciais

Tipos especiais de informações sensíveis, como dados de saúde, origem étnica ou opiniões políticas, conforme definido pelo GDPR e outros regulamentos de privacidade. "Saiba mais sobre dados pessoais confidenciais".

Categorias

O Cloud Compliance pega os dados que digitalizou e os divide em diferentes tipos de categorias. Categorias são tópicos baseados na análise de IA do conteúdo e metadados de cada arquivo. "Saiba mais sobre categorias".

Reconhecimento de entidade de nome

O Cloud Compliance usa IA para extrair nomes de pessoas naturais de documentos. "Saiba mais sobre como responder às solicitações de acesso do titular dos dados".

Visão geral da rede

O Cloud Manager implanta a instância do Cloud Compliance com um grupo de segurança que permite conexões HTTP de entrada da instância do conetor.

Ao usar o Cloud Manager no modo SaaS, a conexão com o Cloud Manager é feita por HTTPS, e os dados privados enviados entre o navegador e a instância de conformidade da nuvem são protegidos com criptografia de ponta a ponta, o que significa que o NetApp e terceiros não podem lê-lo.

Se você precisar usar a interface de usuário local em vez da interface de usuário SaaS por qualquer motivo, ainda poderá "Acesse a IU local".

As regras de saída estão completamente abertas. O acesso à Internet é necessário para instalar e atualizar o software Cloud Compliance e enviar métricas de uso.

Se você tem exigências estritas da rede, "Saiba mais sobre os endpoints que o Cloud Compliance contacta".

Acesso do usuário às informações de conformidade

A função atribuída a cada usuário fornece diferentes recursos no Cloud Manager e no Cloud Compliance:

- **Administradores de conta** podem gerenciar configurações de conformidade e visualizar informações de conformidade para todos os ambientes de trabalho.
- **Os administradores do Workspace** podem gerenciar as configurações de conformidade e exibir informações de conformidade somente para sistemas aos quais eles têm permissões de acesso. Se um administrador do Workspace não puder acessar um ambiente de trabalho no Cloud Manager, ele não poderá ver nenhuma informação de conformidade para o ambiente de trabalho na guia Compliance.
- Os usuários com a função **Visualizador de conformidade na nuvem** só podem visualizar informações de conformidade e gerar relatórios para sistemas que eles têm permissão para acessar. Esses usuários não podem ativar/desativar a digitalização de volumes, buckets ou esquemas de banco de dados.

"Saiba mais sobre as funções do Cloud Manager" e como "adicione usuários com funções específicas".

Comece agora

Implante o Cloud Compliance

Execute algumas etapas para implantar a instância de Cloud Compliance no workspace do Cloud Manager.

Início rápido

Comece rapidamente seguindo estas etapas ou role para baixo até as seções restantes para obter detalhes completos.

Crie um conetor

Se você ainda não tiver um conetor, crie um conetor no Azure ou na AWS. "Criando um conetor na AWS"Consulte ou "Criando um conetor no Azure".

Reveja os pré-requisitos

Certifique-se de que seu ambiente de nuvem atenda aos pré-requisitos, que incluem 16 vCPUs para a instância Cloud Compliance, acesso de saída à Internet para a instância, conetividade entre o conetor e o Cloud Compliance pela porta 80 e muito mais. Veja a lista completa.

Implante o Cloud Compliance

Inicie o assistente de instalação para implantar a instância de Cloud Compliance no Cloud Manager.

Inscreva-se no serviço Cloud Compliance

Os primeiros 1 TB de dados verificados pelo Cloud Compliance no Cloud Manager são gratuitos. Uma assinatura do AWS ou Azure Marketplace é necessária para continuar a digitalizar dados após esse ponto.

Criando um conetor

Se você ainda não tiver um conetor, crie um conetor no Azure ou na AWS. "Criando um conetor na AWS"Consulte ou "Criando um conetor no Azure". Na maioria dos casos, você provavelmente terá um conetor configurado antes de tentar ativar o Cloud Compliance porque a maioria "Os recursos do Cloud Manager precisam de um conetor", mas há casos em que você precisa configurar um agora.

Há alguns cenários em que você precisa usar um conetor na AWS ou no Azure para conformidade com a nuvem.

- Ao digitalizar dados no Cloud Volumes ONTAP na AWS ou nos buckets do AWS S3, você usa um conetor na AWS.
- Ao digitalizar dados no Cloud Volumes ONTAP no Azure ou no Azure NetApp Files, você usa um conetor no Azure.
- Os bancos de dados podem ser digitalizados usando qualquer um dos conetores.

Como você pode ver, pode haver algumas situações em que você precisa usar "Vários conetores".

Se você está planejando digitalizar o Azure NetApp Files, você precisa garantir que está implantando na mesma região que os volumes que deseja digitalizar.

Rever pré-requisitos

Revise os pré-requisitos a seguir para garantir que você tenha uma configuração compatível antes de implantar o Cloud Compliance.

Ative o acesso de saída à Internet

A conformidade com a nuvem requer acesso de saída à Internet. Se a sua rede virtual usar um servidor proxy para acesso à Internet, certifique-se de que a instância do Cloud Compliance tenha acesso de saída à Internet para contactar os seguintes endpoints. Observe que o Cloud Manager implanta a instância de Cloud Compliance na mesma sub-rede que o conetor.

Endpoints	Finalidade
https://cloudmanager.cloud.NetApp.com	Comunicação com o serviço Cloud Manager, que inclui contas do Cloud Central.
https://NetApp-cloud-account.auth0.com https://auth0.com	Comunicação com o NetApp Cloud Central para autenticação centralizada de usuários.
https://cloud-compliance-support-NetApp.s3.us-west-2.amazonaws.com https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Fornece acesso a imagens de software, manifestos e modelos.
https://kinesis.us-east-1.amazonaws.com	Permite que o NetApp transmita dados de Registros de auditoria.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com	Permite que o Cloud Compliance acesse e baixe manifestos e modelos e envie logs e métricas.

Certifique-se de que o Cloud Manager tenha as permissões necessárias

Certifique-se de que o Cloud Manager tenha permissões para implantar recursos e criar grupos de segurança para a instância do Cloud Compliance. Você pode encontrar as permissões mais recentes do Cloud Manager no "As políticas fornecidas pela NetApp".

Verifique os limites do seu vCPU

Certifique-se de que o limite de vCPU do seu provedor de nuvem permita a implantação de uma instância com 16 núcleos. Você precisará verificar o limite do vCPU para a família de instâncias relevante na região em que o Cloud Manager está sendo executado.

Na AWS, a família de instâncias é *instâncias padrão sob demanda*. No Azure, a família de instâncias é *Standard DSv3 Family*.

Para obter mais detalhes sobre os limites do vCPU, consulte o seguinte:

- "Documentação da AWS: Limites de serviço do Amazon EC2"
- "Documentação do Azure: Cotas de vCPU de máquina virtual"

Garantir que o Cloud Manager possa acessar o Cloud Compliance

Garanta a conetividade entre o conetor e a instância de conformidade com a nuvem. O grupo de segurança do conetor deve permitir o tráfego de entrada e saída pela porta 80 de e para a instância do Cloud Compliance.

Essa conexão permite a implantação da instância de conformidade na nuvem e permite exibir informações na guia conformidade.

Configure a descoberta do Azure NetApp Files

Antes de poder digitalizar volumes para Azure NetApp Files, "O Cloud Manager deve estar configurado para descobrir a configuração".

Garanta que você mantenha o Cloud Compliance em execução

A instância do Cloud Compliance precisa continuar a analisar seus dados continuamente.

Garanta a conetividade do navegador da Web com o Cloud Compliance

Depois que o Cloud Compliance estiver ativado, certifique-se de que os usuários acessem a interface do Cloud Manager a partir de um host que tenha uma conexão com a instância do Cloud Compliance.

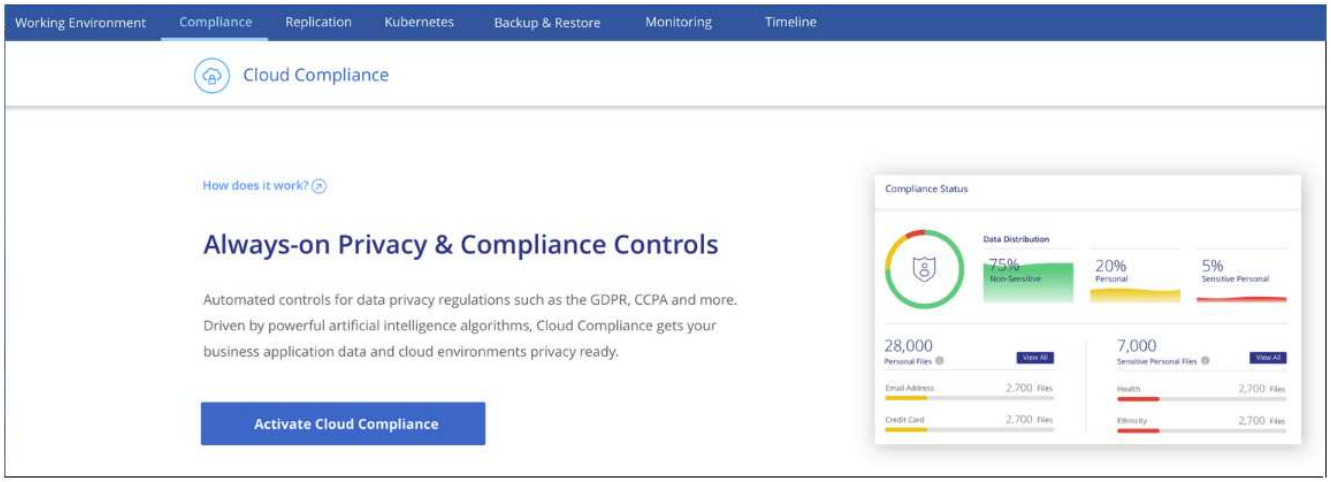
A instância Cloud Compliance usa um endereço IP privado para garantir que os dados indexados não sejam acessíveis à Internet. Como resultado, o navegador da Web que você usa para acessar o Cloud Manager deve ter uma conexão com esse endereço IP privado. Essa conexão pode vir de uma conexão direta com a AWS ou o Azure (por exemplo, uma VPN) ou de um host que esteja dentro da mesma rede que a instância de conformidade com a nuvem.

Implantando a instância de Cloud Compliance

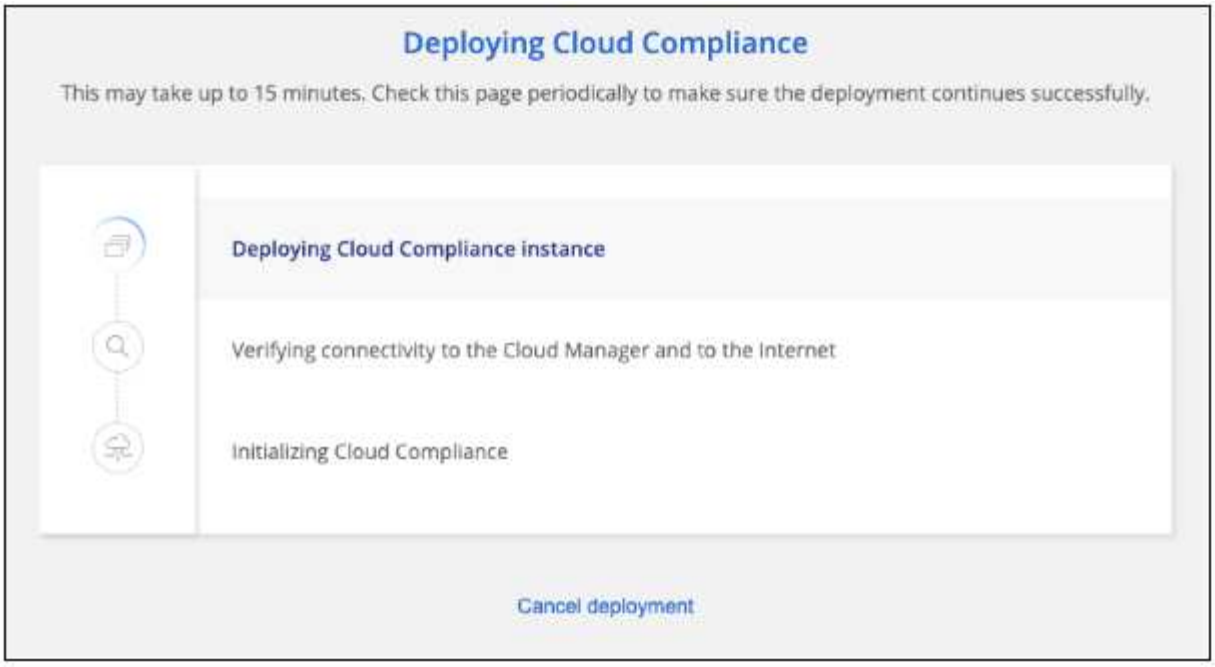
Você implanta uma instância do Cloud Compliance para cada instância do Cloud Manager.

Passos

1. No Cloud Manager, clique em **Cloud Compliance**.
2. Clique em **Ativar Cloud Compliance** para iniciar o assistente de implantação.



3. O assistente exibe o progresso à medida que passa pelas etapas de implantação. Ele vai parar e pedir a entrada se ele se deparar com quaisquer problemas.



4. Quando a instância for implantada, clique em **Continue to Configuration** para ir para a página *Scan Configuration*.

Resultado

O Cloud Manager implanta a instância de Cloud Compliance no seu provedor de nuvem.

O que vem a seguir

Na página Configuração de digitalização, você pode selecionar os ambientes de trabalho, volumes e buckets que você deseja verificar para conformidade. Você também pode se conetar a um servidor de banco de dados para verificar esquemas de banco de dados específicos. Ative o Cloud Compliance em qualquer uma dessas fontes de dados.

Subscrever o serviço Cloud Compliance

Os primeiros 1 TB de dados verificados pelo Cloud Compliance em um espaço de trabalho do Cloud Manager são gratuitos. Uma assinatura do AWS ou Azure Marketplace é necessária para continuar a digitalizar dados após esse ponto.

Você pode se inscrever a qualquer momento e não será cobrado até que a quantidade de dados exceda 1 TB. Você sempre pode ver a quantidade total de dados que está sendo digitalizada no Painel de conformidade da nuvem. E o botão *Inscrever-se agora* facilita a assinatura quando estiver pronto.

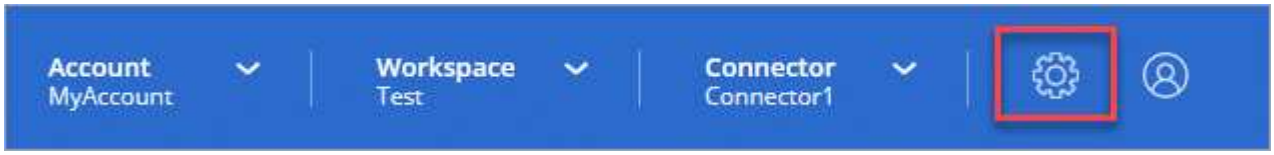
Observação: se você for solicitado pelo Cloud Compliance para se inscrever, mas já tiver uma assinatura do Azure, provavelmente estará usando a antiga assinatura do **Gerenciador de nuvem** e precisará mudar para a nova assinatura do **Gerenciador de nuvem** do NetApp. Mudando para o novo plano do NetApp Cloud

Manager no AzureConsulte para obter detalhes.

Passos

Essas etapas devem ser concluídas por um usuário que tenha a função *Account Admin*.

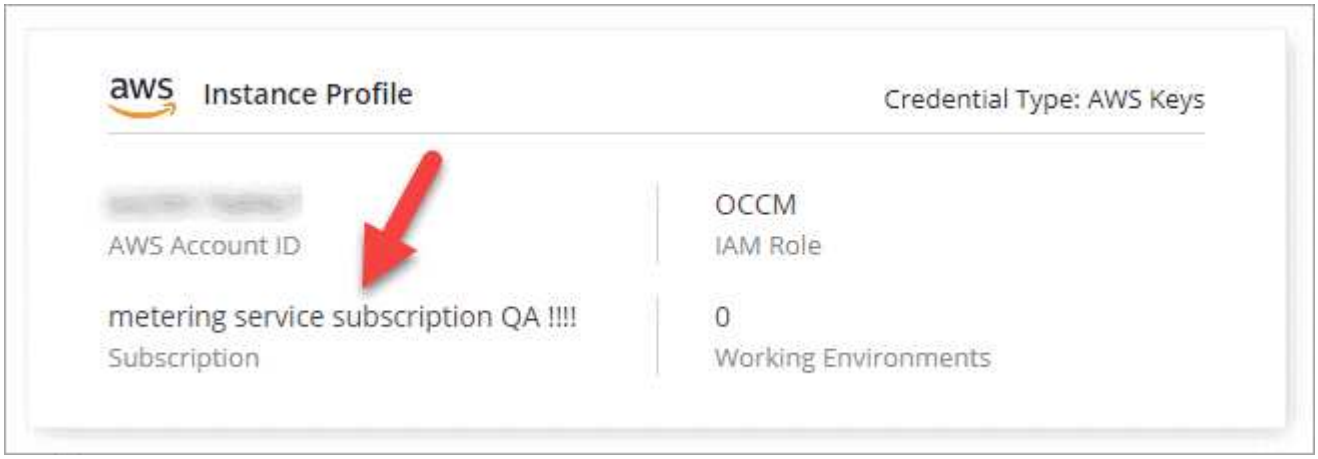
1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **credenciais**.



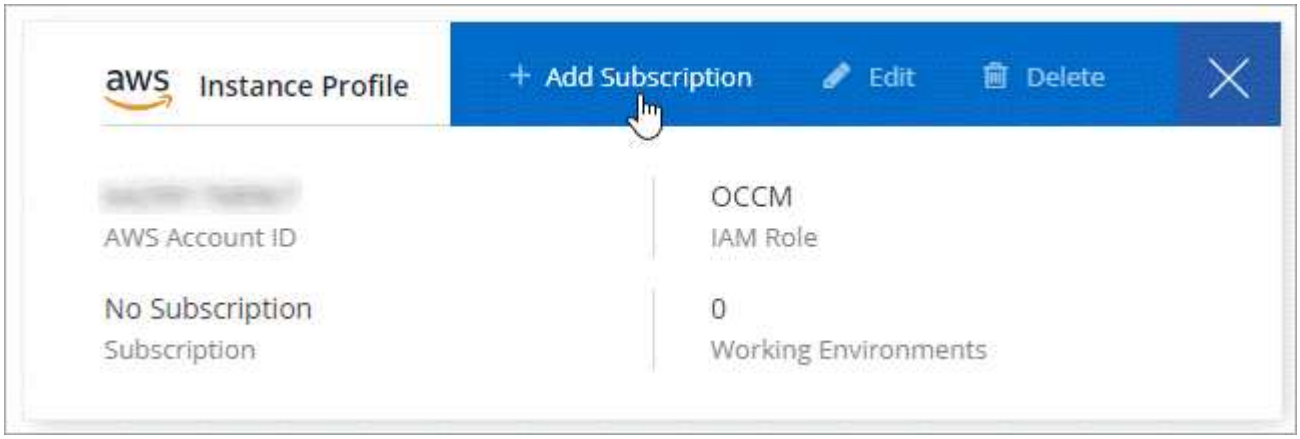
2. Encontre as credenciais para o perfil de instância da AWS ou identidade do serviço gerenciado do Azure.

   A assinatura deve ser adicionada ao Perfil de instância ou identidade de serviço gerenciado. O carregamento não funciona de outra forma.

   Se você já tem uma assinatura, então você está tudo pronto - não há mais nada que você precisa fazer.



3. Se você ainda não tiver uma assinatura, passe o Mouse sobre as credenciais e clique no menu de ação.
4. Clique em **Adicionar assinatura**.



5. Clique em **Adicionar assinatura**, clique em **continuar** e siga as etapas.

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

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

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

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

Mudando para o novo plano do Cloud Manager no Azure

O Cloud Compliance foi adicionado à assinatura do Azure Marketplace chamada **Gerenciador de nuvem da NetApp** em 7 de outubro de 2020. Se você já tiver a assinatura original do Azure **Cloud Manager**, ela não permitirá que você use o Cloud Compliance.

Você precisa seguir estas etapas e selecionar a nova assinatura **Gerenciador de nuvem do NetApp** e remover a antiga assinatura **Gerenciador de nuvem**.

Se sua assinatura já tiver sido emitida com uma oferta particular especial, você precisa entrar em Contato com a NetApp para que possamos emitir uma nova oferta privada especial com conformidade incluída.

Passos

Essas etapas são semelhantes à adição de uma nova assinatura conforme descrito acima, mas variam em alguns lugares.

1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **credenciais**.
2. Encontre as credenciais para a identidade do Serviço gerenciado do Azure para a qual você deseja alterar a assinatura e passe o Mouse sobre as credenciais e clique em **assinatura associada**.

   Os detalhes da sua assinatura atual do Marketplace são exibidos.
3. Clique em **Adicionar assinatura**, clique em **continuar** e siga as etapas. Você é redirecionado para o portal do Azure para criar a nova assinatura.
4. Certifique-se de selecionar o plano **Gerenciador de nuvem da NetApp** que fornece acesso ao Cloud Compliance e não ao **Gerenciador de nuvem**.
5. Siga as etapas no vídeo para associar uma assinatura do Marketplace a uma assinatura do Azure:

   ► https://docs.netapp.com/pt-br/occm38//media/video_subscribing_azure.mp4 *(video)*
6. Retorne ao Cloud Manager, selecione a nova assinatura e clique em **Associate**.
7. Para verificar se sua assinatura foi alterada, passe o Mouse sobre a assinatura "i" acima no cartão de credenciais.

   Agora você pode cancelar sua assinatura antiga no portal do Azure.
8. No portal do Azure, acesse Software as a Service (SaaS), selecione a assinatura e clique em **Cancelar inscrição**.

Ative a digitalização nas suas fontes de dados

Primeiros passos com o Cloud Compliance para Cloud Volumes ONTAP e Azure NetApp Files

Conclua algumas etapas para dar os primeiros passos com o Cloud Compliance for Cloud Volumes ONTAP ou Azure NetApp Files.

Início rápido

Comece rapidamente seguindo estas etapas ou role para baixo até as seções restantes para obter detalhes completos.

Implante a instância do Cloud Compliance

"Implante o Cloud Compliance no Cloud Manager" se ainda não houver uma instância implantada.

Habilite o Cloud Compliance em seus ambientes de trabalho

Clique em **Cloud Compliance**, selecione a guia **Configuration** e ative as verificações de conformidade para ambientes de trabalho específicos.

Garanta o acesso aos volumes

Agora que o Cloud Compliance está ativado, garanta que ele possa acessar volumes.

- A instância de conformidade em nuvem precisa de uma conexão de rede para cada sub-rede Cloud Volumes ONTAP ou sub-rede Azure NetApp Files.
- Os grupos de segurança do Cloud Volumes ONTAP devem permitir conexões de entrada da instância de conformidade com a nuvem.
- As políticas de exportação de volume NFS devem permitir o acesso a partir da instância do Cloud Compliance.
- O Cloud Compliance precisa de credenciais do active Directory para verificar volumes CIFS.

  Clique em **Cloud Compliance** > **Scan Configuration** > **Edit CIFS Credentials** e forneça as credenciais. As credenciais podem ser somente leitura, mas fornecer credenciais de administrador garante que o Cloud Compliance possa ler dados que exigem permissões elevadas.

Configure volumes para digitalizar

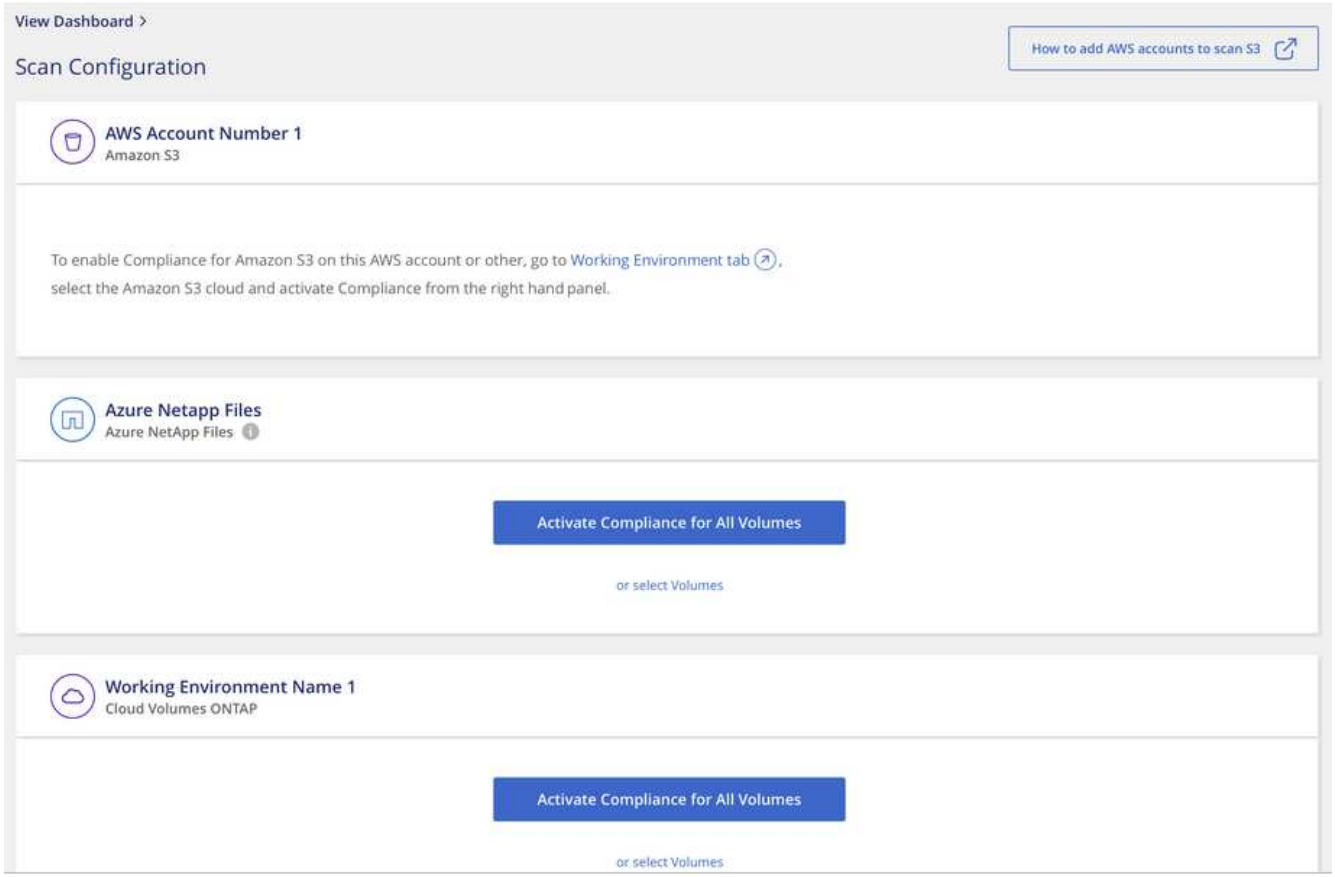
Selecione os volumes que você deseja verificar e o Cloud Compliance começará a digitalizá-los.

Implantando a instância de Cloud Compliance

"Implante o Cloud Compliance no Cloud Manager" se ainda não houver uma instância implantada.

Habilitando o Cloud Compliance em seus ambientes de trabalho

1. Na parte superior do Cloud Manager, clique em **Cloud Compliance** e selecione a guia **Configuration**.



2. Para digitalizar todos os volumes em um ambiente de trabalho, clique em **Ativar conformidade para todos os volumes**.

   Para digitalizar apenas determinados volumes num ambiente de trabalho, clique em **ou selecione volumes** e, em seguida, escolha os volumes que pretende digitalizar.

Ativar e desativar verificações de conformidade em volumesConsulte para obter detalhes.

Resultado

O Cloud Compliance começa a analisar os dados em cada ambiente de trabalho. Os resultados estarão disponíveis no painel de conformidade assim que o Cloud Compliance concluir as verificações iniciais. O tempo que leva depende da quantidade de dados - pode ser de alguns minutos ou horas.

Verificar se o Cloud Compliance tem acesso a volumes

Verifique se o Cloud Compliance pode acessar volumes verificando suas políticas de rede, grupos de segurança e exportação. Você precisará fornecer as credenciais CIFS do Cloud Compliance para acessar os volumes CIFS.

Passos

1. Verifique se há uma conexão de rede entre a instância do Cloud Compliance e cada rede que inclua volumes para Cloud Volumes ONTAP ou Azure NetApp Files.

   Para o Azure NetApp Files, o Cloud Compliance só pode verificar volumes que estejam na mesma região que o Cloud Manager.

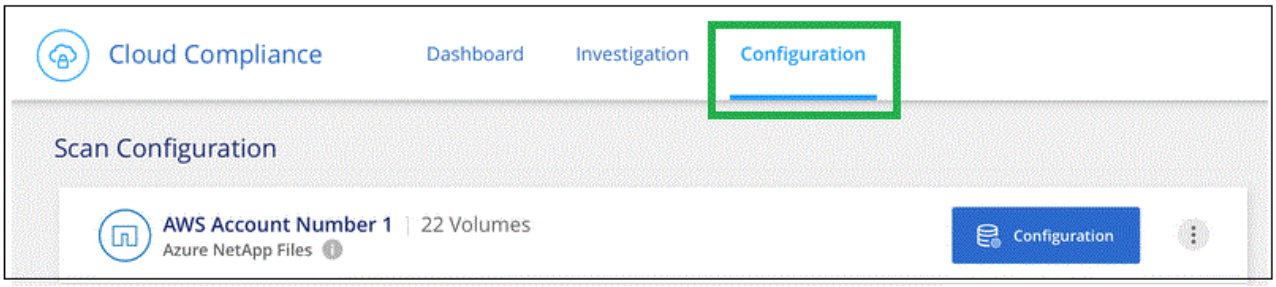
2. Certifique-se de que o grupo de segurança do Cloud Volumes ONTAP permita o tráfego de entrada da instância de conformidade com a nuvem.

   Você pode abrir o grupo de segurança para o tráfego a partir do endereço IP da instância de conformidade na nuvem ou abrir o grupo de segurança para todo o tráfego dentro da rede virtual.

3. Certifique-se de que as políticas de exportação de volume NFS incluam o endereço IP da instância de Cloud Compliance para que ela possa acessar os dados em cada volume.
4. Se você usar CIFS, forneça as credenciais do Cloud Compliance para que ele possa verificar os volumes CIFS.

   a. Na parte superior do Cloud Manager, clique em **Cloud Compliance**.

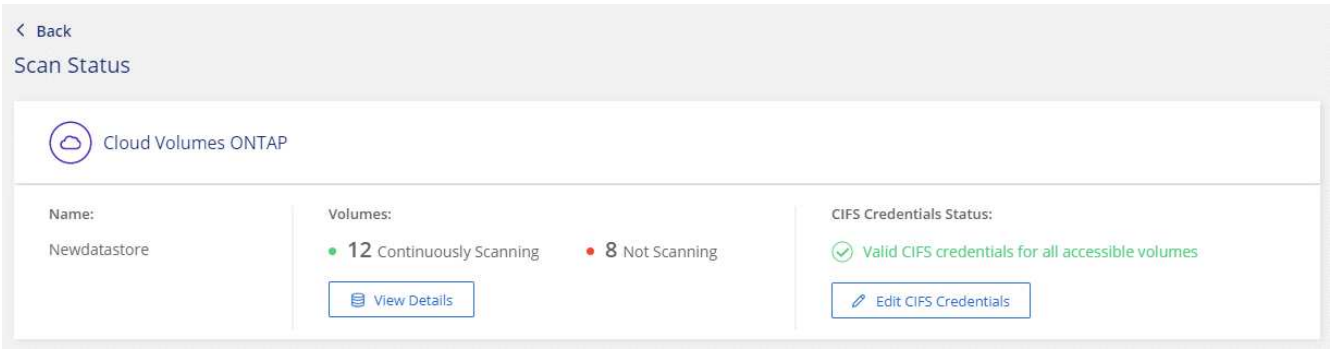
   b. Clique na guia **Configuração**.



   c. Para cada ambiente de trabalho, clique em **Editar credenciais CIFS** e insira o nome de usuário e a senha que o Cloud Compliance precisa para acessar volumes CIFS no sistema.

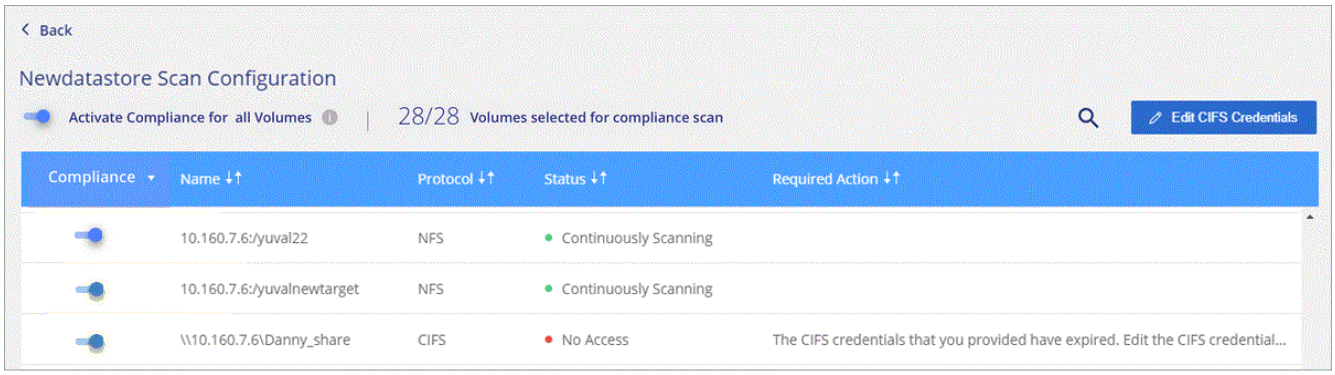
      As credenciais podem ser somente leitura, mas fornecer credenciais de administrador garante que o Cloud Compliance possa ler todos os dados que exigem permissões elevadas. As credenciais são armazenadas na instância do Cloud Compliance.

      Depois de inserir as credenciais, você verá uma mensagem informando que todos os volumes CIFS foram autenticados com êxito.



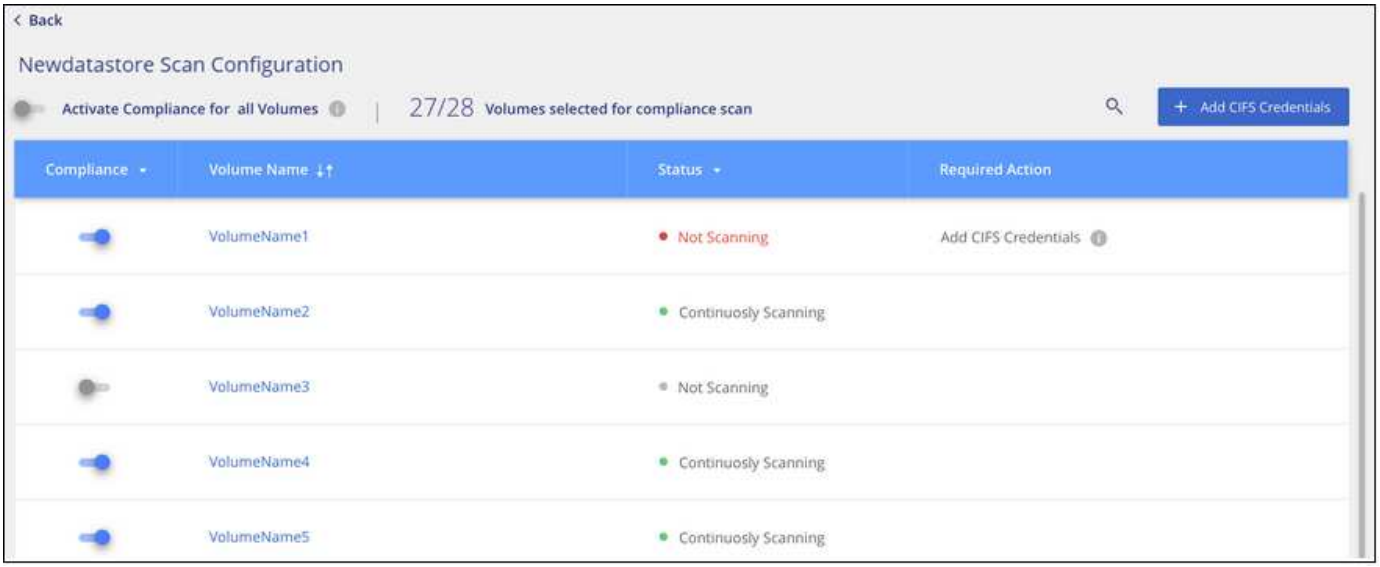
5. Na página *Scan Configuration*, clique em **View Details** (Ver detalhes) para rever o estado de cada volume CIFS e NFS e corrigir quaisquer erros.

   Por exemplo, a imagem a seguir mostra três volumes; um dos quais o Cloud Compliance não pode ser verificado devido a problemas de conetividade de rede entre a instância do Cloud Compliance e o volume.



Ativar e desativar verificações de conformidade em volumes

Pode parar ou iniciar a digitalização de volumes num ambiente de trabalho a qualquer momento a partir da página Configuração de digitalização. Recomendamos que você digitalize todos os volumes.



Para:	Faça isso:
Desativar a procura de um volume	Mova o controle deslizante de volume para a esquerda
Desative a digitalização de todos os volumes	Mova o controle deslizante **Ativar conformidade para todos os volumes** para a esquerda
Ativar a digitalização de um volume	Mova o controle deslizante de volume para a direita
Ative a digitalização de todos os volumes	Mova o controle deslizante **Ativar conformidade para todos os volumes** para a direita

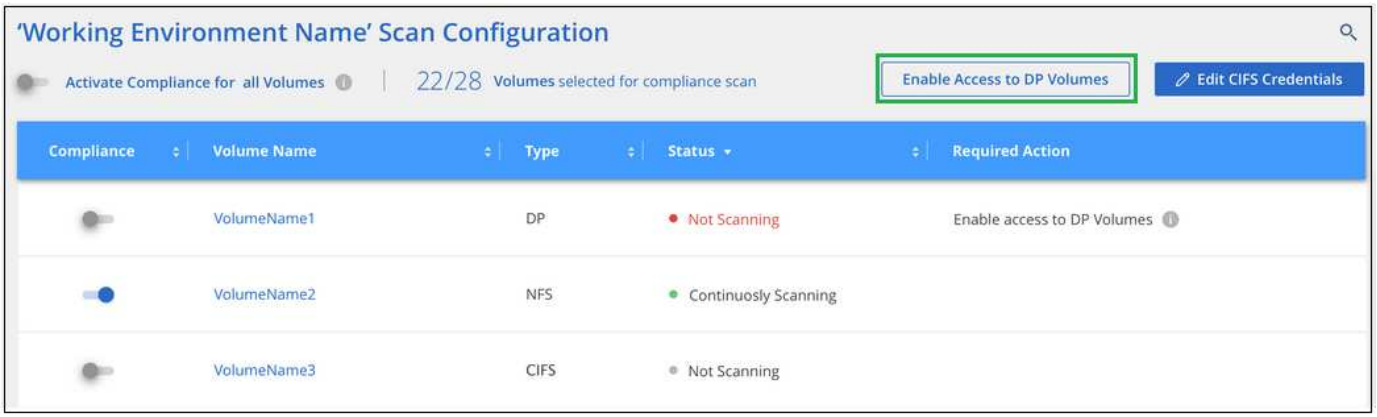
Os novos volumes adicionados ao ambiente de trabalho são automaticamente verificados somente quando a configuração **Ativar conformidade para todos os volumes** estiver ativada. Quando esta definição estiver desativada, terá de ativar a digitalização em cada novo volume criado no ambiente de trabalho.

Digitalização de volumes de proteção de dados

Por padrão, os volumes de proteção de dados (DP) não são verificados porque não são expostos externamente e o Cloud Compliance não pode acessá-los. Esses volumes geralmente são os volumes de

destino para operações do SnapMirror a partir de um cluster do ONTAP no local.

Inicialmente, a lista de volumes do Cloud Compliance identifica esses volumes como *Type* **DP** com o *Status* **Not Scanning** e a *Required Action* **Enable Access to DP volumes**.



Passos

Se você quiser analisar esses volumes de proteção de dados:

1. Clique no botão **Ativar acesso aos volumes DP** na parte superior da página.
2. Ative cada volume DP que você deseja digitalizar ou use o controle **Ativar conformidade para todos os volumes** para habilitar todos os volumes, incluindo todos os volumes DP.

Uma vez ativado, o Cloud Compliance cria um compartilhamento NFS a partir de cada volume DP ativado para conformidade, para que possa ser verificado. As políticas de exportação de compartilhamento só permitem acesso a partir da instância de conformidade com a nuvem.

Apenas os volumes criados inicialmente como volumes NFS no sistema ONTAP de origem são mostrados na lista de volumes. Os volumes de origem criados inicialmente como CIFS não aparecem no Cloud Compliance.

Introdução ao Cloud Compliance para Amazon S3

O Cloud Compliance pode verificar seus buckets do Amazon S3 para identificar os dados pessoais e confidenciais que residem no storage de objetos do S3. O Cloud Compliance pode verificar qualquer bucket da conta, independentemente de ter sido criado para uma solução da NetApp.

Início rápido

Comece rapidamente seguindo estas etapas ou role para baixo até as seções restantes para obter detalhes completos.

Configure os requisitos do S3 em seu ambiente de nuvem

Garanta que seu ambiente de nuvem atenda aos requisitos de conformidade com a nuvem, incluindo a preparação de uma função do IAM e a configuração da conectividade do Cloud Compliance para o S3. Veja a lista completa.

Implante a instância do Cloud Compliance

"Implante o Cloud Compliance no Cloud Manager" se ainda não houver uma instância implantada.

Ative a conformidade no seu ambiente de trabalho S3

Selecione o ambiente de trabalho do Amazon S3, clique em **Ativar conformidade** e selecione uma função do IAM que inclua as permissões necessárias.

Selecione os intervalos para digitalizar

Selecione os buckets que você gostaria de verificar e o Cloud Compliance começará a digitalizá-los.

Rever os pré-requisitos do S3

Os requisitos a seguir são específicos para a digitalização de buckets S3.

Configure uma função do IAM para a instância do Cloud Compliance

O Cloud Compliance precisa de permissões para se conetar aos buckets do S3 na sua conta e verificá-los. Configure uma função do IAM que inclua as permissões listadas abaixo. O Cloud Manager solicita que você selecione uma função do IAM ao ativar o Cloud Compliance no ambiente de trabalho do Amazon S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:HeadBucket"
          ],
          "Resource": "*"
      },
      {
          "Effect": "Allow",
          "Action": [
              "iam:GetPolicyVersion",
              "iam:GetPolicy",
              "iam:ListAttachedRolePolicies"
          ],
          "Resource": [
              "arn:aws:iam::*:policy/*",
              "arn:aws:iam::*:role/*"
          ]
      }
  ]
}
```

Fornecer conectividade do Cloud Compliance para o Amazon S3

O Cloud Compliance precisa de uma conexão com o Amazon S3. A melhor maneira de fornecer essa conexão é por meio de um VPC Endpoint ao serviço S3. Para obter instruções, "Documentação da AWS: Criando um endpoint do Gateway" consulte .

Quando você criar o VPC Endpoint, certifique-se de selecionar a região, VPC e tabela de rotas que corresponde à instância do Cloud Compliance. Você também deve modificar o grupo de segurança para adicionar uma regra HTTPS de saída que permita o tráfego para o endpoint S3. Caso contrário, o Cloud Compliance não pode se conetar ao serviço S3.

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

Uma alternativa é fornecer a conexão usando um NAT Gateway.

Você não pode usar um proxy para chegar ao S3 pela internet.

Implantando a instância de Cloud Compliance

"Implante o Cloud Compliance no Cloud Manager" se ainda não houver uma instância implantada.

Você precisa implantar a instância em um AWS Connector para que o Cloud Manager descubra automaticamente os buckets do S3 nessa conta da AWS e os exiba em um ambiente de trabalho do Amazon S3.

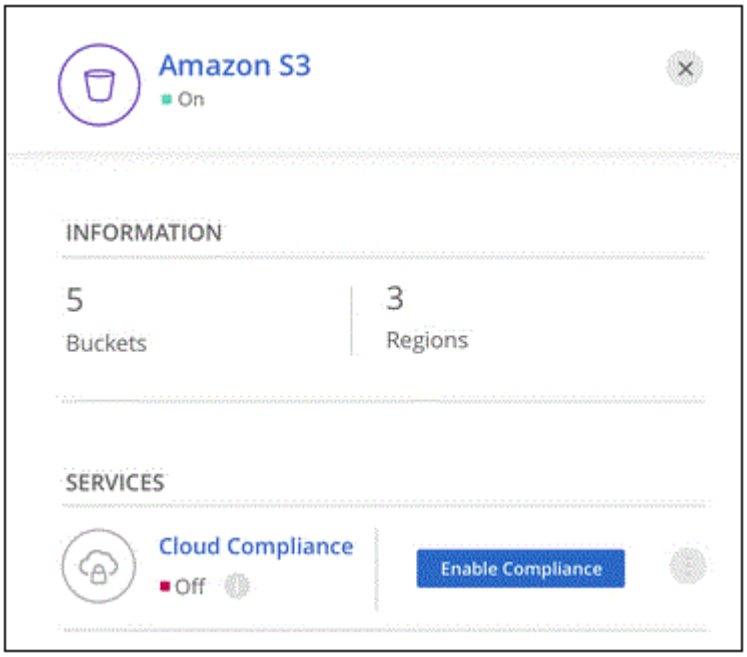
Ativar a conformidade no seu ambiente de trabalho S3

Ative o Cloud Compliance no Amazon S3 depois de verificar os pré-requisitos.

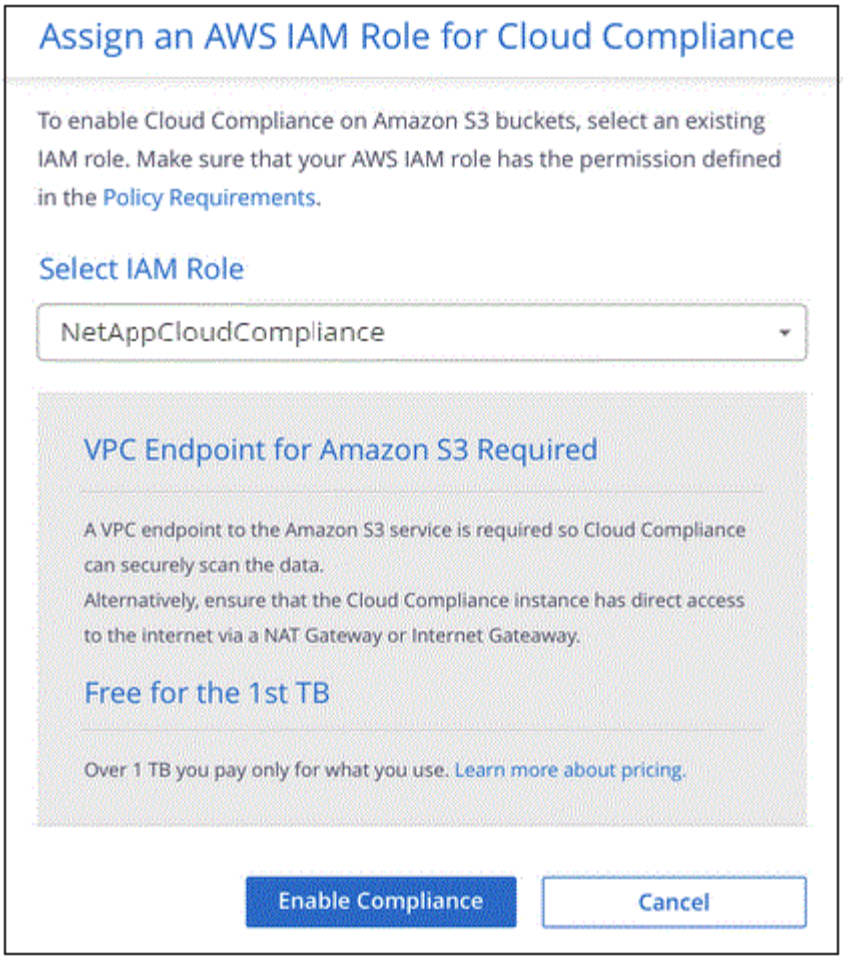
Passos

1. Na parte superior do Cloud Manager, clique em **ambientes de trabalho**.
2. Selecione o ambiente de trabalho do Amazon S3.

3. No painel à direita, clique em **Ativar conformidade**.



4. Quando solicitado, atribua uma função do IAM à instância do Cloud Compliance que tem as permissões necessáriaso .



5. Clique em **Ativar conformidade**.

Você também pode habilitar verificações de conformidade para um ambiente de trabalho na página Configuração de digitalização clicando no botão e selecionando **Ativar conformidade**.

Resultado

O Cloud Manager atribui a função IAM à instância.

Ativar e desativar verificações de conformidade em buckets do S3

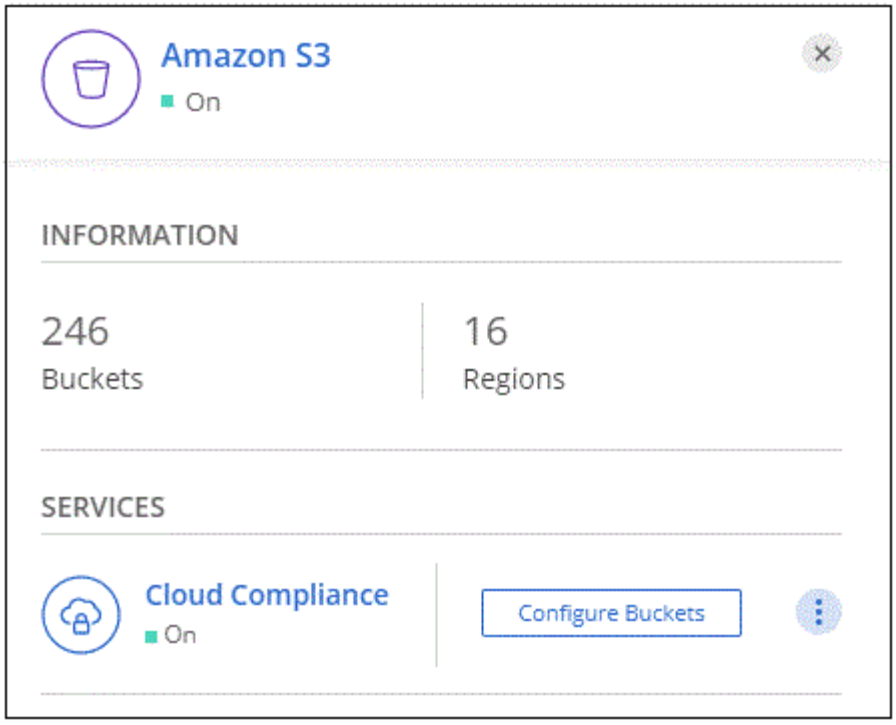
Depois que o Cloud Manager ativar o Cloud Compliance no Amazon S3, a próxima etapa é configurar os buckets que você deseja analisar.

Quando o Cloud Manager está em execução na conta da AWS que tem os buckets do S3 que você deseja verificar, ele descobre esses buckets e os exibe em um ambiente de trabalho do Amazon S3.

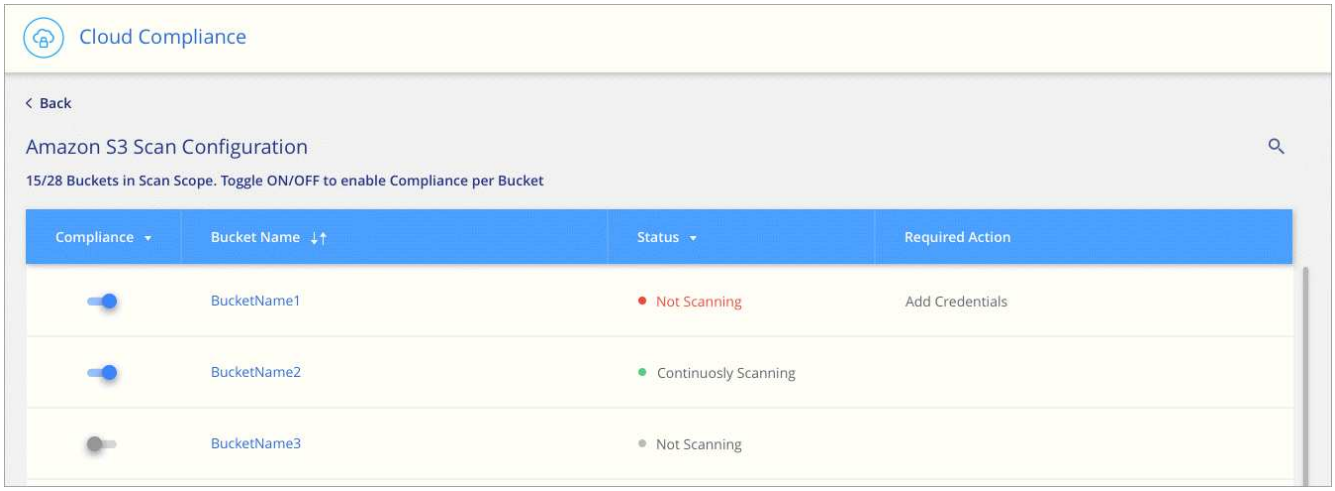
O Cloud Compliance também Examine os buckets do S3 que estão em diferentes contas da AWSpode .

Passos

1. Selecione o ambiente de trabalho do Amazon S3.
2. No painel à direita, clique em **Configurar baldes**.



3. Ative a conformidade nos buckets que você deseja analisar.



Resultado

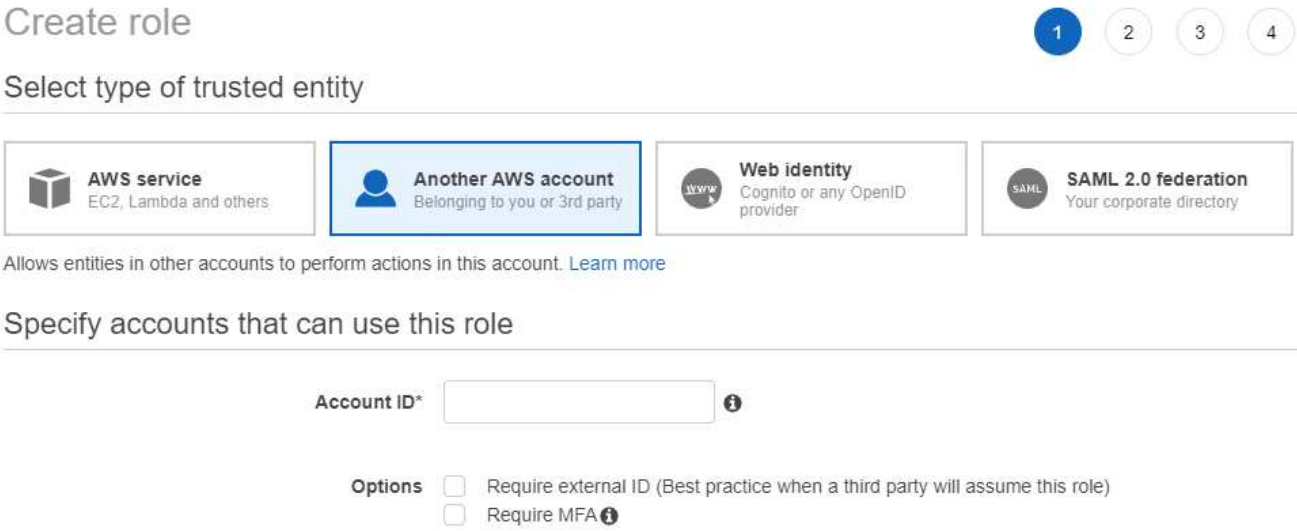
O Cloud Compliance começa a verificar os buckets do S3 ativados. Se houver algum erro, eles aparecerão na coluna Status, juntamente com a ação necessária para corrigir o erro.

Digitalização de buckets a partir de contas adicionais da AWS

Você pode verificar buckets do S3 em uma conta diferente da AWS atribuindo uma função dessa conta para acessar a instância existente do Cloud Compliance.

Passos

1. Vá para a conta AWS de destino onde você deseja analisar buckets do S3 e criar uma função do IAM selecionando **outra conta da AWS**.



Certifique-se de fazer o seguinte:

- Insira o ID da conta onde reside a instância do Cloud Compliance.
- Altere a duração máxima da sessão CLI/API* de 1 hora para 12 horas e salve essa alteração.
- Anexe a política do Cloud Compliance IAM. Certifique-se de que tem as permissões necessárias.

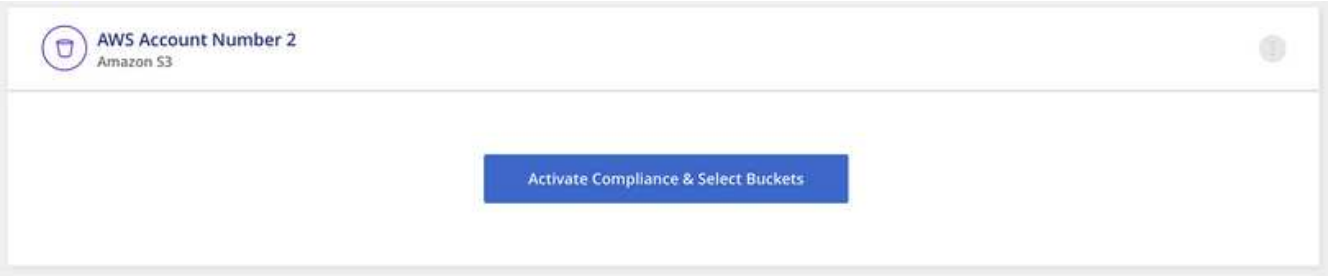
```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:HeadBucket"
          ],
          "Resource": "*"
      },
  ]
}
```

2. Vá para a conta da AWS de origem onde reside a instância do Cloud Compliance e selecione a função do IAM anexada à instância.
   a. Altere a duração máxima da sessão CLI/API* de 1 hora para 12 horas e salve essa alteração.
   b. Clique em **Anexar políticas** e, em seguida, clique em **criar política**.
   c. Crie uma política que inclua a ação "sts:AssumeRole" e o ARN da função que você criou na conta de destino.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::<ADDITIONAL-ACCOUNT-
ID>:role/<ADDITIONAL_ROLE_NAME>"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies"
            ],
            "Resource": [
                "arn:aws:iam::*:policy/*",
                "arn:aws:iam::*:role/*"
            ]
        }
    ]
}
```

A conta de perfil de instância do Cloud Compliance agora tem acesso à conta AWS adicional.

3. Vá para a página **Configuração de digitalização do Amazon S3** e a nova conta da AWS será exibida. Observe que pode levar alguns minutos para que o Cloud Compliance sincronize o ambiente de trabalho da nova conta e mostre essas informações.



4. Clique em **Activate Compliance & Select Buckets** (Ativar conformidade e Selecionar baldes*) e selecione os baldes que pretende digitalizar.

Resultado

O Cloud Compliance começa a verificar os novos buckets do S3 ativados.

Digitalização de esquemas de banco de dados

Conclua algumas etapas para começar a verificar seus esquemas de banco de dados

com o Cloud Compliance.

Início rápido

Comece rapidamente seguindo estas etapas ou role para baixo até as seções restantes para obter detalhes completos.

 **Rever pré-requisitos da base de dados**

Certifique-se de que a sua base de dados é suportada e de que tem as informações necessárias para se ligar à base de dados.

 **Implante a instância do Cloud Compliance**

"Implante o Cloud Compliance no Cloud Manager" se ainda não houver uma instância implantada.

 **Adicione o servidor de banco de dados**

Adicione o servidor de banco de dados que você deseja acessar.

 **Selecione os esquemas**

Selecione os esquemas que pretende digitalizar.

Rever pré-requisitos

Revise os pré-requisitos a seguir para garantir que você tenha uma configuração compatível antes de ativar o Cloud Compliance.

Bancos de dados compatíveis

O Cloud Compliance pode verificar esquemas dos seguintes bancos de dados:

- MongoDB
- Oracle
- PostgreSQL
- SAP HANA
- SQL Server (MSSQL)

 O recurso de coleta de estatísticas **deve estar ativado** no banco de dados.

Requisitos de banco de dados

Qualquer banco de dados com conetividade com a instância de conformidade com a nuvem pode ser verificado, independentemente de onde esteja hospedado. Você só precisa das seguintes informações para se conetar ao banco de dados:

- Endereço IP ou nome do host
- Porta
- Nome do serviço (somente para acessar bancos de dados Oracle)
- Credenciais que permitem acesso de leitura aos esquemas

  Ao escolher um nome de usuário e senha, é importante escolher um que tenha permissões de leitura completas para todos os esquemas e tabelas que você deseja digitalizar. Recomendamos que você crie um usuário dedicado para o sistema de conformidade com a nuvem com todas as permissões necessárias.

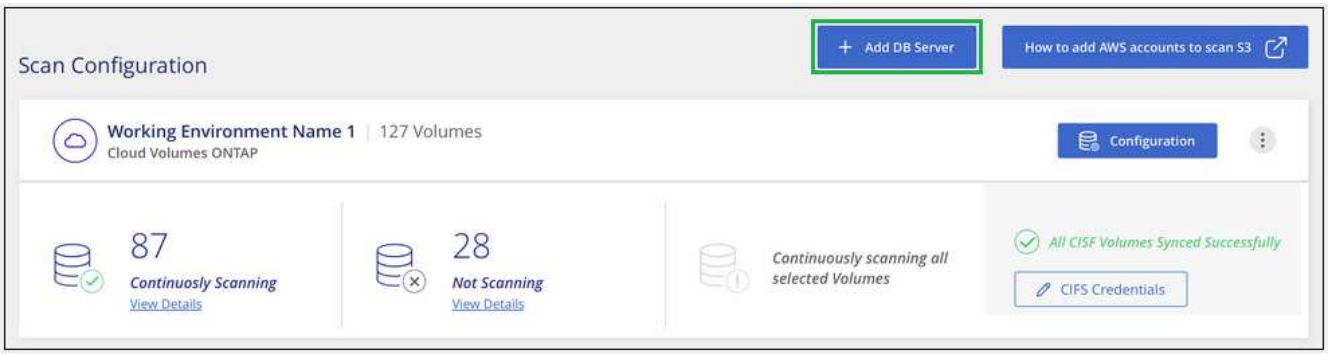
Observação: para MongoDB, é necessária uma função de administração somente leitura.

Adicionando o servidor de banco de dados

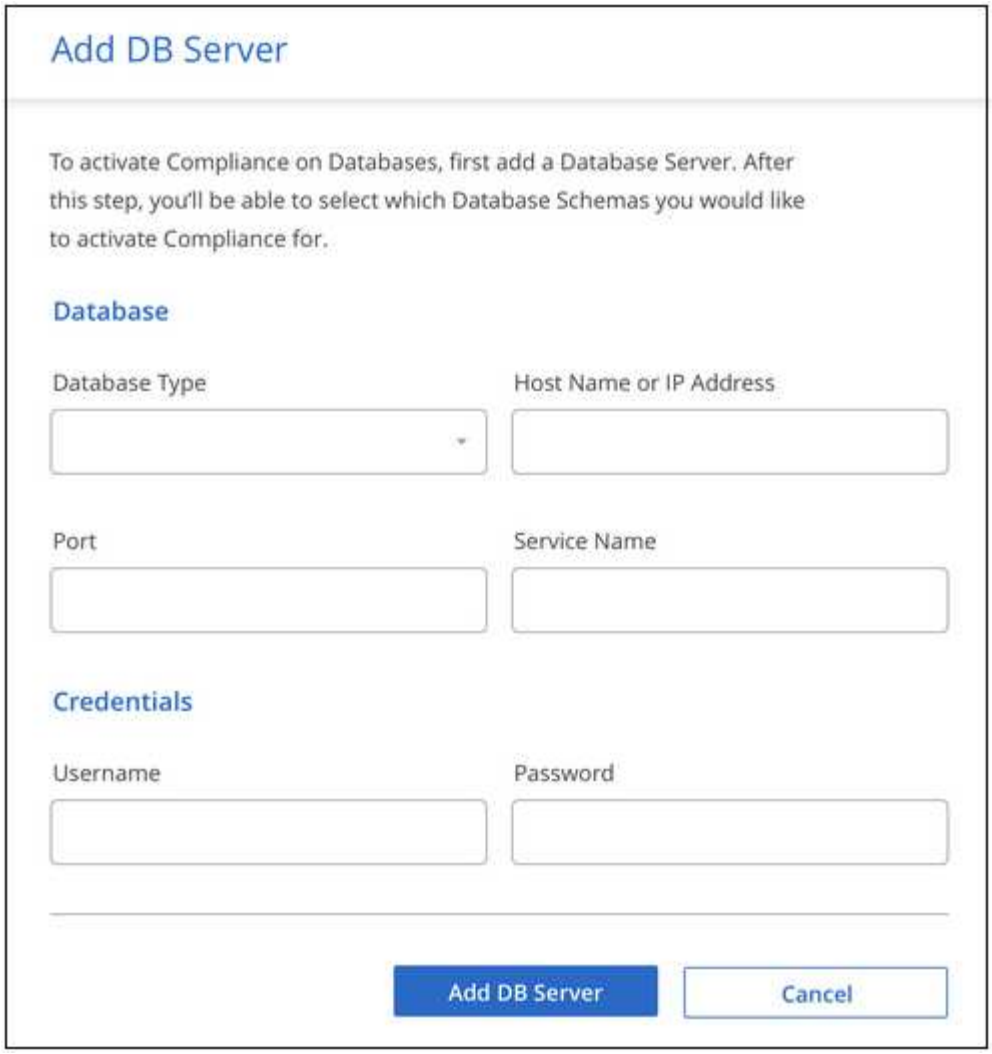
Você deve ter "Já implantou uma instância do Cloud Compliance no Cloud Manager".

Adicione o servidor de banco de dados onde os esquemas residem.

1. Na página *Scan Configuration*, clique no botão **Add DB Server**.



2. Introduza as informações necessárias para identificar o servidor da base de dados.
   a. Selecione o tipo de banco de dados.
   b. Insira a porta e o nome do host ou endereço IP para se conetar ao banco de dados.
   c. Para bancos de dados Oracle, insira o nome do serviço.
   d. Insira as credenciais para que o Cloud Compliance possa acessar o servidor.
   e. Clique em **Add DB Server**.



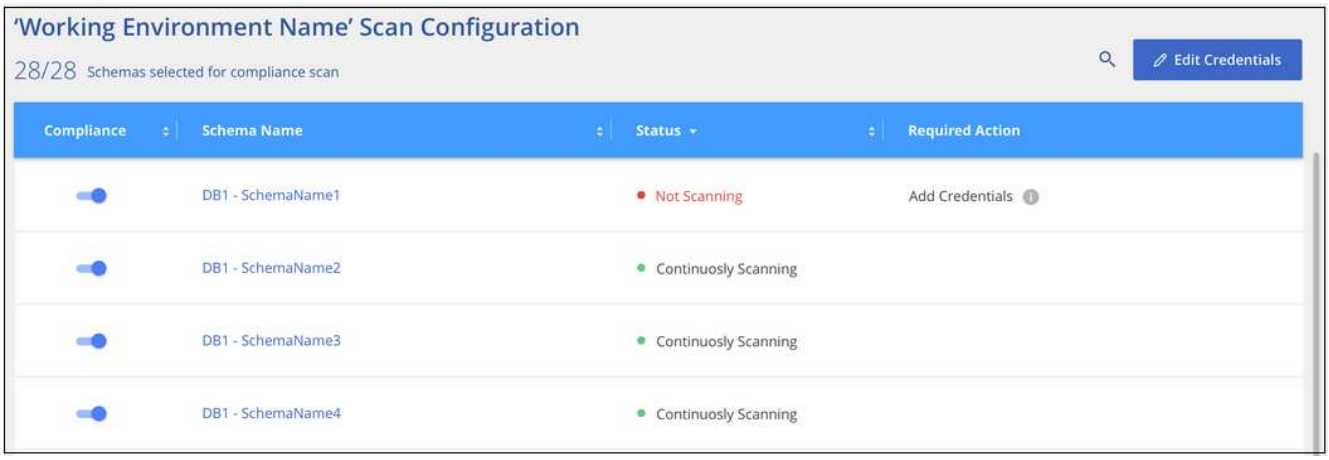
O banco de dados é adicionado à lista de diretórios de trabalho.

Ativar e desativar verificações de conformidade em esquemas de banco de dados

Você pode parar ou começar a digitalizar esquemas a qualquer momento.

1. Na página *Scan Configuration*, clique no botão **Configuration** do banco de dados que deseja configurar.

2. Selecione os esquemas que deseja digitalizar movendo o controle deslizante para a direita.



Resultado

O Cloud Compliance começa a verificar os esquemas de banco de dados que você ativou. Se houver algum erro, eles aparecerão na coluna Status, juntamente com a ação necessária para corrigir o erro.

Removendo um banco de dados do Cloud Manager

Se você não quiser mais digitalizar um determinado banco de dados, você pode excluí-lo da interface do Cloud Manager e parar todas as verificações.

Na página *Scan Configuration*, clique no botão na linha do banco de dados e clique em **Remove DB Server**.

Verificação de dados do ONTAP no local com o Cloud Compliance usando o SnapMirror

Você pode digitalizar seus dados ONTAP locais com o Cloud Compliance replicando os dados NFS ou CIFS on-premises em um ambiente operacional da Cloud Volumes ONTAP e habilitando a conformidade. A digitalização dos dados diretamente de um ambiente de trabalho ONTAP local não é suportada.

Você deve ter "Já implantou uma instância do Cloud Compliance no Cloud Manager".

Passos

1. No Cloud Manager, crie uma relação de SnapMirror entre o cluster ONTAP no local e o Cloud Volumes ONTAP.
   a. "Descubra o cluster no local no Cloud Manager".
   b. "Crie uma replicação do SnapMirror entre o cluster do ONTAP no local e o Cloud Volumes ONTAP a

partir do Cloud Manager".

2. Para volumes DP criados a partir de volumes de origem SMB, a partir da CLI do ONTAP, configure os volumes de destino SMB para acesso aos dados. (Isso não é necessário para volumes NFS porque o acesso aos dados é habilitado automaticamente pelo Cloud Compliance.)
   a. "Crie um compartilhamento SMB no volume de destino".
   b. "Aplique as ACLs apropriadas ao compartilhamento SMB no volume de destino".
3. No Cloud Manager, ative o Cloud Compliance no ambiente de trabalho do Cloud Volumes ONTAP que contém os dados do SnapMirror:
   a. Clique em **ambientes de trabalho**.
   b. Selecione o ambiente de trabalho que contém os dados do SnapMirror e clique em **Ativar conformidade**.

      "Clique aqui se precisar de ajuda para ativar o Cloud Compliance em um sistema Cloud Volumes ONTAP".

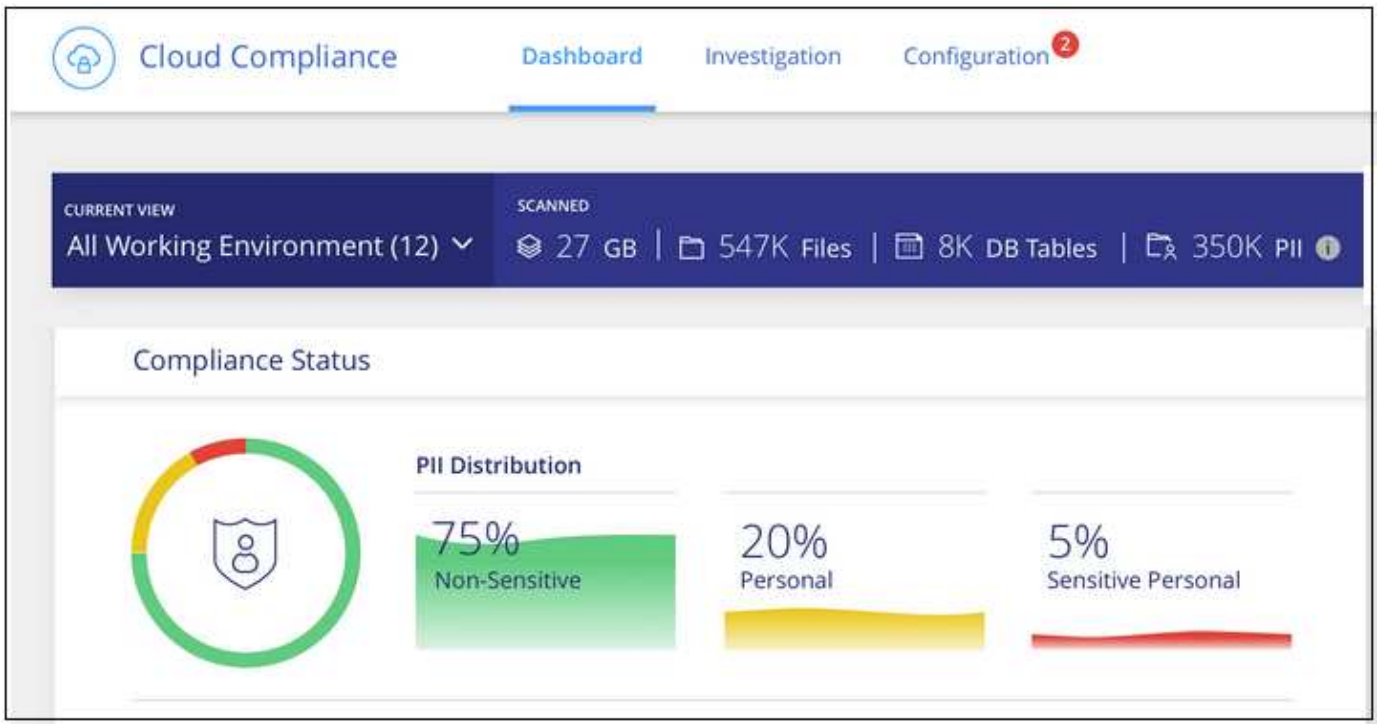
   c. Clique no botão **Ativar acesso aos volumes DP** na parte superior da página *Configuração de digitalização*.
   d. Ative cada volume DP que você deseja digitalizar ou use o controle **Ativar conformidade para todos os volumes** para habilitar todos os volumes, incluindo todos os volumes DP.

Consulte "Digitalização de volumes de proteção de dados" para obter mais informações sobre a digitalização de volumes DP.

Ter visibilidade e controle de dados privados

Obtenha controle de seus dados privados visualizando detalhes sobre os dados pessoais e dados pessoais confidenciais em sua organização. Você também pode ter visibilidade revisando as categorias e tipos de arquivo que o Cloud Compliance encontrou nos seus dados.

Por padrão, o dashboard do Cloud Compliance exibe dados de conformidade para todos os ambientes de trabalho e bancos de dados.



Se desejar ver os dados apenas para alguns dos ambientes de trabalhoselecione esses ambientes de trabalho, .

Dados pessoais

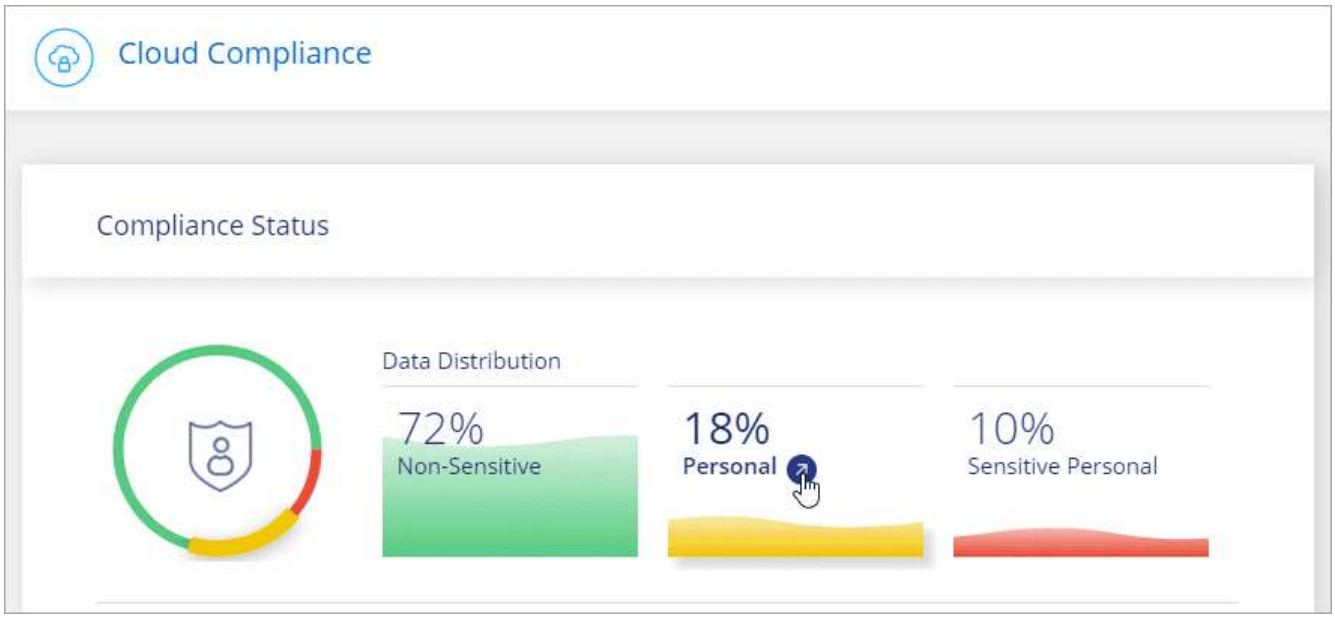
O Cloud Compliance identifica automaticamente palavras, strings e padrões específicos (Regex) dentro dos dados. Por exemplo, informações de identificação pessoal (PII), números de cartão de crédito, números de segurança social, números de conta bancária e muito mais. Veja a lista completa.

Para alguns tipos de dados pessoais, o Cloud Compliance usa *validação de proximidade* para validar suas descobertas. A validação ocorre procurando uma ou mais palavras-chave predefinidas próximas aos dados pessoais encontrados. Por exemplo, o Cloud Compliance identifica um SSN (número de segurança social) dos EUA como um SSN se ele vir uma palavra de proximidade ao lado dele - por exemplo, *SSN* ou *segurança social*. A lista abaixo Mostra quando o Cloud Compliance usa validação de proximidade.

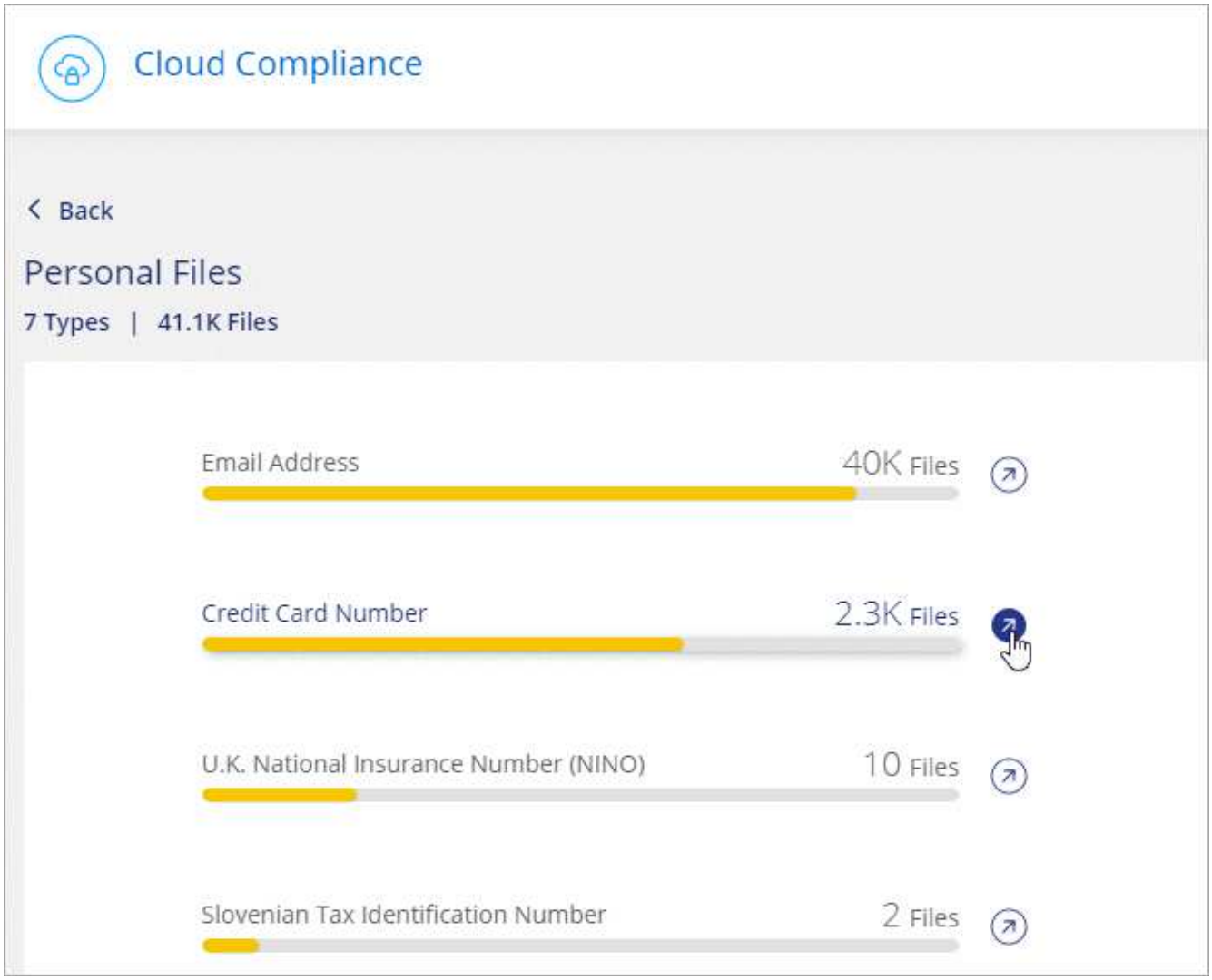
Visualização de arquivos que contêm dados pessoais

Passos

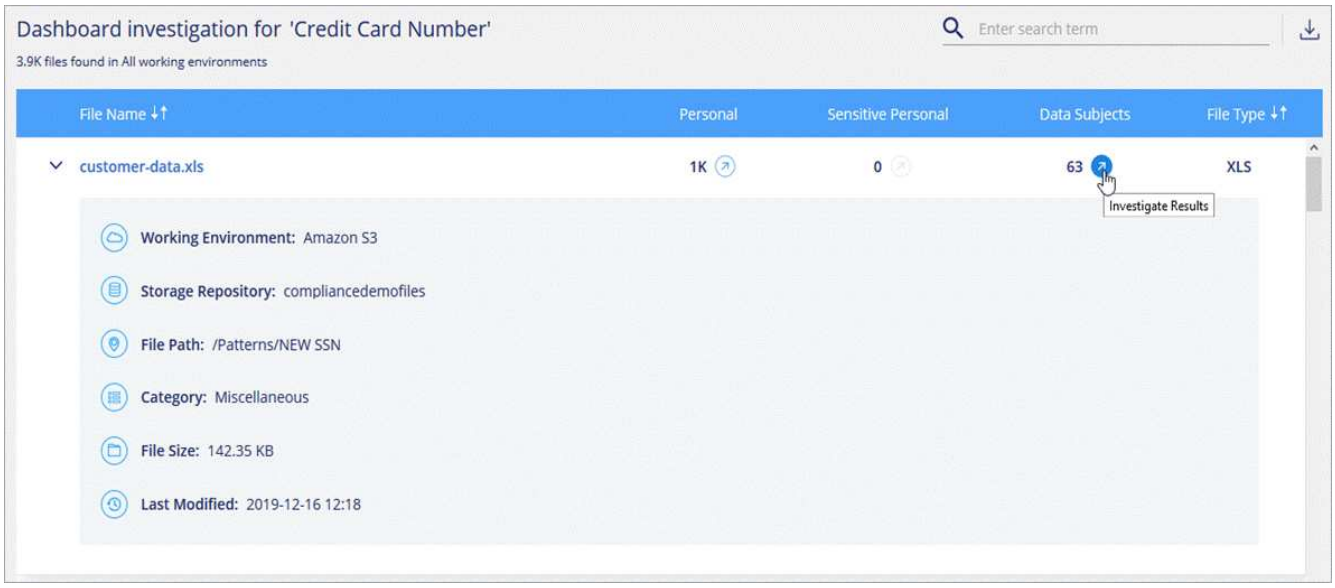
1. Na parte superior do Cloud Manager, clique em **Cloud Compliance** e clique na guia **Dashboard**.
2. Para investigar os detalhes de todos os dados pessoais, clique no ícone ao lado da porcentagem de dados pessoais.



3. Para investigar os detalhes de um tipo específico de dados pessoais, clique em **Exibir todos** e, em seguida, clique no ícone **investigar resultados** para um tipo específico de dados pessoais.

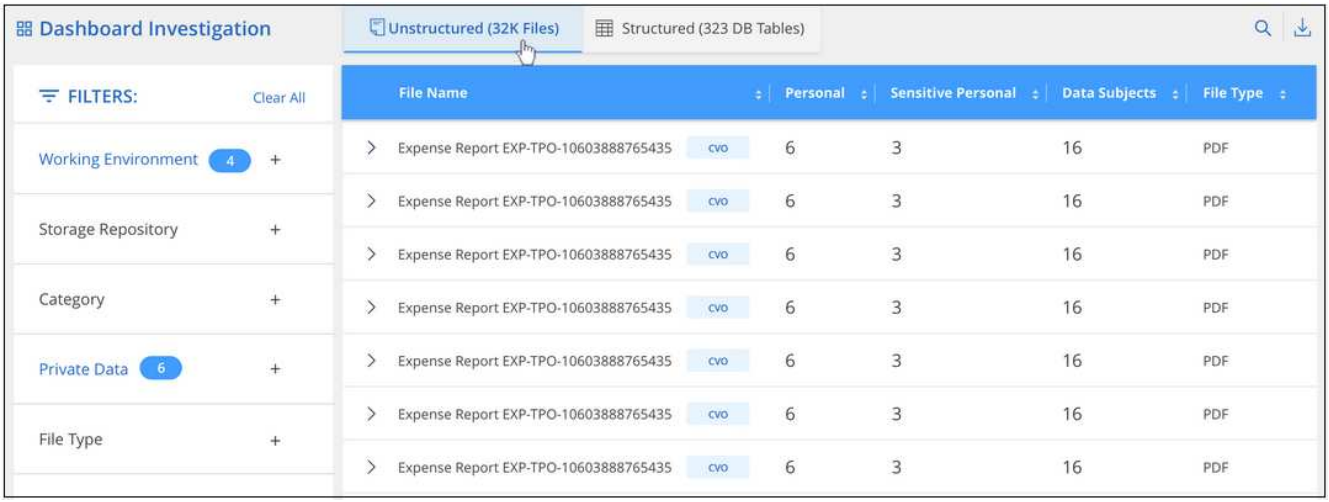


4. Investigue os dados pesquisando, classificando, expandindo detalhes para um arquivo específico, clicando em **investigar resultados** para ver informações mascaradas ou baixando a lista de arquivos.



5. Você também pode filtrar o conteúdo da página de investigação para exibir apenas os resultados que deseja ver. As guias de nível superior permitem exibir dados de arquivos (dados não estruturados) ou de bancos de dados (dados estruturados).

   Em seguida, você tem filtros para ambiente de trabalho, repositório de armazenamento, categoria, dados privados, tipo de arquivo, data da última modificação e se as permissões do objeto S3 estão abertas ao acesso público.



Tipos de dados pessoais

Os dados pessoais encontrados nos arquivos podem ser dados pessoais gerais ou identificadores nacionais. A terceira coluna identifica se o Cloud Compliance usa validação de proximidade para validar suas descobertas para o identificador.

Tipo	Identificador	Validação de proximidade?
Geral	Endereço de e-mail	Não
	Número do cartão de crédito	Não
	Número IBAN (número de conta bancária internacional)	Não

Tipo	Identificador	Validação de proximidade?
Identificadores nacionais	ID belga (Numero National)	Sim
	Identidade Brasileira (CPF)	Sim
	ID búlgaro (UCN)	Sim
	Licença de motorista da Califórnia	Sim
	ID croata (OIB)	Sim
	Número de identificação fiscal do Chipre (TIC)	Sim
	Código checo/eslovaco	Sim
	ID dinamarquesa (CPR)	Sim
	ID holandesa (BSN)	Sim
	ID da Estónia	Sim
	ID finlandês (HETU)	Sim
	Número de identificação fiscal Francês (SPI)	Sim
	Número de identificação fiscal Alemão (Steuerliche Identifikationsrommer)	Sim
	ID grega	Sim
	Número de identificação fiscal húngaro	Sim
	ID irlandesa (PPS)	Sim
	ID israelense	Sim
	Número de identificação fiscal italiano	Sim
	ID letão	Sim
	ID lituano	Sim
	ID Luxemburgo	Sim
	ID maltês	Sim
	ID polaco (PESEL)	Sim
	Número de identificação fiscal Português (NIF)	Sim
	Identificação romena (CNP)	Sim
	Slovenian ID (EMSO)	Sim
	ID sul-africana	Sim
	Número de identificação fiscal espanhol	Sim
	ID sueco	Sim
	ID DO REINO UNIDO (NINO)	Sim
	Número da Segurança Social dos EUA (SSN)	Sim

Dados pessoais confidenciais

O Cloud Compliance identifica automaticamente tipos especiais de informações pessoais confidenciais, conforme definido por regulamentos de privacidade, "artigos 9.º e 10.º do RGPD" como . Por exemplo, informações sobre a saúde de uma pessoa, origem étnica ou orientação sexual. Veja a lista completa.

O Cloud Compliance usa inteligência artificial (AI), processamento de linguagem natural (NLP), aprendizado de máquina (ML) e computação cognitiva (CC) para entender o significado do conteúdo verificado para extrair entidades e categorizá-lo de acordo.

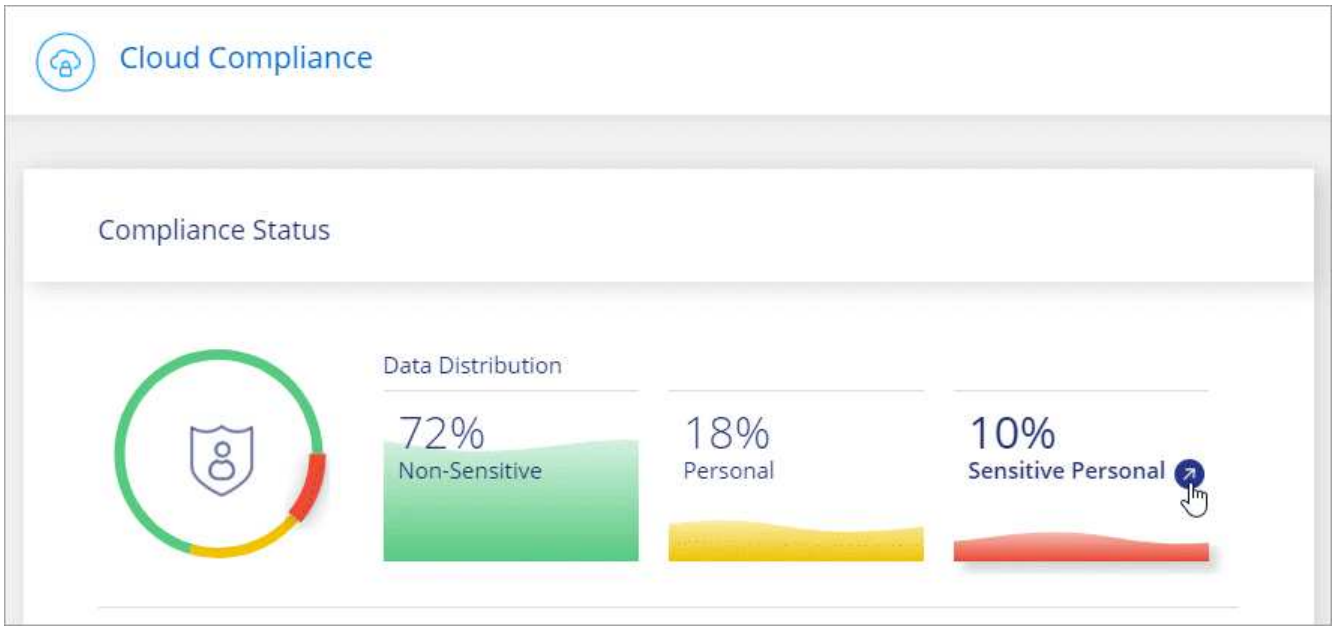
Por exemplo, uma categoria de dados confidenciais do GDPR é a origem étnica. Por causa de suas habilidades de PNL, o Cloud Compliance pode distinguir a diferença entre uma frase que diz "George é mexicano" (indicando dados confidenciais conforme especificado no artigo 9 do GDPR), em comparação com "George está comendo comida mexicana".

Apenas o inglês é suportado durante a digitalização de dados pessoais confidenciais. O suporte para mais idiomas será adicionado mais tarde.

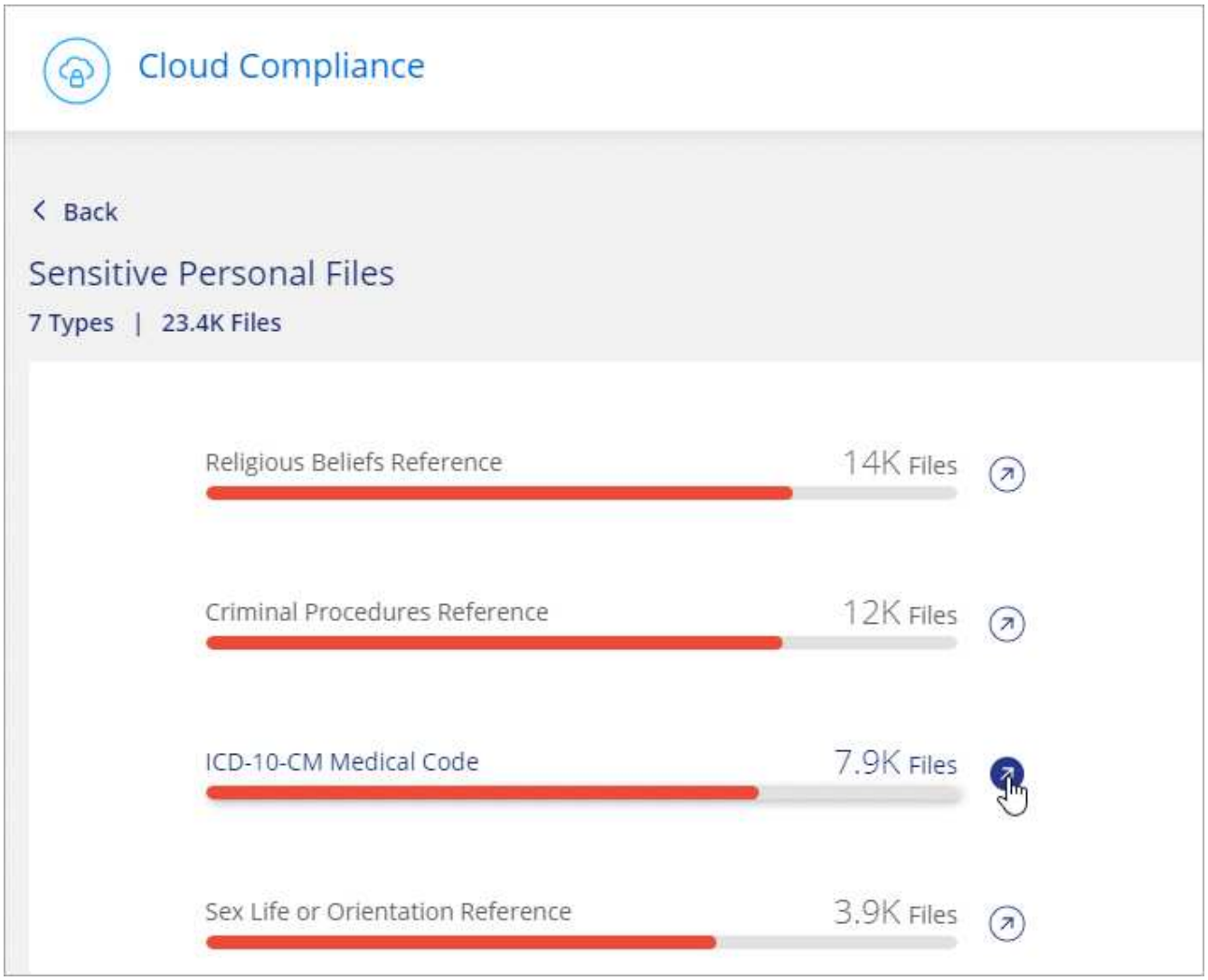
Visualização de arquivos que contêm dados pessoais confidenciais

Passos

1. Na parte superior do Cloud Manager, clique em **Cloud Compliance**.
2. Para investigar os detalhes de todos os dados pessoais confidenciais, clique no ícone ao lado da porcentagem de dados pessoais confidenciais.



3. Para investigar os detalhes de um tipo específico de dados pessoais confidenciais, clique em **Exibir todos** e, em seguida, clique no ícone **investigar resultados** para um tipo específico de dados pessoais confidenciais.



4. Investigue os dados pesquisando, classificando, expandindo detalhes para um arquivo específico, clicando em **investigar resultados** para ver informações mascaradas ou baixando a lista de arquivos.

Tipos de dados pessoais sensíveis

Os dados pessoais confidenciais que o Cloud Compliance pode encontrar nos arquivos incluem o seguinte:

Referência de procedimentos criminais
Dados relativos às condenações e infrações penais de uma pessoa singular.

Etnia de referência
Dados relativos à origem racial ou étnica de uma pessoa singular.

Referência de Saúde
Dados relativos à saúde de uma pessoa singular.

Códigos médicos CID-9-CM
Códigos utilizados na indústria médica e de saúde.

Códigos médicos CID-10-CM
Códigos utilizados na indústria médica e de saúde.

Referência de crenças filosóficas

Dados relativos às crenças filosóficas de uma pessoa natural.

Referência de crenças religiosas

Dados relativos às crenças religiosas de uma pessoa natural.

Vida sexual ou Orientação Referência

Dados relativos à vida sexual ou orientação sexual de uma pessoa natural.

Categorias

O Cloud Compliance pega os dados que digitalizou e os divide em diferentes tipos de categorias. Categorias são tópicos baseados na análise de IA do conteúdo e metadados de cada arquivo. Veja a lista de categorias.

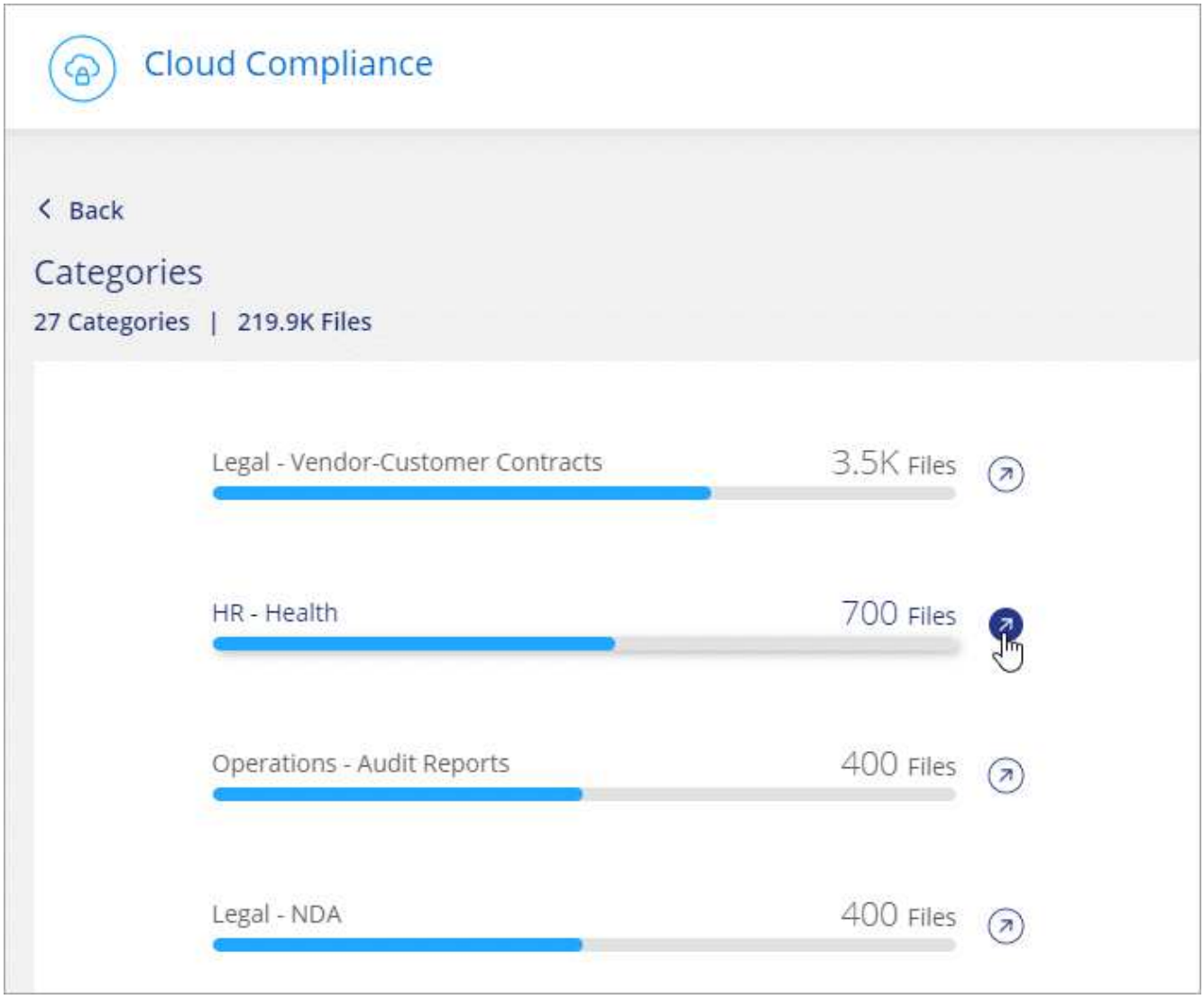
As categorias podem ajudá-lo a entender o que está acontecendo com seus dados, mostrando os tipos de informações que você tem. Por exemplo, uma categoria como currículos ou contratos de funcionários pode incluir dados confidenciais. Ao investigar os resultados, você pode descobrir que os contratos de funcionários são armazenados em um local inseguro. Você pode então corrigir esse problema.

Apenas o inglês é suportado para categorias. O suporte para mais idiomas será adicionado mais tarde.

Visualizar ficheiros por categorias

Passos

1. Na parte superior do Cloud Manager, clique em **Cloud Compliance**.
2. Clique no ícone **investigar resultados** para uma das 4 categorias principais diretamente da tela principal ou clique em **Exibir tudo** e, em seguida, clique no ícone de qualquer uma das categorias.



3. Investigue os dados pesquisando, classificando, expandindo detalhes para um arquivo específico, clicando em **investigar resultados** para ver informações mascaradas ou baixando a lista de arquivos.

Tipos de categorias

O Cloud Compliance categoriza seus dados da seguinte forma:

Finanças

- Balanços
- Ordens compra
- Faturas
- Relatórios trimestrais

HR

- Verificações de fundo
- Planos de compensação
- Contratos de funcionários
- Avaliações de funcionários

- Saúde
- Retoma

Legal
- NDAs
- Contratos fornecedor-cliente

Marketing
- Campanhas
- Conferências

Operações
- Relatórios de auditoria

Vendas
- Ordens vendas

Serviços
- RFI
- RFP
- SOW
- Formação

Suporte
- Reclamações e bilhetes

Categorias de metadados
- Dados da aplicação
- Arquivar ficheiros
- Áudio
- Dados de aplicações empresariais
- Ficheiros CAD
- Código
- Banco de dados e arquivos de índice
- Arquivos de design
- Dados do aplicativo de e-mail
- Executáveis
- Dados de aplicações financeiras
- Dados da aplicação de integridade
- Imagens
- Registos
- Documentos diversos
- Apresentações diversas

- Folhas de cálculo diversas
- Vídeos

Tipos de ficheiros

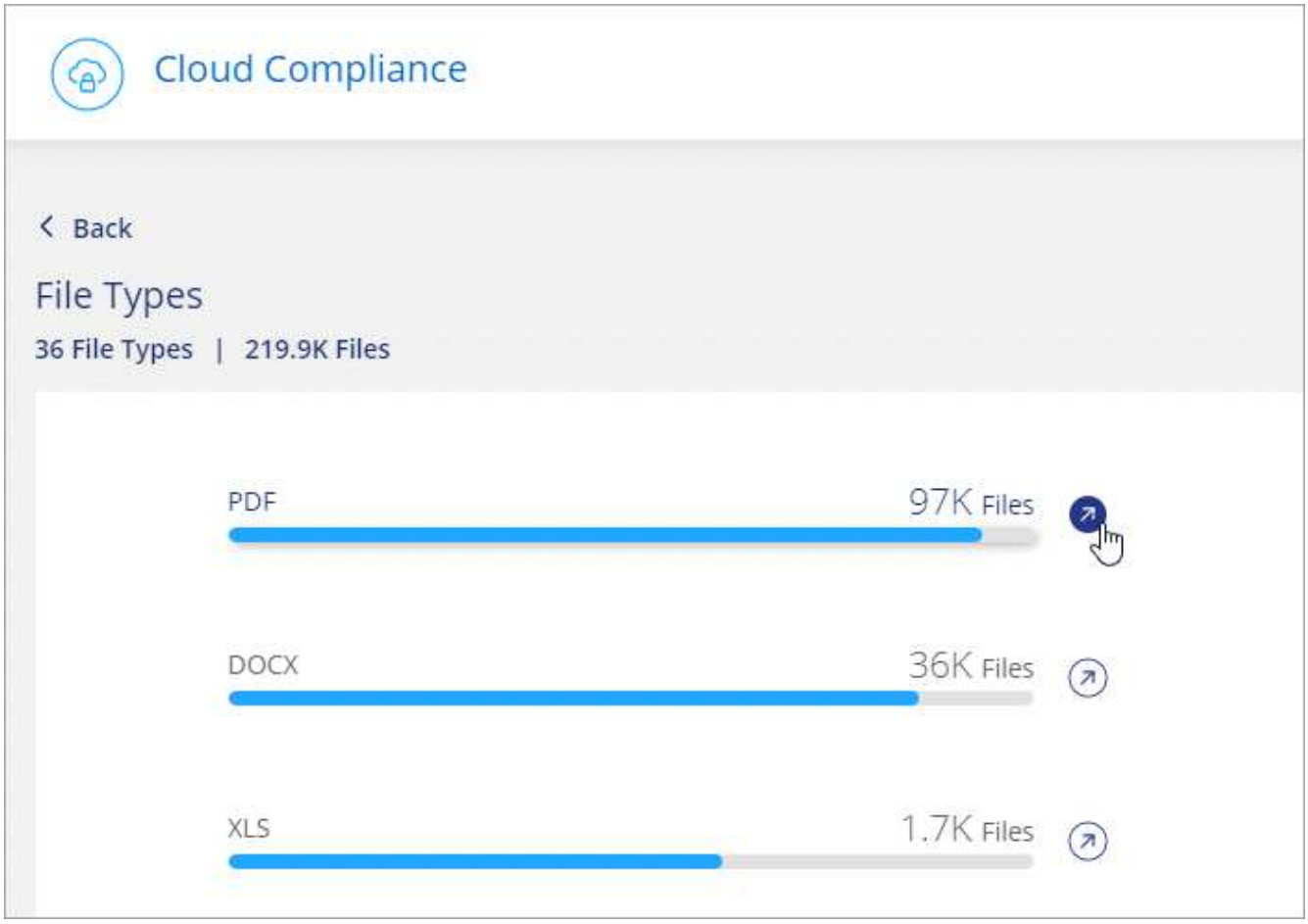
O Cloud Compliance coleta os dados que digitalizou e os divide por tipo de arquivo. A revisão dos tipos de arquivo pode ajudá-lo a controlar seus dados confidenciais, porque você pode descobrir que certos tipos de arquivo não estão armazenados corretamente. Veja a lista de tipos de arquivo.

Por exemplo, você pode estar armazenando arquivos CAD que incluem informações muito confidenciais sobre sua organização. Se eles não estiverem protegidos, você poderá assumir o controle dos dados confidenciais restringindo permissões ou movendo os arquivos para outro local.

Exibindo tipos de arquivo

Passos

1. Na parte superior do Cloud Manager, clique em **Cloud Compliance**.
2. Clique no ícone **investigar resultados** para um dos 4 principais tipos de arquivo diretamente da tela principal ou clique em **Exibir tudo** e, em seguida, clique no ícone para qualquer um dos tipos de arquivo.



3. Investigue os dados pesquisando, classificando, expandindo detalhes para um arquivo específico, clicando em **investigar resultados** para ver informações mascaradas ou baixando a lista de arquivos.

Tipos de arquivos

O Cloud Compliance verifica todos os arquivos para obter informações sobre categorias e metadados e exibe todos os tipos de arquivo na seção tipos de arquivo do painel.

Mas quando o Cloud Compliance deteta informações pessoais identificáveis (PII), ou quando realiza uma pesquisa DSAR, apenas os seguintes formatos de arquivo são suportados: .PDF, .DOCX, .DOC, .PPTX, .XLS, .XLSX, .CSV, .TXT, .RTF e .JSON.

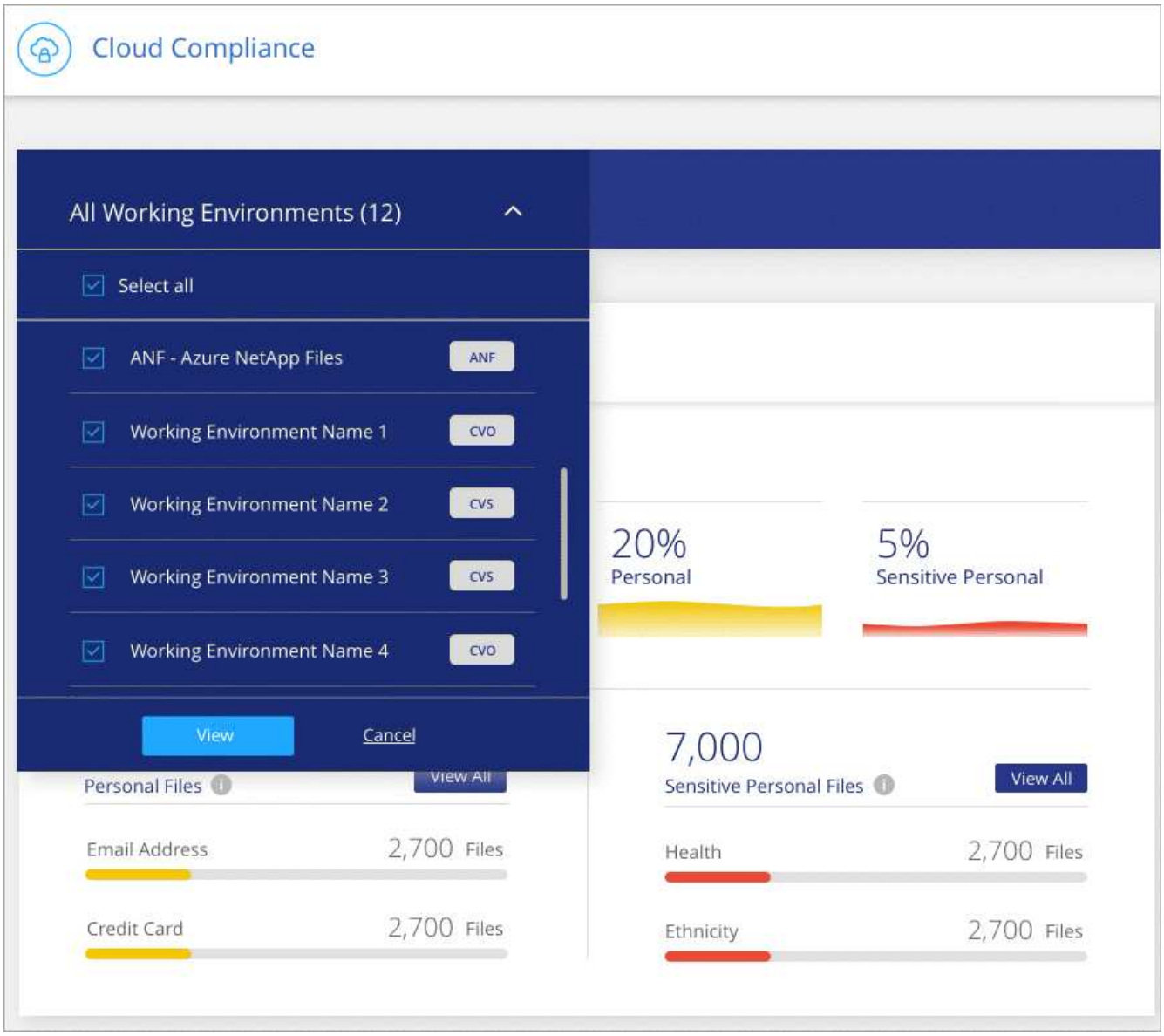
Visualização de dados de ambientes de trabalho específicos

Você pode filtrar o conteúdo do dashboard do Cloud Compliance para ver os dados de conformidade de todos os ambientes de trabalho e bancos de dados ou apenas para ambientes de trabalho específicos.

Quando você filtra o painel, o Cloud Compliance escoa os dados de conformidade e os relatórios apenas para os ambientes de trabalho selecionados.

Passos

1. Clique no menu suspenso filtro, selecione os ambientes de trabalho para os quais deseja exibir dados e clique em **Exibir**.



Precisão das informações encontradas

A NetApp não pode garantir 100% de precisão dos dados pessoais e dados pessoais confidenciais que o Cloud Compliance identifica. Deve sempre validar as informações através da revisão dos dados.

Com base em nossos testes, a tabela abaixo mostra a precisão das informações encontradas pelo Cloud Compliance. Nós quebramos isso por *precisão* e *recall*:

Precisão

A probabilidade de que o Cloud Compliance encontre tenha sido identificado corretamente. Por exemplo, uma taxa de precisão de 90% para dados pessoais significa que 9 em cada 10 arquivos identificados como contendo informações pessoais, contêm informações pessoais. 1 de 10 arquivos seria um falso positivo.

Recolha

A probabilidade de o Cloud Compliance encontrar o que deveria. Por exemplo, uma taxa de recall de 70% para dados pessoais significa que o Cloud Compliance pode identificar 7 em cada 10 arquivos que realmente contêm informações pessoais em sua organização. O Cloud Compliance perderia 30% dos dados, e isso não aparecerá no painel.

O Cloud Compliance está em uma versão de disponibilidade controlada e estamos constantemente melhorando a precisão de nossos resultados. Essas melhorias estarão disponíveis automaticamente em futuras versões do Cloud Compliance.

Tipo	Precisão	Recolha
Dados pessoais - Geral	90%-95%	60%-80%
Dados pessoais - identificadores de país	30%-60%	40%-60%
Dados pessoais confidenciais	80%-95%	20%-30%
Categorias	90%-97%	60%-80%

O que está incluído em cada relatório de lista de arquivos (arquivo CSV)

A partir de cada página de investigação, você pode baixar listas de arquivos (em formato CSV) que incluem detalhes sobre os arquivos identificados. Se houver mais de 10.000 resultados, apenas os 10.000 primeiros aparecem na lista.

Cada lista de arquivos inclui as seguintes informações:

- Nome do ficheiro
- Tipo de localização
- Ambiente de trabalho
- Repositório de storage
- Protocolo
- Caminho do ficheiro
- Tipo de ficheiro
- Categoria
- Informações pessoais
- Informações pessoais sensíveis
- Data de deteção de eliminação

  Uma data de deteção de exclusão identifica a data em que o arquivo foi excluído ou movido. Isso permite que você identifique quando os arquivos confidenciais foram movidos. Os arquivos excluídos não fazem parte da contagem de números de arquivo que aparece no painel ou na página de investigação. Os arquivos só aparecem nos relatórios CSV.

Visualização de relatórios de conformidade

O Cloud Compliance fornece relatórios que você pode usar para entender melhor o status do programa de privacidade de dados da sua organização.

Por padrão, o dashboard do Cloud Compliance exibe dados de conformidade para todos os ambientes de trabalho e bancos de dados. Se desejar exibir relatórios que contenham dados apenas para alguns dos ambientes de trabalhoselecione esses ambientes de trabalho, .

A NetApp não pode garantir 100% de precisão dos dados pessoais e dados pessoais confidenciais que o Cloud Compliance identifica. Deve sempre validar as informações através da revisão dos dados.

Relatório de avaliação de risco de privacidade

O Relatório de avaliação de risco de privacidade fornece uma visão geral do status de risco à privacidade da sua organização, conforme exigido pelas regulamentações de privacidade, como GDPR e CCPA. O relatório inclui as seguintes informações:

Status de conformidade

A pontuação de gravidade e a distribuição de dados, sejam eles não sensíveis, pessoais ou sensíveis.

Visão geral da avaliação

Uma discriminação dos tipos de dados pessoais encontrados, bem como das categorias de dados.

Sujeitos de dados nesta avaliação

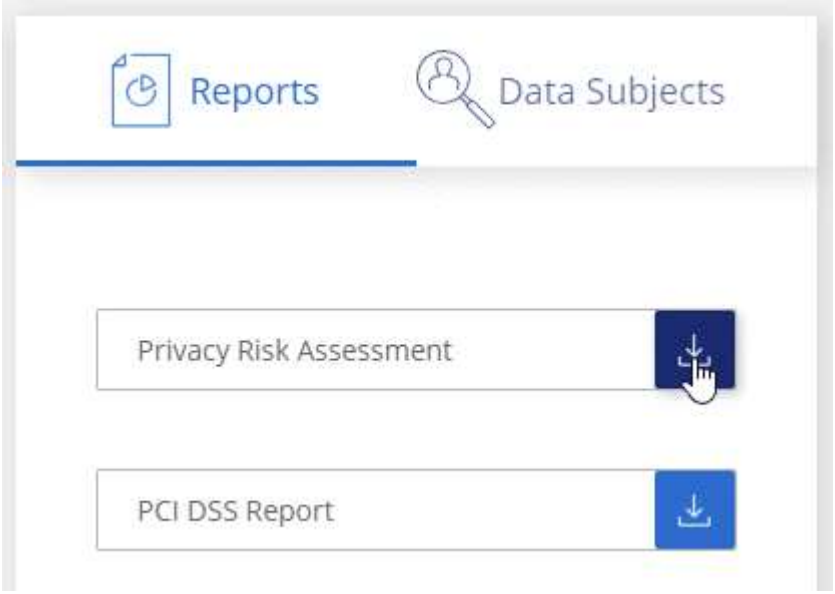
O número de pessoas, por localização, para as quais foram encontrados identificadores nacionais.

Gerando o Relatório de avaliação de risco de Privacidade

Vá para a guia conformidade para gerar o relatório.

Passos

1. Na parte superior do Cloud Manager, clique em **Cloud Compliance**.
2. Em **relatórios**, clique no ícone de download ao lado de **avaliação de risco de privacidade**.



Resultado

O Cloud Compliance gera um relatório em PDF que você pode revisar e enviar para outros grupos conforme necessário.

Pontuação de gravidade

O Cloud Compliance calcula a pontuação de gravidade para o Relatório de avaliação de risco de privacidade com base em três variáveis:

- A percentagem de dados pessoais de todos os dados.
- A percentagem de dados pessoais sensíveis de todos os dados.
- O percentual de arquivos que incluem titulares de dados, determinado por identificadores nacionais, como IDs nacionais, números de Segurança Social e números de identificação fiscal.

A lógica utilizada para determinar a pontuação é a seguinte:

Pontuação de gravidade	Lógica
0	Todas as três variáveis são exatamente 0%
1	Uma das variáveis é maior que 0%
2	Uma das variáveis é maior que 3%
3	Duas das variáveis são maiores que 3%
4	Três das variáveis são maiores que 3%
5	Uma das variáveis é maior que 6%
6	Duas das variáveis são maiores que 6%
7	Três das variáveis são maiores que 6%
8	Uma das variáveis é maior que 15%
9	Duas das variáveis são maiores que 15%
10	Três das variáveis são maiores que 15%

Relatório PCI DSS

O Relatório padrão de Segurança de dados da indústria de cartões de pagamento (PCI DSS) pode ajudá-lo a identificar a distribuição de informações de cartão de crédito entre seus arquivos. O relatório inclui as seguintes informações:

Visão geral

Quantos arquivos contêm informações de cartão de crédito e em que ambientes de trabalho.

Criptografia

A porcentagem de arquivos que contêm informações de cartão de crédito que estão em ambientes de trabalho criptografados ou não criptografados. Esta informação é específica do Cloud Volumes ONTAP.

Proteção contra ransomware

A porcentagem de arquivos que contêm informações de cartão de crédito que estão em ambientes de trabalho que possuem ou não proteção contra ransomware ativada. Esta informação é específica do Cloud Volumes ONTAP.

Retenção

O período de tempo em que os arquivos foram modificados pela última vez. Isso é útil porque você não deve manter as informações do cartão de crédito por mais tempo do que precisa processá-las.

Distribuição de informações de cartão de crédito

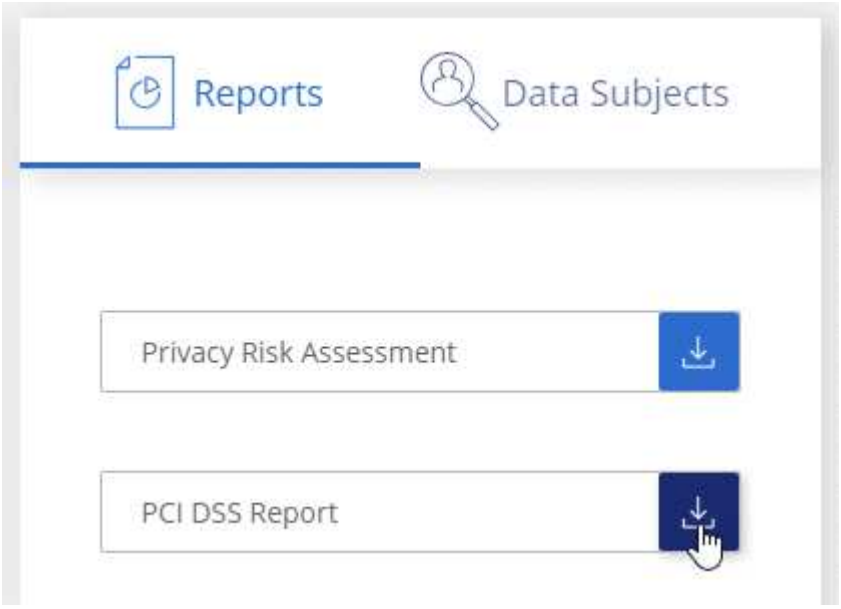
Os ambientes de trabalho onde as informações do cartão de crédito foram encontradas e se a criptografia e a proteção contra ransomware estão ativadas.

Gerando o Relatório PCI DSS

Vá para a guia conformidade para gerar o relatório.

Passos

1. Na parte superior do Cloud Manager, clique em **Cloud Compliance**.
2. Em **relatórios**, clique no ícone de download ao lado de **Relatório PCI DSS**.



Resultado

O Cloud Compliance gera um relatório em PDF que você pode revisar e enviar para outros grupos conforme necessário.

Relatório HIPAA

O Relatório HIPAA (Health Insurance Portability and Accountability Act) pode ajudá-lo a identificar arquivos contendo informações de saúde. Criado para auxiliar a organização a obedecer às leis de privacidade de dados HIPAA. As informações que o Cloud Compliance procura incluem:

- Padrão de referência de saúde
- Código médico ICD-10-CM
- Código médico ICD-9-CM
- RH – categoria Saúde
- Categoria de dados da aplicação de integridade

O relatório inclui as seguintes informações:

Visão geral

Quantos arquivos contêm informações de saúde e em quais ambientes de trabalho.

Criptografia

A porcentagem de arquivos que contêm informações de integridade que estão em ambientes de trabalho criptografados ou não criptografados. Esta informação é específica do Cloud Volumes ONTAP.

Proteção contra ransomware

A porcentagem de arquivos que contêm informações de integridade que estão em ambientes de trabalho que possuem ou não proteção contra ransomware habilitada. Esta informação é específica do Cloud Volumes ONTAP.

Retenção

O período de tempo em que os arquivos foram modificados pela última vez. Isso é útil porque você não deve manter as informações de saúde por mais tempo do que precisa processá-las.

Distribuição de informações em Saúde

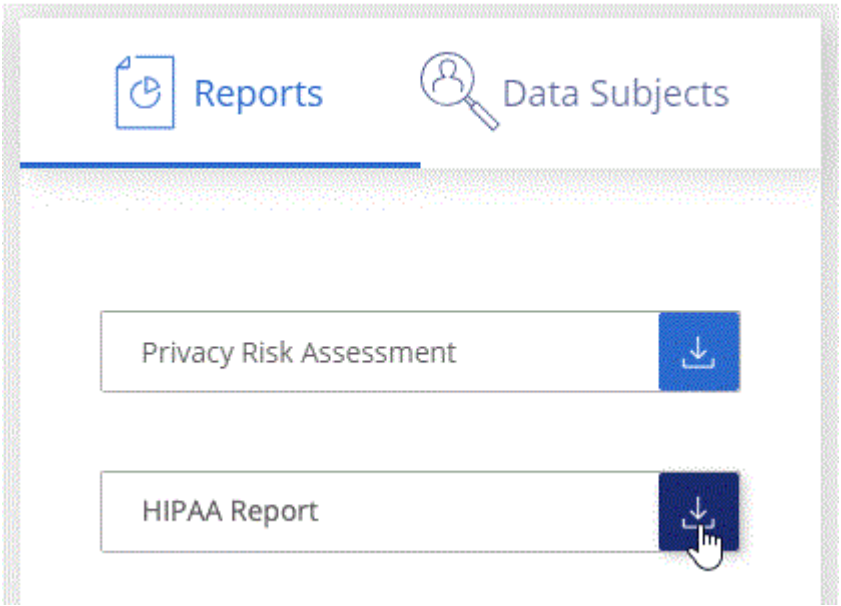
Os ambientes de trabalho onde as informações de integridade foram encontradas e se a criptografia e a proteção contra ransomware estão ativadas.

Gerando o Relatório HIPAA

Vá para a guia conformidade para gerar o relatório.

Passos

1. Na parte superior do Cloud Manager, clique em **Cloud Compliance**.
2. Em **relatórios**, clique no ícone de download ao lado de **Relatório HIPAA**.



Resultado

O Cloud Compliance gera um relatório em PDF que você pode revisar e enviar para outros grupos conforme necessário.

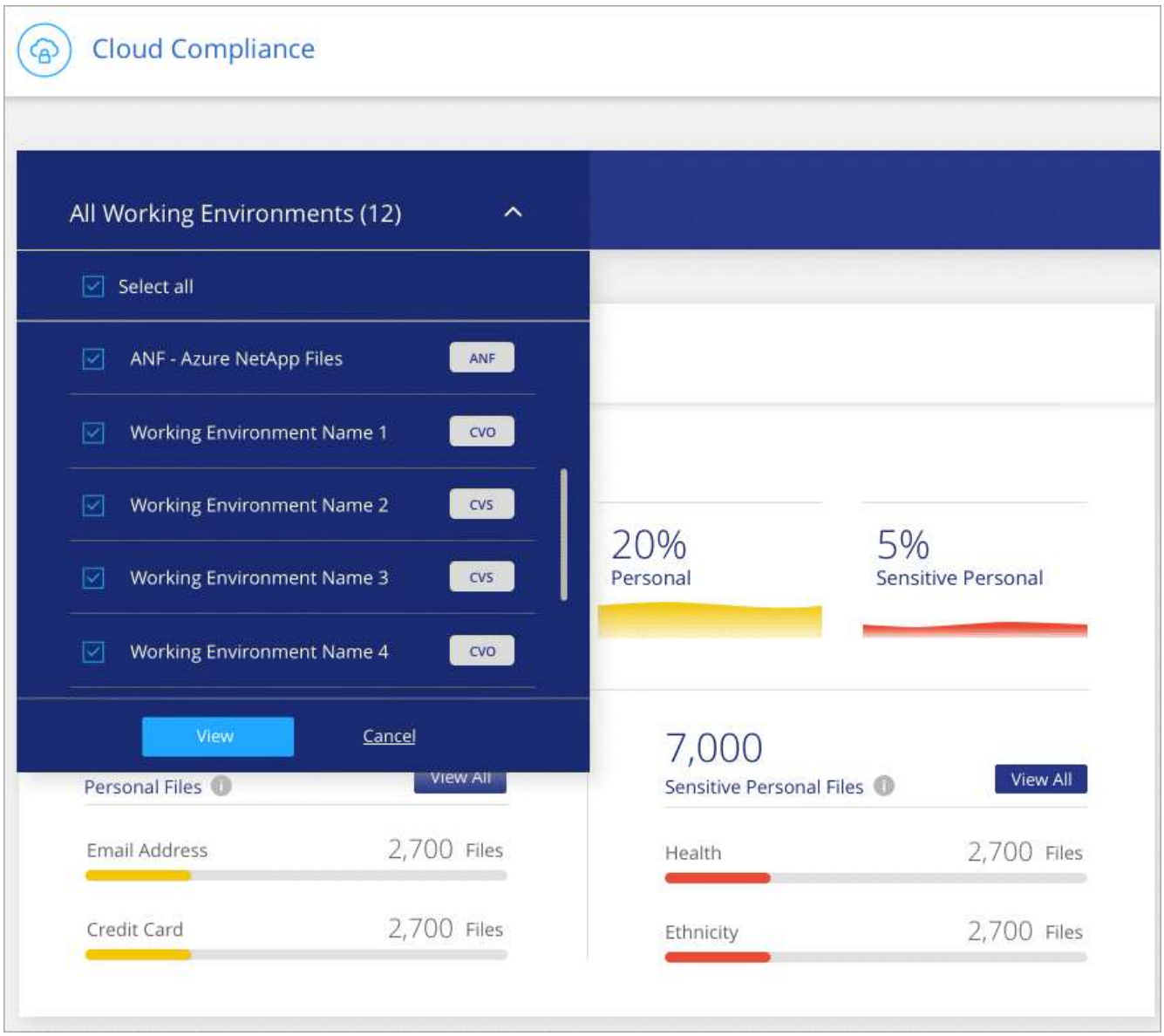
Selecionar os ambientes de trabalho para relatórios

Você pode filtrar o conteúdo do dashboard do Cloud Compliance para ver os dados de conformidade de todos os ambientes de trabalho e bancos de dados ou apenas para ambientes de trabalho específicos.

Quando você filtra o painel, o Cloud Compliance escoa os dados de conformidade e os relatórios apenas para os ambientes de trabalho selecionados.

Passos

1. Clique no menu suspenso filtro, selecione os ambientes de trabalho para os quais deseja exibir dados e clique em **Exibir**.



Resposta a uma solicitação de acesso do titular dos dados

Responder a uma solicitação de acesso ao titular dos dados (DSAR), pesquisando o nome completo ou identificador conhecido de um indivíduo (como um endereço de e-mail) e, em seguida, baixando um relatório. O relatório foi projetado para auxiliar na

exigência de sua organização em cumprir com o GDPR ou leis de privacidade de dados semelhantes.

> A NetApp não pode garantir 100% de precisão dos dados pessoais e dados pessoais confidenciais que o Cloud Compliance identifica. Deve sempre validar as informações através da revisão dos dados.

O que é uma solicitação de acesso ao titular dos dados?

As regulamentações de privacidade, como o GDPR europeu, concedem aos titulares dos dados (como clientes ou funcionários) o direito de acessar seus dados pessoais. Quando um titular de dados solicita essas informações, isso é conhecido como DSAR (solicitação de acesso do titular dos dados). As organizações devem responder a essas solicitações "sem demora indevida" e, o mais tardar, no prazo de um mês após o recebimento.

Como o Cloud Compliance pode ajudá-lo a responder a um DSAR?

Quando você realiza uma pesquisa de titular de dados, o Cloud Compliance localiza todos os arquivos que possuem o nome ou identificador dessa pessoa. O Cloud Compliance verifica os dados pré-indexados mais recentes para o nome ou identificador. Não inicia uma nova digitalização.

Depois que a pesquisa estiver concluída, você poderá baixar a lista de arquivos para um relatório de solicitação de acesso do titular dos dados. O relatório agrega insights dos dados e os coloca em termos legais que você pode enviar de volta para a pessoa.

Procurar por titulares de dados e transferir relatórios

Procure o nome completo ou identificador conhecido do titular dos dados e, em seguida, transfira um relatório de lista de ficheiros ou relatório DSAR. Pode pesquisar por "qualquer tipo de informação pessoal".

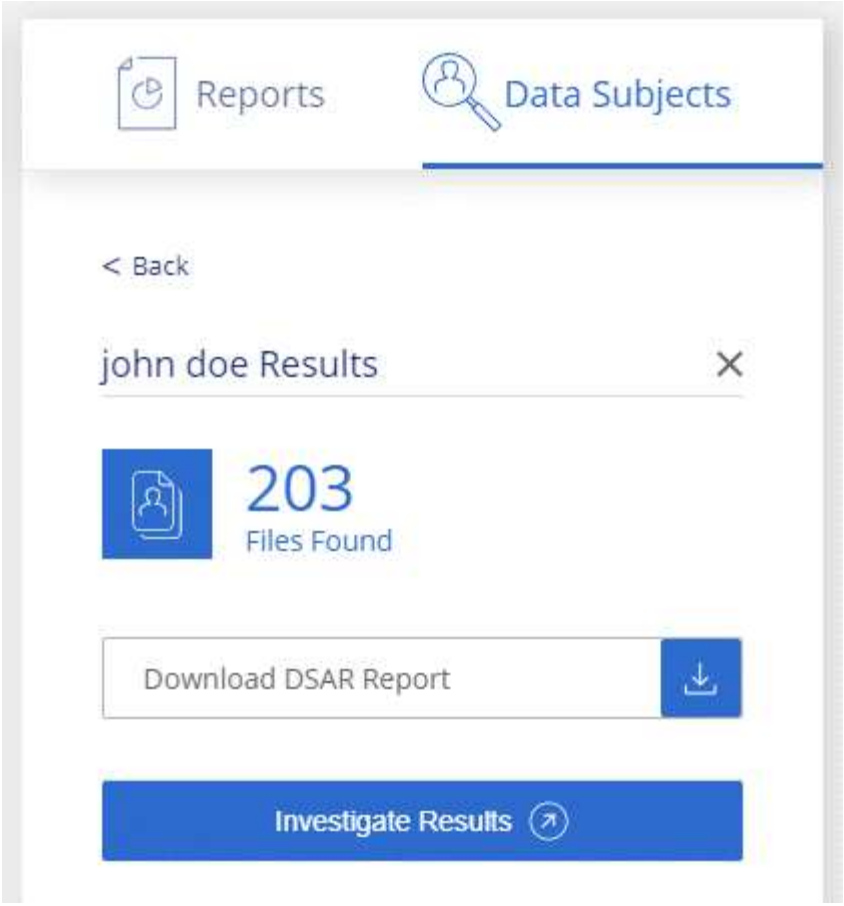
Apenas o inglês é suportado ao procurar os nomes dos titulares dos dados. O suporte para mais idiomas será adicionado mais tarde.

> A pesquisa de titulares de dados não é suportada em bases de dados neste momento.

Passos

1. Na parte superior do Cloud Manager, clique em **Cloud Compliance**.
2. Clique em **Assunto de dados**.
3. Procure o nome completo ou identificador conhecido do titular dos dados.

   Aqui está um exemplo que mostra uma pesquisa para o nome *john doe*:



4. Escolha uma das opções disponíveis:
   - **Download de Relatório DSAR**: Uma resposta formal à solicitação de acesso que você pode enviar ao titular dos dados. Este relatório contém informações geradas automaticamente com base nos dados que o Cloud Compliance foi encontrado no titular dos dados e foi projetado para ser usado como modelo. Você deve preencher o formulário e revisá-lo internamente antes de enviá-lo para o titular dos dados.
   - **Investigar resultados**: Uma página que permite investigar os dados pesquisando, classificando, expandindo detalhes para um arquivo específico e baixando a lista de arquivos.

     Se houver mais de 10.000 resultados, apenas os 10.000 primeiros aparecem na lista de arquivos.

Desativação do Cloud Compliance

Se necessário, você pode impedir que o Cloud Compliance escaneie um ou mais ambientes de trabalho ou bancos de dados. Você também pode excluir a instância do Cloud Compliance se não quiser mais usar o Cloud Compliance com seus ambientes de trabalho.

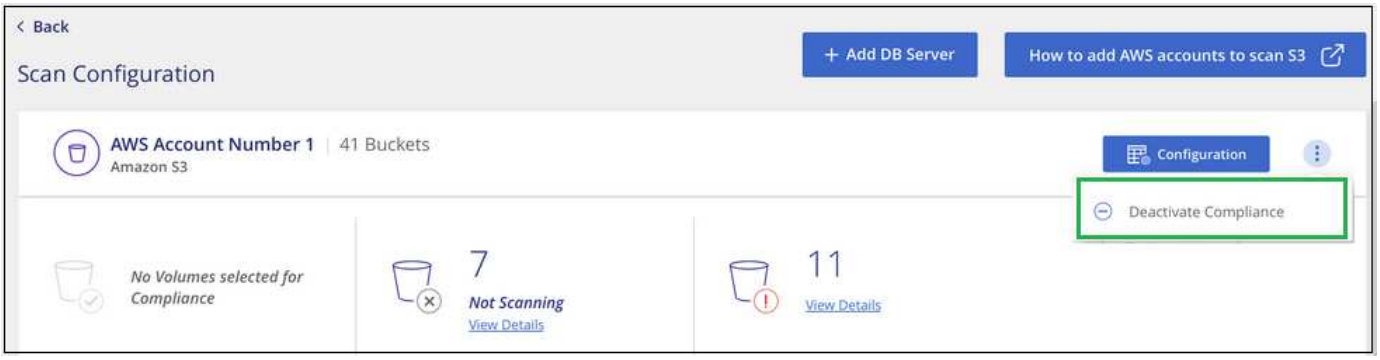
A desativação da conformidade verifica se há um ambiente de trabalho

Quando você desativa as verificações, o Cloud Compliance não verifica mais os dados no sistema e remove os insights de conformidade indexados da instância do Cloud Compliance (os dados do ambiente de trabalho

ou do próprio banco de dados não são excluídos).

Passos

Na página *Scan Configuration*, clique no botão na linha do ambiente de trabalho e, em seguida, clique em **Deactivate Compliance**.



Você também pode desativar as verificações de conformidade para um ambiente de trabalho no painel Serviços quando você selecionar o ambiente de trabalho.

Excluindo a instância do Cloud Compliance

Você pode excluir a instância do Cloud Compliance se não quiser mais usar o Cloud Compliance. A exclusão da instância também exclui os discos associados onde os dados indexados residem.

Passo

1. Vá para o console do seu provedor de nuvem e exclua a instância do Cloud Compliance.

   A instância é chamada *CloudCompliance* com um hash gerado (UUID) concatenado a ela. Por exemplo: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

Perguntas frequentes sobre o Cloud Compliance

Esta FAQ pode ajudar se você está apenas procurando uma resposta rápida para uma pergunta.

O que é o Cloud Compliance?

O Cloud Compliance é uma oferta de nuvem que usa a tecnologia orientada por Inteligência artificial (AI) para ajudar as organizações a entender o contexto dos dados e identificar dados confidenciais em suas configurações do Azure NetApp Files, sistemas Cloud Volumes ONTAP hospedados na AWS ou Azure, buckets do Amazon S3 e bancos de dados.

O Cloud Compliance fornece parâmetros predefinidos (como categorias e tipos de informações confidenciais) para lidar com as novas regulamentações de conformidade de dados para a privacidade e a sensibilidade dos dados, como GDPR, CCPA, HIPAA e muito mais.

Por que devo usar o Cloud Compliance?

O Cloud Compliance ajuda você a:

- Cumprir as regulamentações de privacidade e conformidade de dados.
- Obedecer às políticas de retenção de dados.
- Localize e reporte facilmente dados específicos em resposta aos titulares do dados, conforme exigido pelo GDPR, CCPA, HIPAA e outras regulamentações sobre a privacidade de dados.

Quais são os casos de uso comuns para o Cloud Compliance?

- Identificar informações pessoais identificáveis (PII).
- Identifique um amplo escopo de informações confidenciais conforme exigido pelas regulamentações de privacidade do GDPR e CCPA.
- Cumprir as novas e futuras regulamentações de privacidade de dados.

"Saiba mais sobre os casos de uso do Cloud Compliance".

Que tipos de dados podem ser verificados com o Cloud Compliance?

O Cloud Compliance dá suporte à verificação de dados não estruturados em protocolos NFS e CIFS gerenciados pela Cloud Volumes ONTAP e Azure NetApp Files. O Cloud Compliance também pode verificar os dados armazenados nos buckets do Amazon S3.

Além disso, o Cloud Compliance pode verificar bancos de dados localizados em qualquer lugar - eles não precisam ser gerenciados pelo Cloud Manager.

"Saiba como as digitalizações funcionam".

Quais fornecedores de nuvem são compatíveis?

O Cloud Compliance opera como parte do Cloud Manager e, atualmente, é compatível com AWS e Azure. Isso proporciona à sua organização uma visibilidade unificada da privacidade entre diferentes fornecedores de nuvem. O suporte ao Google Cloud Platform (GCP) será adicionado em breve.

Como faço para acessar o Cloud Compliance?

O Cloud Compliance é operado e gerenciado por meio do Cloud Manager. Você pode acessar os recursos de conformidade na nuvem a partir da guia **Compliance** no Cloud Manager.

Como funciona o Cloud Compliance?

O Cloud Compliance implanta outra camada de inteligência artificial ao lado do sistema e dos sistemas de storage do Cloud Manager. Em seguida, ele verifica os dados em volumes, buckets e bancos de dados e indexa os insights de dados encontrados.

"Saiba mais sobre como o Cloud Compliance funciona".

Quanto custa o Cloud Compliance?

O custo para usar o Cloud Compliance depende da quantidade de dados que você está digitalizando. Os primeiros 1 TB de dados verificados pelo Cloud Compliance em um espaço de trabalho do Cloud Manager são gratuitos. Uma assinatura do AWS ou Azure Marketplace é necessária para continuar a digitalizar dados após esse ponto. "preços"Consulte para obter detalhes.

Com que frequência o Cloud Compliance verifica meus dados?

Os dados são alterados com frequência. Assim, o Cloud Compliance verifica seus dados continuamente sem impacto nos dados. Embora a digitalização inicial dos seus dados possa demorar mais tempo, as digitalizações subsequentes apenas analisam as alterações incrementais, o que reduz os tempos de digitalização do sistema.

"Saiba como as digitalizações funcionam".

O Cloud Compliance oferece relatórios?

Sim. As informações oferecidas pelo Cloud Compliance podem ser relevantes para outras partes interessadas em suas organizações, por isso, permitimos que você gere relatórios para compartilhar os insights.

Os seguintes relatórios estão disponíveis para conformidade com a nuvem:

Relatório de avaliação de risco de privacidade
: Fornece insights de privacidade de seus dados e uma pontuação de risco de privacidade. "Saiba mais".

Relatório de solicitação de acesso do titular dos dados
: Permite que você extraia um relatório de todos os arquivos que contêm informações sobre o nome específico ou identificador pessoal de um titular de dados. "Saiba mais".

Relatório PCI DSS
: Ajuda você a identificar a distribuição de informações de cartão de crédito entre seus arquivos. "Saiba mais".

Relatório HIPAA
: Ajuda você a identificar a distribuição de informações de saúde entre seus arquivos. "Saiba mais".

Relatórios sobre um tipo de informação específico
: Estão disponíveis relatórios que incluem detalhes sobre os arquivos identificados que contêm dados pessoais e dados pessoais confidenciais. Você também pode ver os arquivos divididos por categoria e tipo de arquivo. "Saiba mais".

Que tipo de instância ou VM é necessário para o Cloud Compliance?

- No Azure, o Cloud Compliance é executado em uma VM Standard_D16s_v3 com um disco de 512 GB.
- Na AWS, o Cloud Compliance é executado em uma instância do m5,4xlarge com um disco GP2 de 500 GB.

  Em regiões onde o m5,4xlarge não está disponível, o Cloud Compliance é executado em uma instância do m4,4xlarge.

> Alterar ou redimensionar o tipo de instância/VM não é suportado. Você precisa usar o tamanho padrão fornecido.

"Saiba mais sobre como o Cloud Compliance funciona".

O desempenho da digitalização varia?

O desempenho da digitalização pode variar com base na largura de banda da rede e no tamanho médio do ficheiro no seu ambiente de nuvem.

Quais tipos de arquivo são suportados?

O Cloud Compliance verifica todos os arquivos para obter informações sobre categorias e metadados e exibe todos os tipos de arquivo na seção tipos de arquivo do painel.

Quando o Cloud Compliance deteta informações pessoais identificáveis (PII) ou quando realiza uma pesquisa DSAR, apenas os seguintes formatos de arquivo são suportados: .PDF, .DOCX, .DOC, .PPTX, .XLS, .XLSX, .CSV, .TXT, .RTF e .json.

Como habilito o Cloud Compliance?

Primeiro, você precisa implantar uma instância de Cloud Compliance no Cloud Manager. Quando a instância estiver em execução, você poderá ativá-la em ambientes de trabalho e bancos de dados existentes na guia **Compliance** ou selecionando um ambiente de trabalho específico.

"Saiba como começar".

A ativação do Cloud Compliance resulta em uma verificação inicial imediata. Os resultados de conformidade são exibidos pouco depois.

Como posso desativar o Cloud Compliance?

Você pode desativar o Cloud Compliance na página ambientes de trabalho depois de selecionar um ambiente de trabalho individual.

"Saiba mais".

Para remover completamente a instância do Cloud Compliance, você pode remover manualmente a instância do Cloud Compliance do portal do seu provedor de nuvem.

O que acontece se a disposição de dados em categorias estiver ativada no Cloud Volumes ONTAP?

Você pode querer habilitar o Cloud Compliance em um sistema Cloud Volumes ONTAP que categoriza dados inativos no storage de objetos. Se a disposição de dados em categorias estiver ativada, o Cloud Compliance verifica todos os dados que estão em discos e dados inativos dispostos no storage de objetos.

A verificação de conformidade não aquece os dados frios - permanece fria e dividida em armazenamento de objetos.

Posso usar o Cloud Compliance para analisar o storage ONTAP no local?

A digitalização dos dados diretamente de um ambiente de trabalho do ONTAP no local não é compatível. Mas você pode digitalizar seus dados ONTAP locais replicando os dados NFS ou CIFS locais em um ambiente de trabalho Cloud Volumes ONTAP e ativando a conformidade nesses volumes. Estamos planejando dar suporte ao Cloud Compliance com ofertas de nuvem adicionais, como o Cloud Volumes Service.

"Saiba mais".

O Cloud Compliance pode enviar notificações para minha organização?

Não, mas você pode baixar relatórios de status que você pode compartilhar internamente em sua organização.

Posso personalizar o serviço de acordo com as necessidades da minha organização?

O Cloud Compliance fornece insights prontos para uso para seus dados. Esses insights podem ser extraídos e usados para atender às necessidades da sua organização.

Posso limitar as informações de conformidade na nuvem a usuários específicos?

Sim, o Cloud Compliance é totalmente integrado ao Cloud Manager. Os usuários do Cloud Manager só podem ver informações sobre os ambientes de trabalho que estão qualificados para visualizar de acordo com a Privileges do workspace.

Além disso, se você quiser permitir que certos usuários visualizem apenas os resultados da verificação do Cloud Compliance sem ter a capacidade de gerenciar as configurações de Cloud Compliance, você pode atribuir a esses usuários a função *Cloud Compliance Viewer*.

"Saiba mais".

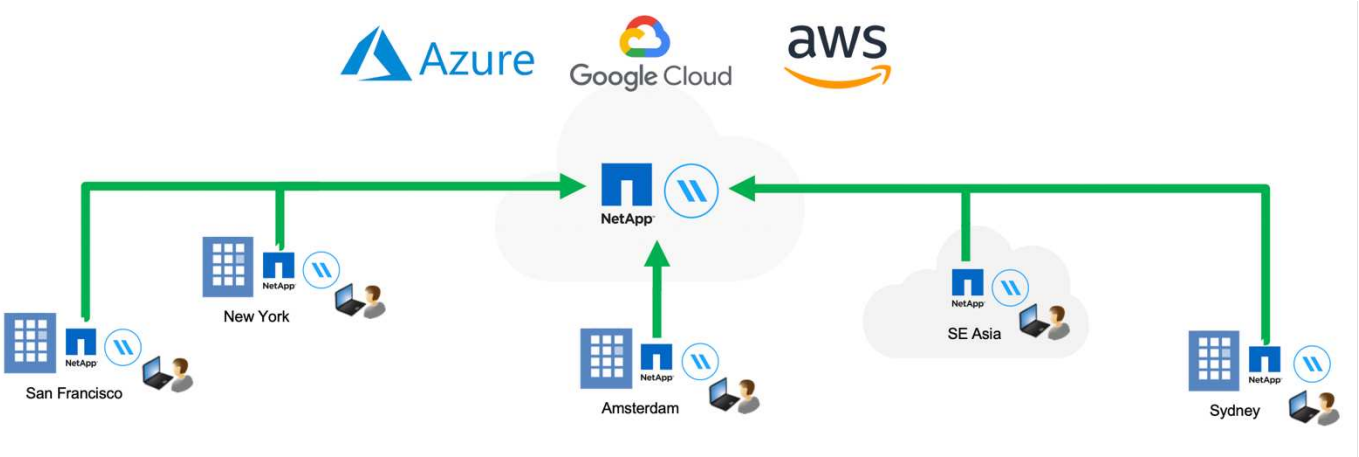
Habilite o compartilhamento global de arquivos em tempo real

Saiba mais sobre o Global File Cache

Com o NetApp, você consolida silos de servidores de arquivos distribuídos em um espaço físico do storage global e coeso na nuvem pública. Isso cria um sistema de arquivos globalmente acessível na nuvem que todos os locais remotos podem usar como se fossem locais.

Visão geral

A implementação do Global File Cache resulta em um espaço físico do storage centralizado e em uma arquitetura de storage distribuída que exija gerenciamento de dados local, backup, gerenciamento de segurança, storage e espaço físico da infraestrutura em cada local.



Caraterísticas

O Global File Cache habilita os seguintes recursos:

- Consolide e centralize seus dados na nuvem pública e aproveite a escalabilidade e o desempenho de soluções de storage de nível empresarial
- Crie um único conjunto de dados para usuários globalmente e aproveite o armazenamento em cache inteligente de arquivos para melhorar o acesso, a colaboração e o desempenho globais dos dados
- Confie em um cache autossustentável e autogerenciado, e elimine cópias de dados e backups completos. Use o armazenamento em cache de arquivos local para dados ativos e reduza os custos de storage
- Acesso transparente a partir de filiais por meio de um namespace global com bloqueio central de arquivos em tempo real

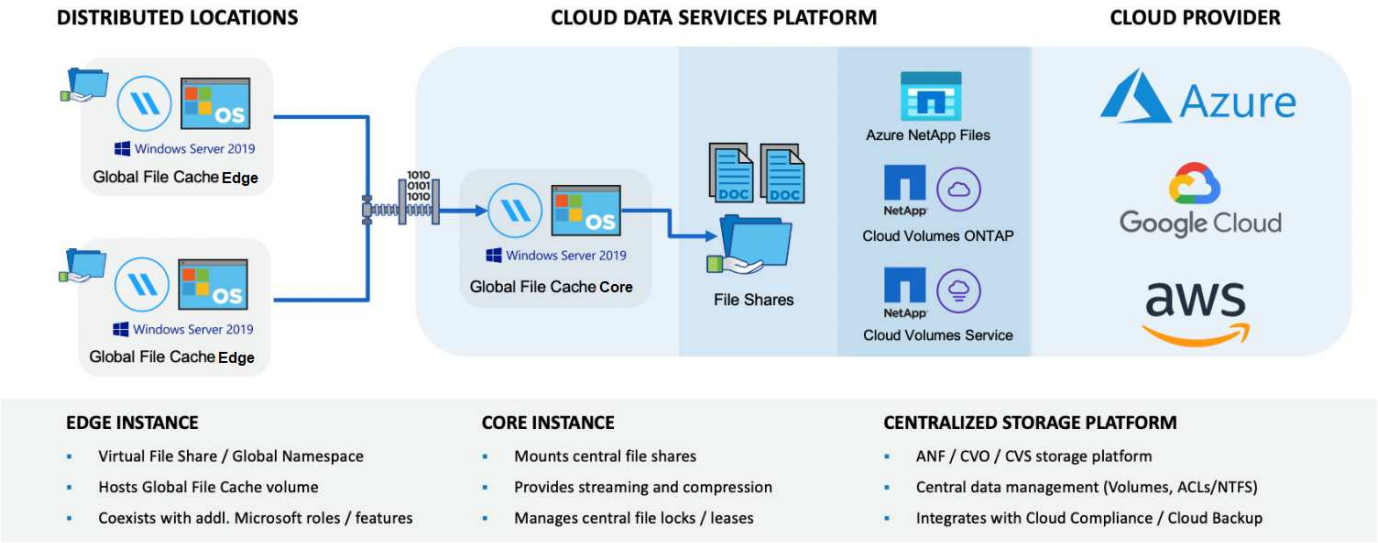
Consulte mais sobre os recursos e casos de uso do Global File Cache "aqui" .

Componentes de cache de arquivos global

O Global File Cache consiste nos seguintes componentes:

- Servidor de gerenciamento global de cache de arquivos
- Global File Cache Core
- Global File Cache Edge (implantado em seus locais remotos)

A instância principal do cache global de arquivos é montada em compartilhamentos de arquivos corporativos hospedados na plataforma de storage de back-end escolhida (como Cloud Volumes ONTAP, Cloud Volumes Service e Azure NetApp Files) e cria o malha de cache global de arquivos que permite centralizar e consolidar dados não estruturados em um único conjunto de dados, estejam eles residindo em uma ou várias plataformas de storage na nuvem pública.



Plataformas de storage compatíveis

As plataformas de armazenamento suportadas para Global File Cache diferem dependendo da opção de implementação selecionada.

Opções de implantação automatizadas

O Global File Cache é compatível com os seguintes tipos de ambientes de trabalho quando implantado usando o Cloud Manager:

- Cloud Volumes ONTAP no Azure
- Cloud Volumes ONTAP na AWS

Essa configuração permite implantar e gerenciar toda a implantação do lado do servidor do Global File Cache, incluindo o Global File Cache Management Server e o Global File Cache Core, a partir do Cloud Manager.

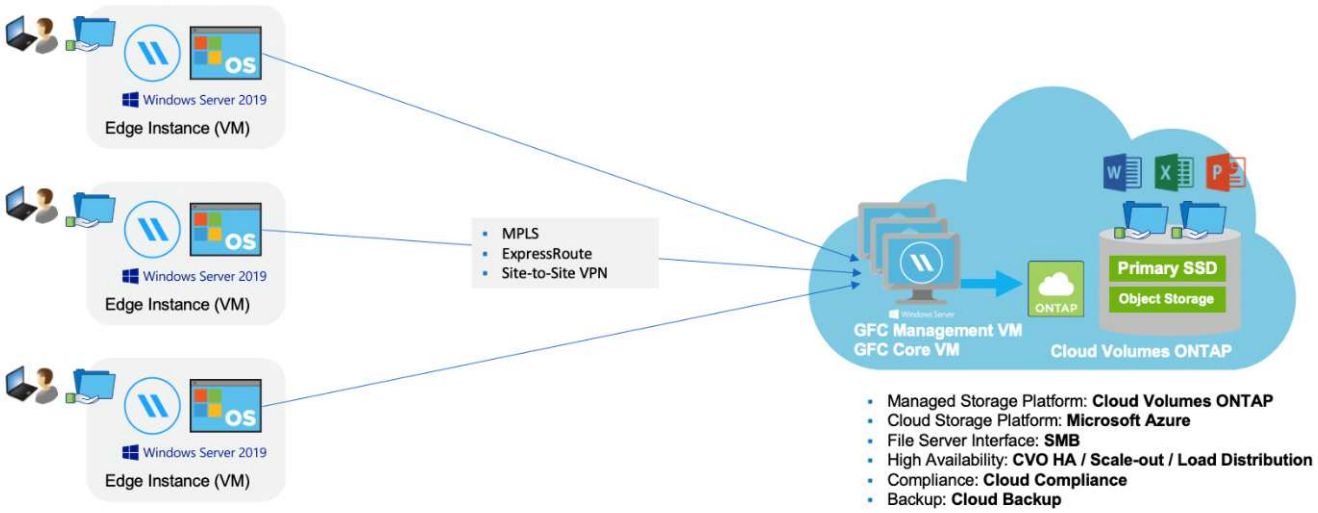
Opções de implantação manual

As configurações globais de cache de arquivos também são compatíveis com o Cloud Volumes ONTAP, o Cloud Volumes Service ou o Azure NetApp Files instalados no Microsoft Azure, no Google Cloud Platform ou na infraestrutura de storage de nuvem pública da Amazon Web Services. Soluções no local também estão disponíveis nas plataformas NetApp AFF e FAS. Nessas instalações, os componentes do lado do servidor do Global File Cache devem ser configurados e implantados manualmente, não usando o Cloud Manager.

Consulte "Guia do usuário do cache global de arquivos da NetApp"para obter detalhes.

Como o Global File Cache funciona

O Global File Cache cria uma malha de software que armazena em cache conjuntos de dados ativos em escritórios remotos globalmente. Como resultado, os usuários de negócios têm acesso transparente aos dados e performance ideal em escala global.



A topologia referenciada neste exemplo é um modelo de hub e spoke, pelo qual a rede de escritórios/locais remotos está acessando um conjunto comum de dados na nuvem. Os pontos-chave deste exemplo são:

- Armazenamento de dados centralizado:
  - Plataforma de storage de nuvem pública empresarial, como o Cloud Volumes ONTAP
- Global File Cache Fabric:
  - Extensão do armazenamento de dados central para os locais remotos
  - Instância global File Cache Core, montagem em compartilhamentos de arquivos corporativos (SMB).
  - Instâncias do Global File Cache Edge em execução em cada local remoto.
  - Apresenta um compartilhamento de arquivo virtual em cada local remoto que fornece acesso a dados centrais.
  - Hospeda o Intelligent File Cache em um volume NTFS personalizado (`D:\`).
- Configuração de rede:
  - Multiprotocolo Label Switching (MPLS), ExpressRoute ou conetividade VPN
- Integração com os serviços de domínio do ative Directory do cliente.
- Namespace DFS para o uso de um namespace global (recomendado).

Custo

O custo para usar o Global File Cache depende do tipo de instalação que você escolheu.

- Todas as instalações exigem que você implante um ou mais volumes na nuvem (Cloud Volumes ONTAP, Cloud Volumes Service ou Azure NetApp Files). Isso resulta em cobranças do provedor de nuvem selecionado.
- Todas as instalações também exigem que você implante duas ou mais máquinas virtuais (VMs) na nuvem.

Isso resulta em cobranças do provedor de nuvem selecionado.

- Servidor de gerenciamento global de cache de arquivos:

  No Azure, isso é executado em uma VM D2S_V3 ou equivalente (2 vCPU/8GB GB de RAM) com 127GB SSD premium

  Na AWS, isso é executado em uma instância M4.Large ou equivalente (2 vCPU/8GB GB de RAM) com 127GB SSD de uso geral

- Global File Cache Core:

  No Azure, isso é executado em uma VM D4S_V3 ou equivalente (4 vCPU/16GB GB de RAM) com 127GB SSD premium

  Na AWS, isso é executado em uma instância M4.xlarge ou equivalente (4 vCPU/16GB GB de RAM) com 127GB SSD de uso geral

- Quando instalado com o Cloud Volumes ONTAP no Azure ou na AWS (as configurações com suporte implantadas completamente por meio do Cloud Manager), há uma cobrança de $3.000 USD por local (para cada instância de borda de cache de arquivos global), por ano.
- Quando instalado usando as opções de implantação manual, o preço é diferente. Para ver uma estimativa de alto nível de custos, consulte "Calcule seu potencial de economia" ou consulte o seu Engenheiro de soluções de Cache Global de arquivos para discutir as melhores opções para a implantação da sua empresa.

Licenciamento

O Global File Cache inclui um servidor de gerenciamento de licenças (LMS) baseado em software, que permite consolidar o gerenciamento de licenças e implantar licenças para todas as instâncias Core e Edge usando um mecanismo automatizado.

Ao implantar sua primeira instância do Core no datacenter ou na nuvem, você pode escolher designar essa instância como LMS para sua organização. Essa instância do LMS é configurada uma vez, coneta-se ao serviço de assinatura (por HTTPS) e valida sua assinatura usando o ID do cliente fornecido pelo nosso departamento de suporte/operações após a habilitação da assinatura. Depois de ter feito essa designação, você associa suas instâncias do Edge ao LMS fornecendo seu ID de cliente e o endereço IP da instância do LMS.

Quando você compra licenças Edge adicionais ou renova sua assinatura, nosso departamento de suporte/operações atualiza os detalhes da licença, por exemplo, o número de sites ou a data de término da assinatura. Depois que o LMS consulta o serviço de assinatura, os detalhes da licença são atualizados automaticamente na instância do LMS e serão aplicados às suas instâncias do GFC Core e Edge.

Consulte o "Guia do usuário do cache global de arquivos da NetApp" para obter detalhes adicionais sobre licenciamento.

Limitações

- A versão do Global File Cache suportada no Cloud Manager requer que a plataforma de storage de back-end usada como seu storage central seja um ambiente operacional no qual você implantou um nó único ou par de HA da Cloud Volumes ONTAP no Azure ou na AWS.

  Outras plataformas de storage e outros provedores de nuvem não são compatíveis no momento usando o

Cloud Manager, mas podem ser implantadas usando procedimentos de implantação legados.

Essas outras configurações, por exemplo, o cache global de arquivos usando o Cloud Volumes ONTAP, o Cloud Volumes Service e o Azure NetApp Files no Microsoft Azure, o Google Cloud e a AWS continuam sendo compatíveis com os procedimentos legados. "Visão geral e integração do Global File Cache"Consulte para obter detalhes.

Antes de começar a implantar o Global File Cache

Há muitos requisitos que você precisa estar ciente antes de começar a implantar o Global File Cache na nuvem e em seus escritórios remotos.

Considerações sobre o design do Global File Cache Core

Dependendo dos seus requisitos, você pode precisar implantar uma ou várias instâncias principais do Global File Cache para criar a malha Global File Cache. A instância Core foi projetada para atuar como um agente de tráfego entre suas instâncias distribuídas do Global File Cache Edge e os recursos do servidor de arquivos do data center, por exemplo, compartilhamentos de arquivos, pastas e arquivos.

Ao projetar sua implantação Global File Cache, você precisa determinar o que é certo para seu ambiente em termos de escala, disponibilidade de recursos e redundância. O Global File Cache Core pode ser implantado das seguintes maneiras:

- Instância autônoma do GFC Core
- Projeto distribuído da carga do núcleo de GFC (Cold Standby)

Diretrizes de dimensionamentoConsulte para compreender o número máximo de instâncias do Edge e o total de usuários que cada configuração pode suportar:

Consulte o seu Engenheiro de soluções de Cache Global de arquivos para discutir as melhores opções para a implantação da sua empresa.

Diretrizes de dimensionamento

Há algumas razões de diretrizes de dimensionamento que você precisa ter em mente ao configurar o sistema inicial. Deve rever estas taxas depois de algum histórico de utilização ter acumulado para se certificar de que está a utilizar o sistema de forma ideal. Estes incluem:

- Relação de bordas/núcleo da cache de arquivos global
- Proporção de usuários distribuídos/margem de cache de arquivos global
- Usuários distribuídos/relação principal do cache de arquivos global

Número de instâncias Edge por instância principal

Nossas diretrizes recomendam até 10 instâncias Edge por instância Global File Cache Core, com um máximo de 20 bordas por instância Global File Cache Core. Isso depende de um grau significativo sobre o tipo e o tamanho médio do arquivo da carga de trabalho mais comum. Em alguns casos, com cargas de trabalho mais comuns, você pode adicionar mais instâncias de borda por núcleo, mas nesses casos você deve entrar em Contato com o suporte da NetApp para dimensionar corretamente o número de instâncias de borda e núcleo, dependendo dos tipos e tamanhos dos conjuntos de arquivos.

Você pode utilizar várias instâncias do Global File Cache Edge e Core simultaneamente para escalar sua infraestrutura, dependendo dos requisitos.

Número de usuários simultâneos por instância do Edge

O Global File Cache Edge lida com o trabalho pesado em termos de algoritmos de armazenamento em cache e diferenciação em nível de arquivo. Uma única instância do Global File Cache Edge pode atender até 400 usuários por instância física dedicada do Edge e até 200 usuários para implantações virtuais dedicadas. Isso depende de um grau significativo sobre o tipo e o tamanho médio do arquivo da carga de trabalho mais comum. Para maiores tipos de arquivos colaborativos, Oriente para 50% do máximo de usuários por limite inferior do Global File Cache Edge (dependendo da implantação física ou virtual). Para itens mais comuns do Office com um tamanho médio de arquivo inferior a 1MB, Oriente para os 100% de usuários por limite superior do Global File Cache Edge (dependendo da implantação física ou virtual).

O Global File Cache Edge deteta se está sendo executado em uma instância virtual ou física e limitará o número de conexões SMB ao compartilhamento de arquivos virtual local ao máximo de 200 ou 400 conexões simultâneas.

Número de usuários simultâneos por instância principal

A instância Global File Cache Core é extremamente escalável, com uma contagem de usuários simultâneos recomendada de 3.000 usuários por núcleo. Isso depende de um grau significativo sobre o tipo e o tamanho médio do arquivo da carga de trabalho mais comum.

Consulte o seu Engenheiro de soluções de Cache Global de arquivos para discutir as melhores opções para a implantação da sua empresa.

Pré-requisitos

Os pré-requisitos descritos nesta seção são para os componentes instalados na nuvem: O Global File Cache Management Server e o Global File Cache Core.

Os pré-requisitos do Global File Cache Edge são descritos "aqui".

Instância do Cloud Manager

Ao usar o Cloud Volumes ONTAP para Azure como sua plataforma de storage, verifique se o Cloud Manager tem permissões, conforme mostrado na última "Política do Cloud Manager para Azure".

As instâncias recém-criadas terão todas as permissões necessárias por padrão. Se você implantou sua instância antes da versão 3.8.7 (3 de agosto de 2020), precisará adicionar esses itens.

```
"Microsoft.Resources/deployments/operationStatuses/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/delete",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
```

Plataforma de storage (volumes)

A plataforma de storage de back-end – nesse caso, sua instância do Cloud Volumes ONTAP implantada – deve apresentar compartilhamentos de arquivos SMB. Quaisquer compartilhamentos que serão expostos por meio do Global File Cache devem permitir o controle total do grupo todos no nível de compartilhamento, enquanto restringem permissões por meio de permissões NTFS.

Se você não tiver configurado pelo menos um compartilhamento de arquivos SMB na instância do Cloud Volumes ONTAP, precisará ter as seguintes informações prontas para que você possa configurar essas informações durante a instalação:

- Nome de domínio do ative Directory, endereço IP do servidor de nomes, credenciais de administrador do ative Directory.
- O nome e o tamanho do volume que você deseja criar, o nome do agregado no qual o volume será criado e o nome do compartilhamento.

Recomendamos que o volume seja grande o suficiente para acomodar o conjunto de dados total para o aplicativo, juntamente com a capacidade de dimensionar de acordo com o crescimento do conjunto de dados. Se você tiver vários agregados no ambiente de trabalho, consulte "Gerenciamento de agregados existentes" para determinar qual agregado tem mais espaço disponível para o novo volume.

Servidor de gerenciamento global de cache de arquivos

Este servidor de gerenciamento de cache de arquivos global requer acesso externo por HTTPS (porta TCP 443) para se conetar ao serviço de assinatura do provedor de nuvem e acessar esses URLs:

- "https://talonazuremicroservices.azurewebsites.net"
- "https://talonlicensing.table.core.windows.net"

Esta porta deve ser excluída de quaisquer dispositivos de otimização WAN ou políticas de restrição de firewall para que o software Global File Cache funcione corretamente.

O Global File Cache Management Server também requer um nome único (geográfico) NetBIOS para a instância (como GFC-MS1).

Um servidor de gerenciamento pode oferecer suporte a várias instâncias globais de Cache de arquivos implantadas em diferentes ambientes de trabalho. Quando implantado a partir do Cloud Manager, cada ambiente de trabalho tem seu próprio storage de back-end separado e não conterá os mesmos dados.

Global File Cache Core

Este Global File Cache Core escuta o intervalo de portas TCP 6618-6630. Dependendo da configuração do firewall ou do grupo de segurança de rede (NSG), talvez seja necessário permitir explicitamente o acesso a essas portas por meio de regras de porta de entrada. Além disso, essas portas devem ser excluídas de quaisquer dispositivos de otimização de WAN ou políticas de restrição de firewall para que o software Global File Cache funcione corretamente.

Os requisitos principais do Global File Cache são:

- Um nome único (geográfico) NetBIOS para a instância (como GFC-Core1)
- Nome de domínio do ative Directory
  - As instâncias de cache de arquivos globais devem ser Unidas ao domínio do ative Directory.
  - As instâncias de cache de arquivo global devem ser gerenciadas em uma unidade organizacional específica (UO) Global File Cache e excluídas dos GPOs herdados da empresa.
- Conta de serviço. Os serviços neste Global File Cache Core são executados como uma conta de usuário de domínio específica. Essa conta, também conhecida como conta de serviço, deve ter o seguinte Privileges em cada um dos servidores SMB que serão associados à instância central de cache de arquivos global:
  - A conta de serviço provisionado deve ser um usuário de domínio.

Dependendo do nível de restrições e GPOs no ambiente de rede, essa conta pode exigir Privileges de administrador de domínio.

- Deve ter Privileges "Executar como serviço".
- A senha deve ser definida como "nunca expire".
- A opção conta "o usuário deve alterar senha no próximo logon" deve ser DESATIVADA (desmarcada).
- Ele deve ser um membro do grupo de operadores de backup internos do servidor de arquivos back-end (isso é ativado automaticamente quando implantado por meio do Cloud Manager).

Servidor de gerenciamento de licenças

- O Global File Cache License Management Server (LMS) deve ser configurado em uma edição padrão ou Datacenter do Microsoft Windows Server 2016 ou edição padrão ou Datacenter do Windows Server 2019, de preferência na instância Global File Cache Core no datacenter ou na nuvem.
- Se você precisar de uma instância separada do Global File Cache LMS, você precisará instalar o pacote de instalação mais recente do software Global File Cache em uma instância do Microsoft Windows Server imaculada.
- A instância do LMS precisa ser capaz de se conetar ao serviço de assinatura (Serviços do Azure / internet pública) usando HTTPS (porta TCP 443).
- As instâncias Core e Edge precisam se conetar à instância LMS usando HTTPS (porta TCP 443).

Rede

- Firewall: As portas TCP devem ser permitidas entre o Global File Cache Edge e as instâncias Core.
- Portas TCP: 443 (HTTPS), 6618–6630.
- Os dispositivos de otimização de rede (como Riverbed Steelhead) devem ser configurados para passar por portas específicas do Global File Cache (TCP 6618-6630).

Como começar

Você usa o Cloud Manager para implantar o Global File Cache Management Server e o software Global File Cache Core no ambiente de trabalho.

Ative o Cache de arquivos global usando o Cloud Manager

Nesta configuração, você implantará o servidor de gerenciamento global de cache de arquivos e o núcleo global de cache de arquivos no mesmo ambiente de trabalho em que você criou seu sistema Cloud Volumes ONTAP usando o Cloud Manager.

Observe "este vídeo" para ver os passos do início ao fim.

Início rápido

Comece rapidamente seguindo estas etapas ou role para baixo até as seções restantes para obter detalhes completos:

Implante o Cloud Volumes ONTAP

Implante o Cloud Volumes ONTAP no Azure ou na AWS e configure compartilhamentos de arquivos SMB. Para obter mais informações, consulte "Iniciar o Cloud Volumes ONTAP no Azure" ou "Iniciando o Cloud Volumes ONTAP na AWS".

Implante o Global File Cache Management Server

Implante uma instância do servidor de gerenciamento de cache de arquivos global no mesmo ambiente de trabalho que a instância do Cloud Volumes ONTAP.

Implante o Global File Cache Core

Implante uma instância, ou várias instâncias, do núcleo de cache de arquivos global no mesmo ambiente de trabalho que a instância do Cloud Volumes ONTAP e associe-a ao seu domínio do ative Directory.

Licencie Global File Cache

Configure o serviço do Global File Cache License Management Server (LMS) em uma instância do Global File Cache Core. Você precisará de suas credenciais NSS ou de um ID de cliente fornecido pela NetApp para ativar sua assinatura.

Implante as instâncias do Global File Cache Edge

"Implantando instâncias do Global File Cache Edge"Consulte para implantar as instâncias do Global File Cache Edge em cada local remoto. Esta etapa não é feita usando o Cloud Manager.

Implante o Cloud Volumes ONTAP como sua plataforma de storage

Na versão atual, o cache global de arquivos oferece suporte ao Cloud Volumes ONTAP implantado no Azure ou na AWS. Para obter pré-requisitos, requisitos e instruções de implantação detalhadas, "Iniciar o Cloud Volumes ONTAP no Azure" consulte ou "Iniciando o Cloud Volumes ONTAP na AWS".

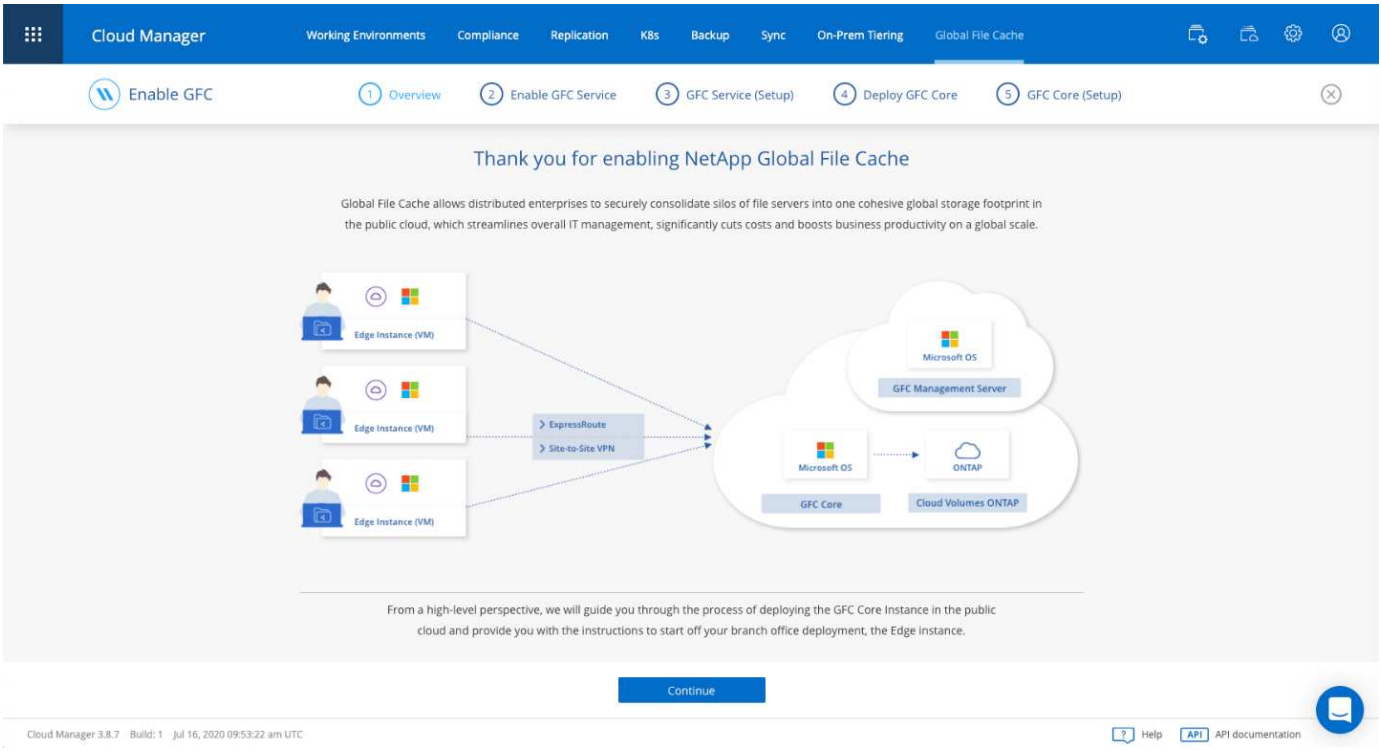
Observe o seguinte requisito adicional Global File Cache:

- Você deve configurar compartilhamentos de arquivo SMB na instância do Cloud Volumes ONTAP.

  Se nenhum compartilhamento de arquivo SMB estiver configurado na instância, você será solicitado a configurar os compartilhamentos SMB durante a instalação dos componentes Global File Cache.

Ative o Global File Cache no seu ambiente de trabalho

O assistente Global File Cache orienta você pelas etapas para implantar a instância do Global File Cache Management Server e a instância Global File Cache Core, conforme destacado abaixo.



Passos

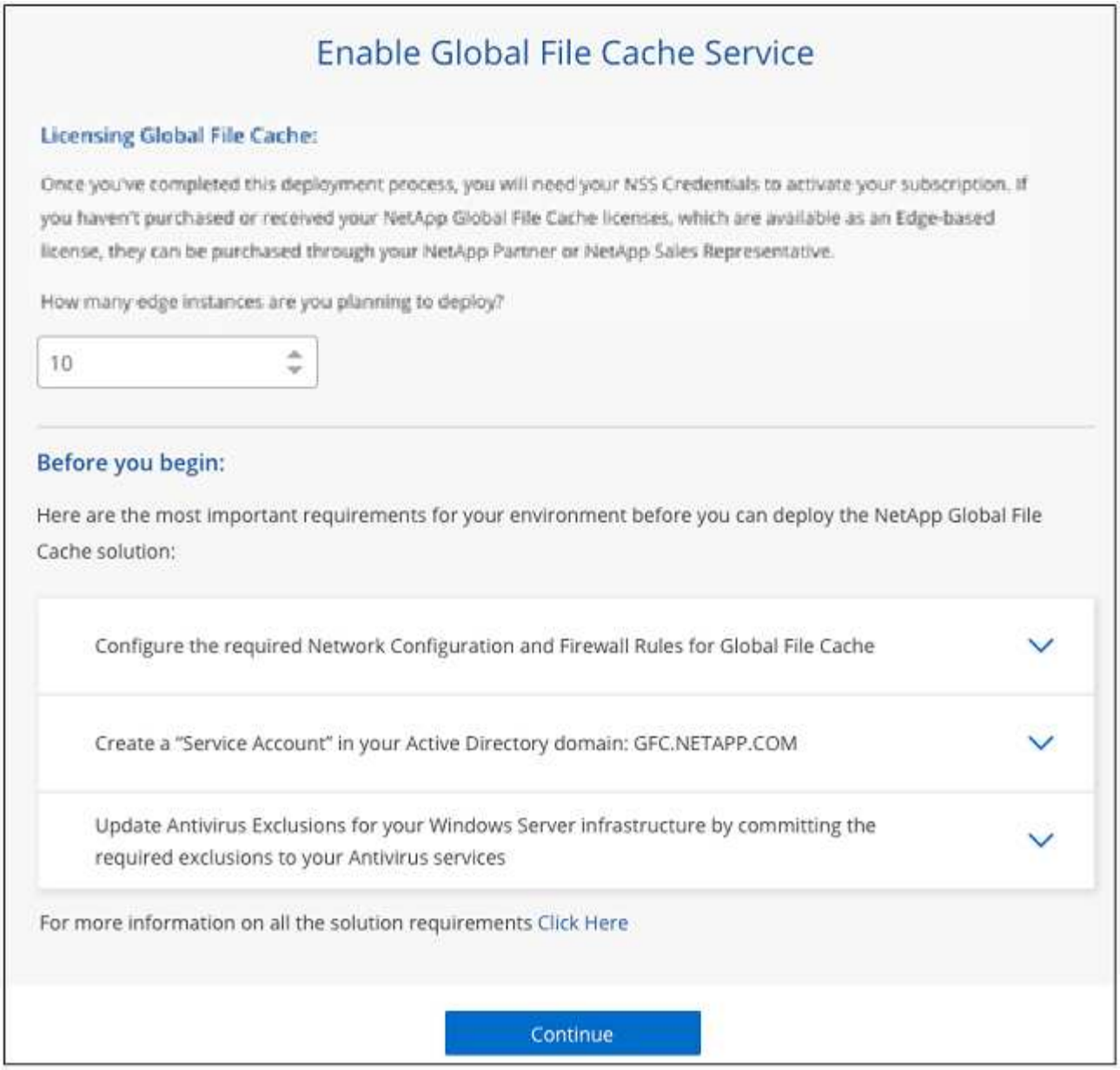
1. Selecione o ambiente de trabalho em que você implantou o Cloud Volumes ONTAP.
2. No painel Serviços, clique em **Ativar GFC**.

3. Leia a página Visão geral e clique em **continuar**.
4. Se nenhum compartilhamento SMB estiver disponível na instância do Cloud Volumes ONTAP, você será solicitado a inserir os detalhes do compartilhamento SMB e SMB para criar o compartilhamento agora.

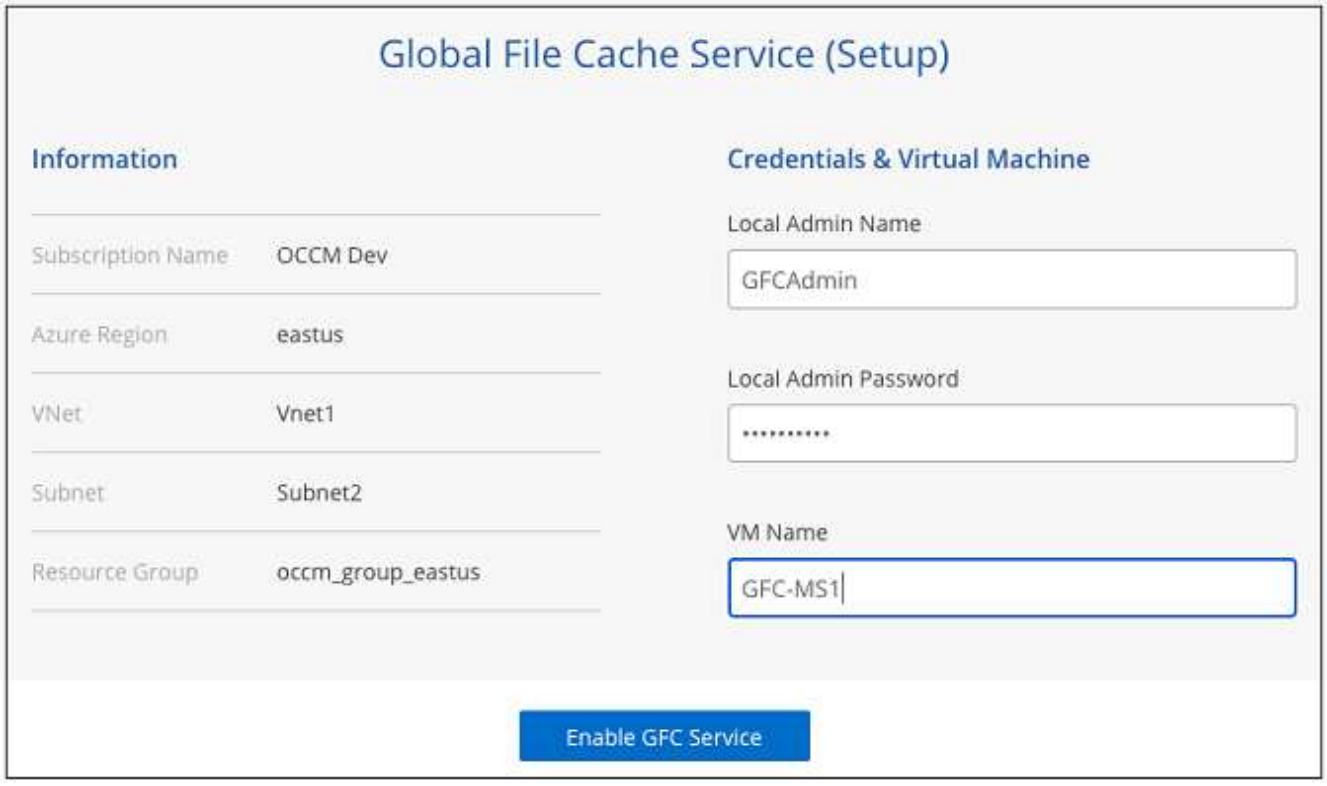
Para obter detalhes sobre a configuração SMB, "Plataforma de storage"consulte .

Quando terminar, clique em **continuar** para criar o compartilhamento SMB.

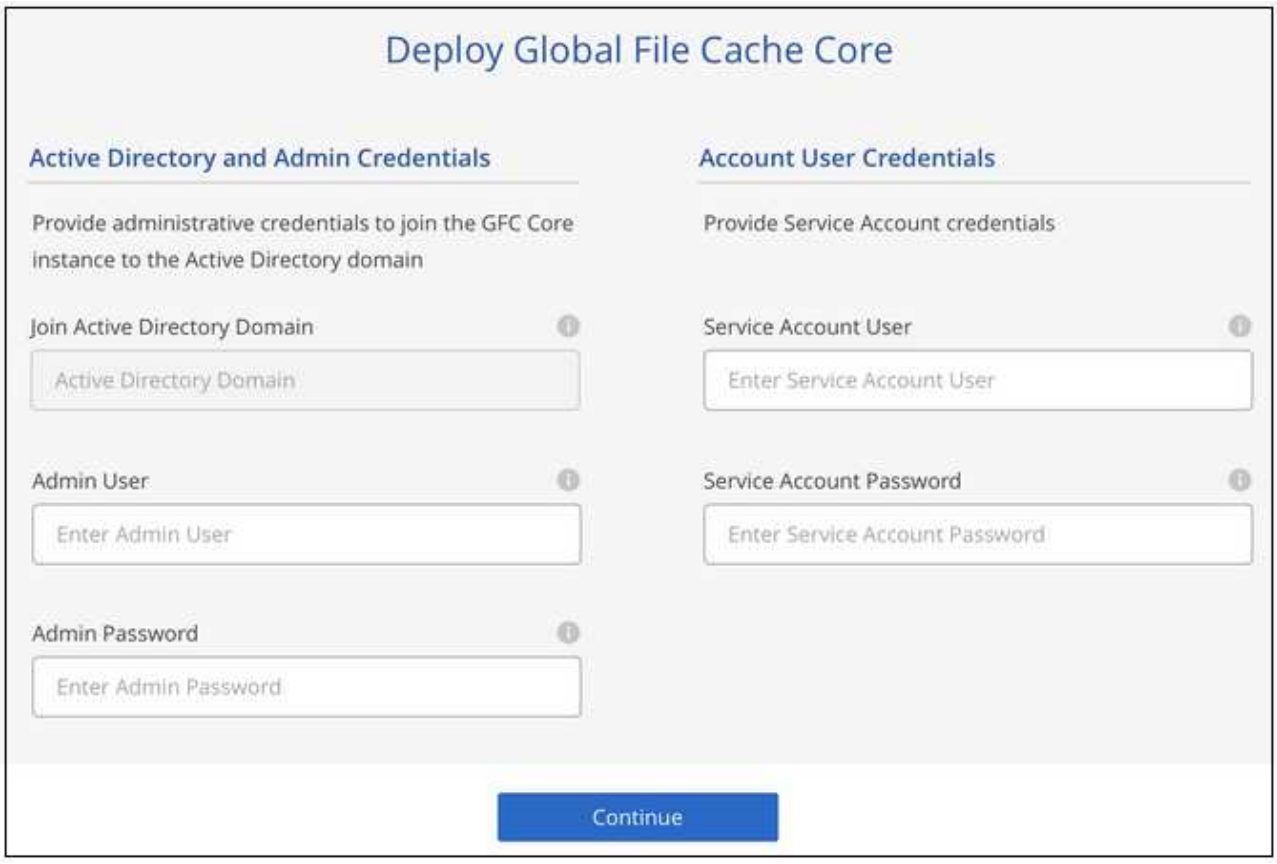
5. Na página Serviço Global de Cache de arquivos, digite o número de instâncias globais de Cache de arquivos que você planeja implantar e verifique se o sistema atende aos requisitos de Configuração de rede e regras de Firewall, configurações do ative Directory e exclusões de antivírus. "Pré-requisitos"Consulte para obter mais detalhes.



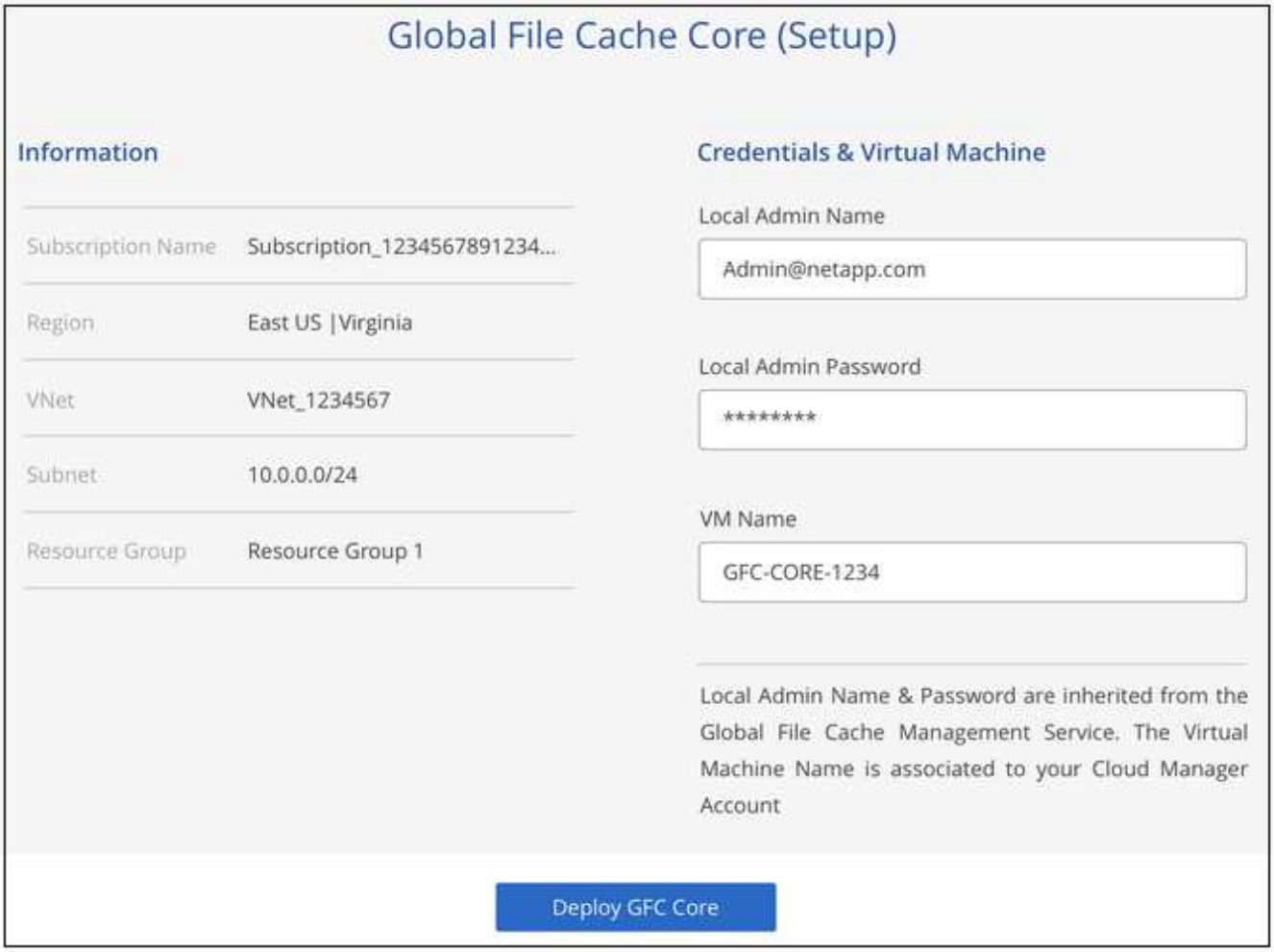
6. Depois de verificar se os requisitos foram atendidos ou se você tem as informações para atender a esses requisitos, clique em **continuar**.
7. Insira as credenciais de administrador que você usará para acessar a VM do Global File Cache Management Server e clique em **Ativar serviço GFC**. Para o Azure, insira as credenciais como nome de usuário e senha; para a AWS, selecione o par de chaves apropriado. Você pode alterar o nome da VM/instância, se desejar.



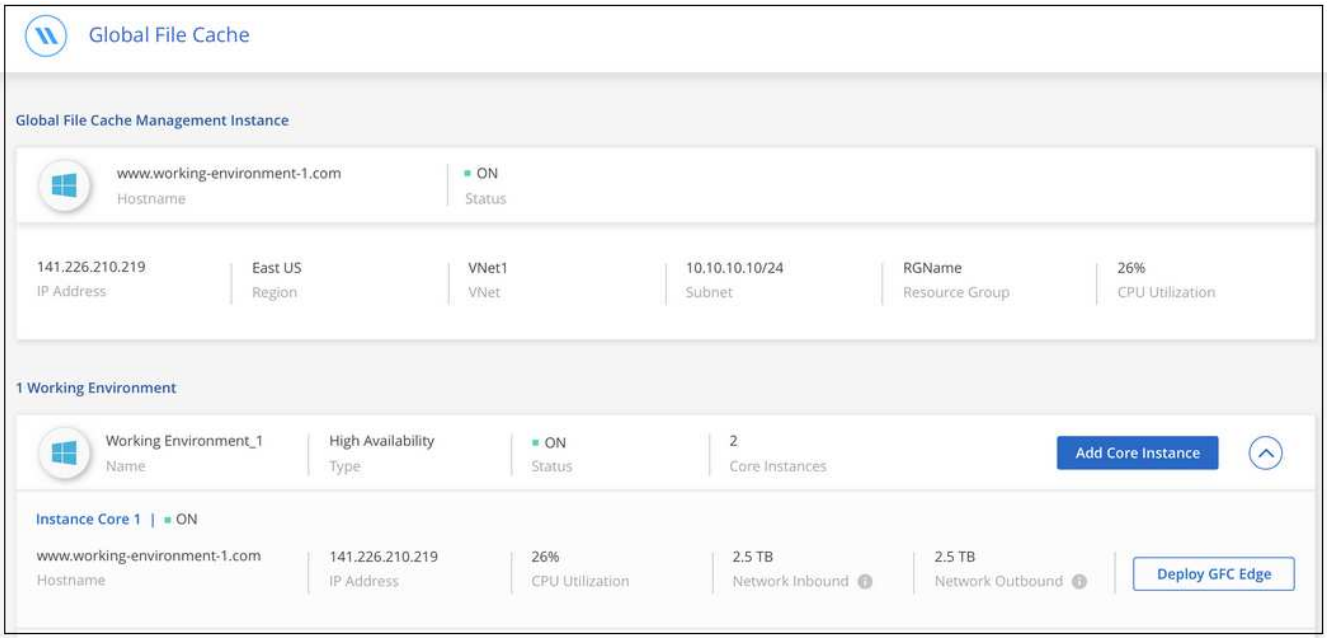
8. Depois que o Serviço Global de Gerenciamento de Cache de Arquivo for implantado com sucesso, clique em **continuar**.
9. Para o Global File Cache Core, insira as credenciais do usuário admin para ingressar no domínio do ative Directory e as credenciais do usuário da conta de serviço. Em seguida, clique em **continuar**.
   - A instância central do cache de arquivos global deve ser implantada no mesmo domínio do ative Directory que a instância do Cloud Volumes ONTAP.
   - A conta de serviço é um usuário de domínio e faz parte do grupo operadores de backup na instância do Cloud Volumes ONTAP.



10. Insira as credenciais de administrador que você usará para acessar a VM Global File Cache Core e clique em **Deploy GFC Core**. Para o Azure, insira as credenciais como nome de usuário e senha; para a AWS, selecione o par de chaves apropriado. Você pode alterar o nome da VM/instância, se desejar.



11. Depois que o Global File Cache Core for implantado com sucesso, clique em **Go to Dashboard**.



O Dashboard mostra que a instância do Management Server e a instância do Core estão **ON** e funcionando.

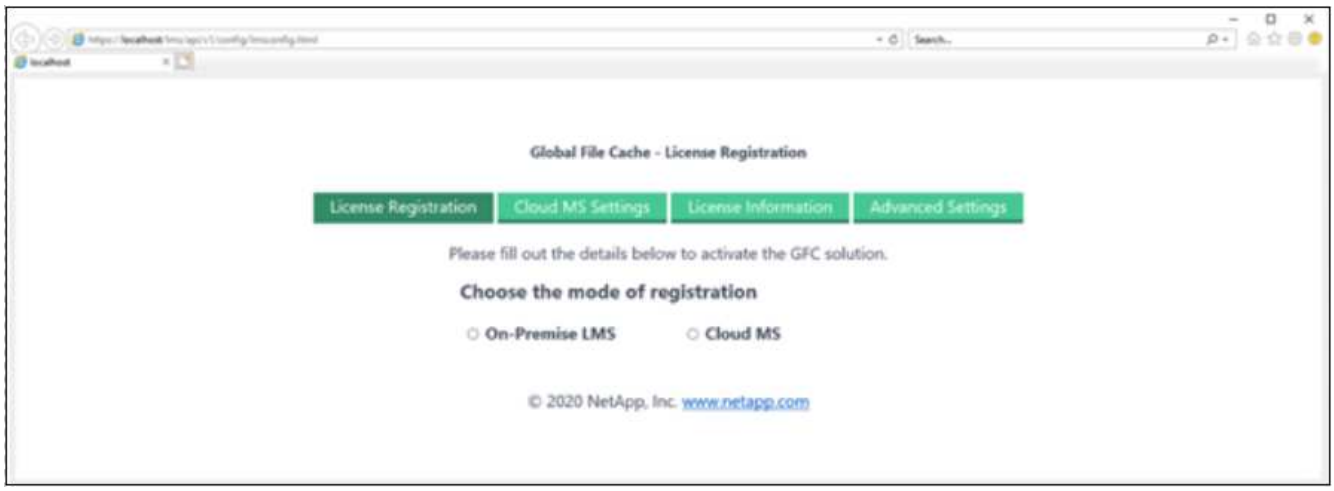
Licencie sua instalação do Global File Cache

Antes de poder usar o Global File Cache, você precisa configurar o serviço Global File Cache License Management Server (LMS) em uma instância Global File Cache Core. Você precisará de suas credenciais NSS ou de uma ID de cliente fornecida NetApp para ativar sua assinatura.

Neste exemplo, configuraremos o serviço LMS em uma instância Core que você acabou de implantar na nuvem pública. Este é um processo único que configura seu serviço LMS.

Passos

1. Abra a página Registro de licença de cache de arquivo global no Global File Cache Core (o núcleo que você está designando como seu serviço LMS) usando o seguinte URL. Substitua *<ip_address>* pelo endereço IP do núcleo global de cache de arquivos: https://<ip_address>/lms/api/v1/config/lmsconfig.html
2. Clique em "continuar para este site (não recomendado)" para continuar. É apresentada uma página que permite configurar o LMS ou verificar as informações de licença existentes.



3. Escolha o modo de Registro selecionando "On-Premise LMS" ou "Cloud MS".
   - "LMS no local" é usado para clientes existentes ou de teste que receberam uma ID de cliente por meio do suporte da NetApp.
   - O "Cloud MS" é usado para clientes que adquiriram licenças de borda de cache de arquivos globais da NetApp da NetApp ou de seus parceiros certificados e que tenham suas credenciais NetApp.
4. Para o Cloud MS, clique em **Cloud MS**, insira suas credenciais NSS e clique em **Enviar**.

5. Para LMS on-premise, clique em **On-Premise LMS**, insira sua ID de cliente e clique em **Register LMS**.

O que vem a seguir?

Se você tiver determinado que precisa implantar vários núcleos de Cache de Arquivo Global para oferecer suporte à sua configuração, clique em **Adicionar instância central** no Painel e siga o assistente de implantação.

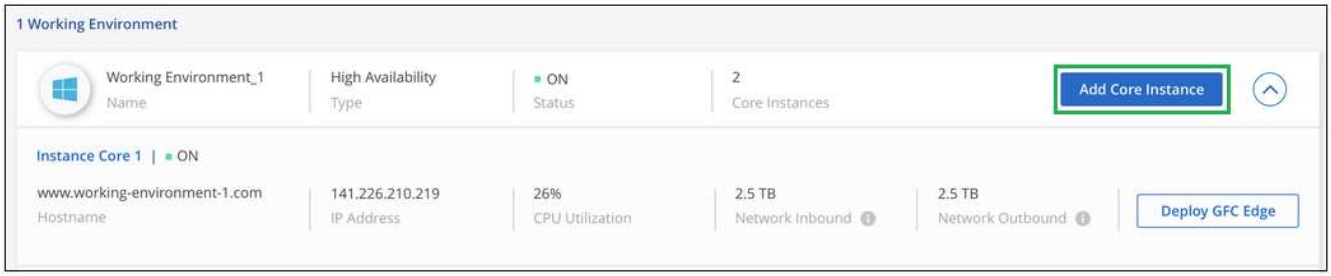
Depois de concluir sua implantação principal, você precisa fazer "Implante as instâncias do Global File Cache Edge" isso em cada um dos escritórios remotos.

Implante instâncias principais adicionais

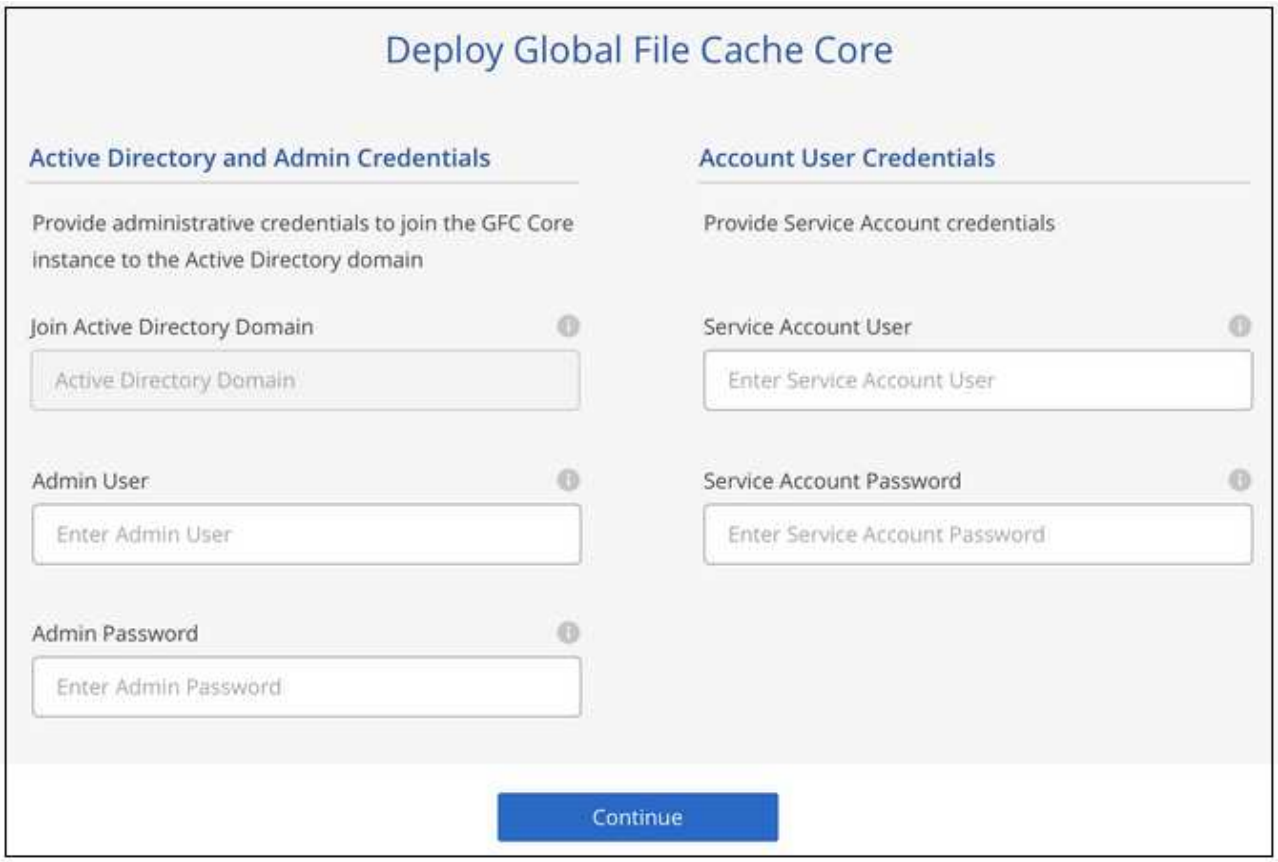
Se a configuração exigir que mais de um Global File Cache Core seja instalado devido a um grande número de instâncias do Edge, você poderá adicionar outro Core ao ambiente de trabalho.

Ao implantar instâncias do Edge, você configurará algumas para se conetar ao primeiro núcleo e outras ao segundo núcleo. Ambas as instâncias principais acessam o mesmo storage de back-end (sua instância do Cloud Volumes ONTAP) no ambiente de trabalho.

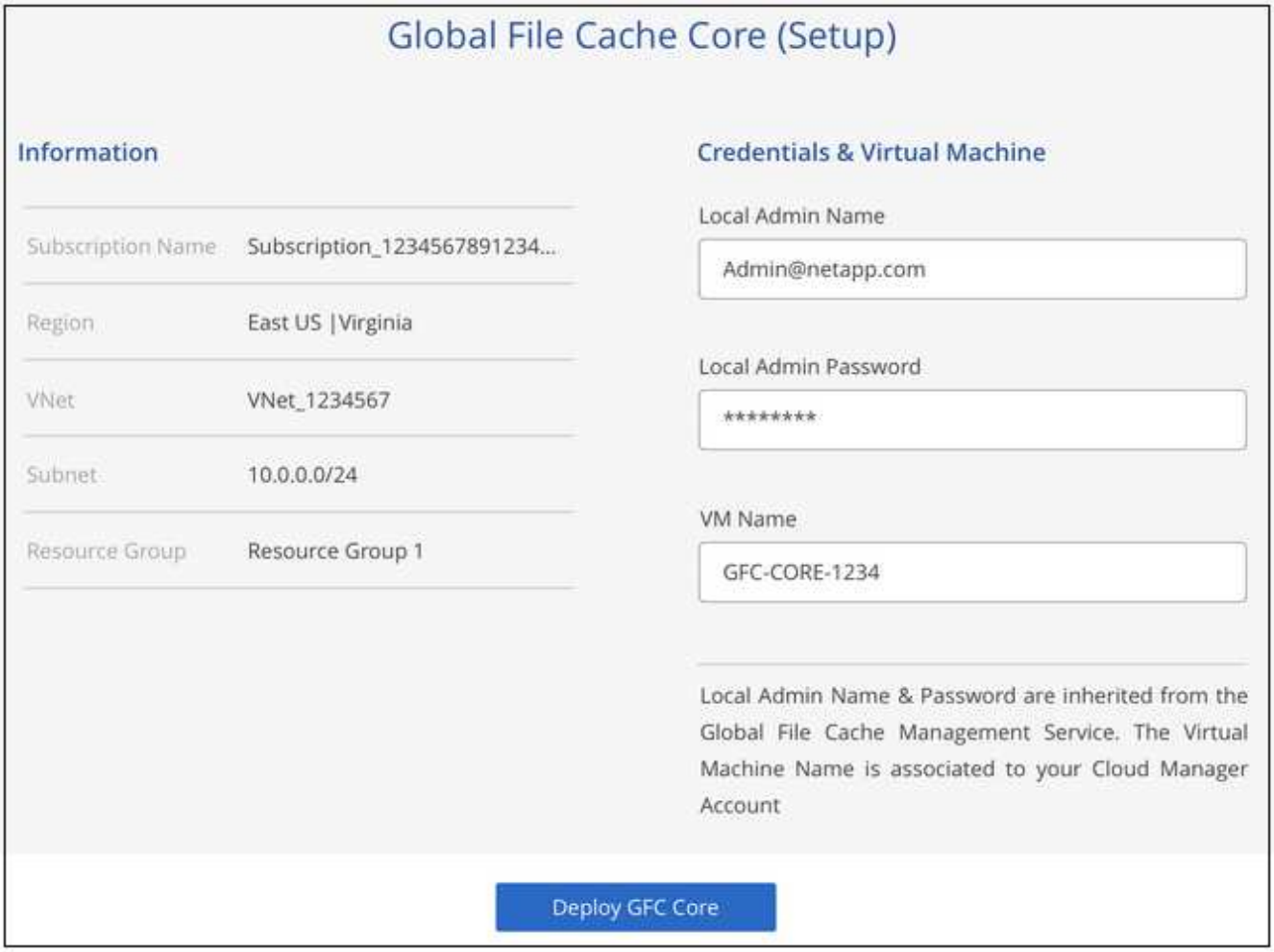
1. No Painel Global File Cache, clique em **Add Core Instance**.



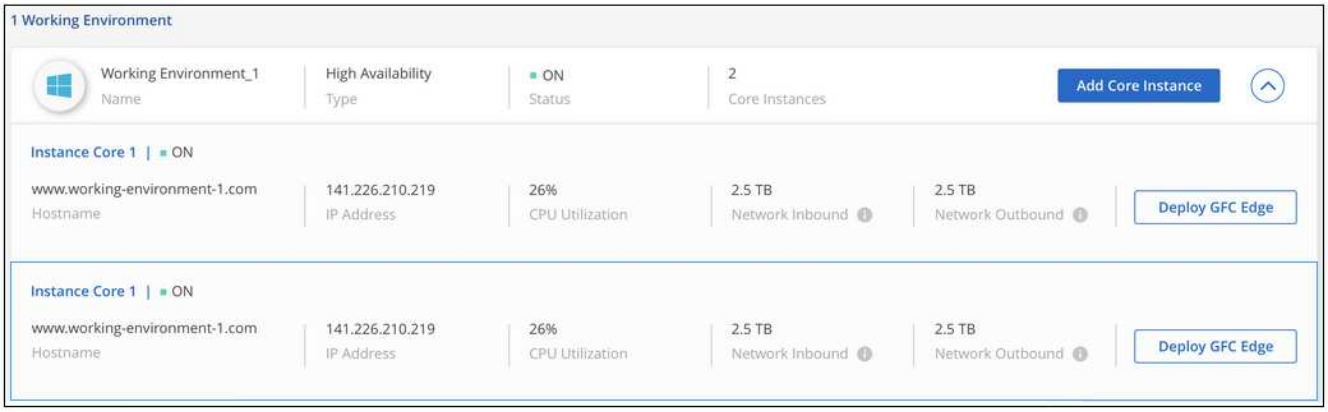
2. Insira as credenciais de usuário admin para ingressar no domínio ative Directory e as credenciais de usuário da conta de serviço. Em seguida, clique em **continuar**.
   - A instância central do cache de arquivos global deve estar no mesmo domínio do ative Directory que a instância do Cloud Volumes ONTAP.
   - A conta de serviço é um usuário de domínio e faz parte do grupo operadores de backup na instância do Cloud Volumes ONTAP.



3. Insira as credenciais de administrador que você usará para acessar a VM Global File Cache Core e clique em **Deploy GFC Core**. Para o Azure, insira as credenciais como nome de usuário e senha; para a AWS, selecione o par de chaves apropriado. Você pode alterar o nome da VM, se desejar.



4. Depois que o Global File Cache Core for implantado com sucesso, clique em **Go to Dashboard**.



O Dashboard reflete a segunda instância do Core para o ambiente de trabalho.

Antes de começar a implantar instâncias do Global File Cache Edge

Há muitos requisitos que você precisa estar ciente antes de começar a instalar o software Global File Cache Edge em seus escritórios remotos.

Faça o download dos recursos necessários

Baixe os modelos virtuais Global File Cache que você está planejando usar em suas filiais, o pacote de instalação de software e documentação de referência adicional:

- Modelo virtual do Windows Server 2016:

  "Windows Server 2016 .OVA incluindo NetApp GFC (VMware vSphere 6,5 ou superior)" "Windows Server 2016 .VHDX incluindo NetApp GFC (Microsoft Hyper-v)"

- Modelo virtual do Windows Server 2019:

  "Windows Server 2019 .OVA incluindo NetApp GFC (VMware vSphere 6,5 ou superior)" "Windows Server 2019 .VHDX incluindo NetApp GFC (Microsoft Hyper-v)"

- Software global File Cache Edge:

  "Software NetApp GFC (.EXE)"

- Documentação Global File Cache:

  "Guia do usuário do cache global de arquivos da NetApp"

Projetando e implantando o Global File Cache Edge

Dependendo dos seus requisitos, talvez seja necessário implantar uma ou várias instâncias do Global File Cache Edge com base nas sessões de usuário simultâneas em uma filial. A instância do Edge apresenta o compartilhamento de arquivos virtual aos usuários finais dentro da filial, que foi estendido de forma transparente a partir da instância associada do Global File Cache Core. O Global File Cache Edge deve conter um `D:\` volume NTFS, que contém os arquivos armazenados em cache dentro da filial.

> Para o Global File Cache Edge, é importante entender o "diretrizes de dimensionamento". Isso ajudará você a criar o design correto para sua implantação Global File Cache. Você também precisaria determinar o que é certo para o seu ambiente em termos de escala, disponibilidade de recursos e redundância.

Instância do Global File Cache Edge

Ao implantar uma instância do Global File Cache Edge, você precisa provisionar uma única VM, seja implantando o Windows Server 2016 Standard ou Datacenter Edition, ou o Windows Server 2019 Standard ou Datacenter Edition, ou usando o Global File Cache `.OVA` ou `.VHD` modelo, que inclui o sistema operacional Windows Server de sua escolha e o software Global File Cache.

Passos rápidos

1. Implante o modelo Virtual Global File Cache ou a VM do Windows Server 2016 ou a edição Standard ou Datacenter do Windows Server 2019.
2. Verifique se a VM está conetada à rede, conetada ao domínio e acessível por meio do RDP.
3. Instale o software Global File Cache Edge mais recente.
4. Identifique a instância Global File Cache Management Server e Core.
5. Configure a instância do Global File Cache Edge.

Requisitos de borda de cache de arquivos global

O Global File Cache Edge foi projetado para funcionar em todas as plataformas compatíveis com o Windows Server 2016 e 2019, trazendo TI simplificada para escritórios remotos corporativos e além. Criticamente, o Global File Cache pode ser implantado em sua infraestrutura de hardware, virtualização ou ambientes de nuvem híbrida/pública existentes em quase todos os casos, se eles atenderem a alguns requisitos de nível básico.

O Global File Cache Edge requer os seguintes recursos de hardware e software para funcionar de forma otimizada. Para obter mais informações sobre as diretrizes gerais de dimensionamento, "Diretrizes de dimensionamento"consulte .

Dispositivo de servidor endurecido

O pacote de instalação Global File Cache cria um dispositivo de software endurecido em qualquer instância do Microsoft Windows Server. *Não desinstalar* o pacote Global File Cache. A desinstalação do Global File Cache afetará a funcionalidade da instância do servidor e pode exigir uma reconstrução completa da instância do servidor.

Requisitos físicos de hardware

- Mínimo de 4 núcleos de CPU
- Mínimo de 16 GB de RAM
- NIC dedicada única ou redundante de 1 Gbps
- HDD ou SSD SAS de 10K RPM (preferido)
- Controlador RAID com funcionalidade de armazenamento em cache write-back ativada

Requisitos de implantação virtual

Sabe-se que as plataformas de hipervisor estão sujeitas a degradação do desempenho da perspetiva do subsistema de storage (por exemplo, latência). Para um desempenho ideal usando o Global File Cache, recomenda-se uma instância de servidor físico com SSD.

Para obter a melhor performance em ambientes virtuais, além dos requisitos de host físico, os seguintes requisitos e reservas de recursos devem ser atendidos:

Microsoft Hyper-V 2012 R2 e posterior:

- Processador (CPU): As CPUs devem ser definidas como **Static**: Mínimo: 4 núcleos vCPU.
- Memória (RAM): Mínimo: 16 GB definido como **estático**.
- Provisionamento de disco rígido: Os discos rígidos devem ser configurados como **Fixed Disk**.

VMware vSphere 6.x e posterior:

- Processador (CPU): A reserva de ciclos de CPU deve ser definida. Mínimo: 4 núcleos vCPU a 10000 MHz.
- Memória (RAM): Mínimo: Reserva de 16 GB.
- Provisionamento de disco rígido:
  - O provisionamento de disco deve ser definido como **thick provisioned eager zerado**.
  - As partilhas do disco rígido têm de ser definidas para **High**.

    - Devices.hotplug deve ser definido como **False** usando o vSphere Client para impedir que o Microsoft Windows apresente unidades de Cache de Arquivo Global como removíveis.
- Rede: A interface de rede deve ser definida como **VMXNET3** (requer ferramentas de VM).

O Global File Cache é executado no Windows Server 2016 e 2019, portanto, a plataforma de virtualização precisa suportar o sistema operacional, bem como a integração com utilitários que melhoram o desempenho do sistema operacional convidado da VM e o gerenciamento da VM, como as Ferramentas da VM.

Requisitos de dimensionamento da partição

- C: - Mínimo 250GB (volume do sistema/arranque)
- D: - Mínimo 1TB (volume de dados separado para Cache de Arquivo Global Intelligent File Cache*)

*O tamanho mínimo é 2xx o conjunto de dados ativo. O volume de cache (D:) pode ser estendido e só é restringido pelas limitações do sistema de arquivos Microsoft Windows NTFS.

Requisitos de disco de Cache de arquivos inteligente Global File Cache

A latência do disco no disco de Cache de Arquivo Inteligente (D:) do Global File Cache deve fornecer latência média de disco de e/S inferior a 0,5ms ms e taxa de transferência de 1MiBps Gbps por usuário simultâneo.

Para obter mais informações, consulte "Guia do usuário do cache global de arquivos da NetApp".

Rede

- Firewall: As portas TCP devem ser permitidas entre a borda do Cache Global de arquivos e as instâncias do Management Server e Core.

  Portas TCP: 443 (HTTPS - LMS), 6618 – 6630.

- Os dispositivos de otimização de rede (como Riverbed Steelhead) devem ser configurados para passar por portas específicas do Global File Cache (TCP 6618-6630).

Práticas recomendadas para workstation e aplicativos do cliente

O Global File Cache integra-se de forma transparente aos ambientes do cliente, permitindo que os usuários acessem dados centralizados usando suas estações de trabalho cliente, executando aplicativos empresariais. Usando o Global File Cache, os dados são acessados por meio de um mapeamento de unidade direta ou por meio de um namespace DFS. Para obter mais informações sobre o Global File Cache Fabric, Intelligent File Caching e os principais aspetos do software, consulte a "Antes de começar a implantar o Global File Cache" seção.

Para garantir uma experiência e desempenho ideais, é importante cumprir os requisitos e as práticas recomendadas do Microsoft Windows Client, conforme descrito no Guia do Usuário do Global File Cache. Isso se aplica a todas as versões do Microsoft Windows.

Para obter mais informações, consulte "Guia do usuário do cache global de arquivos da NetApp".

Melhores práticas de firewall e antivírus

Embora o Global File Cache faça um esforço razoável para validar que os pacotes de aplicativos antivírus mais comuns são compatíveis com o Global File Cache, a NetApp não pode garantir e não é responsável por quaisquer incompatibilidades ou problemas de desempenho causados por esses programas, ou por suas atualizações, Service packs ou modificações associadas.

O Global File Cache não recomenda a instalação nem o aplicativo de soluções de monitoramento ou antivírus em qualquer instância habilitada pelo Global File Cache (Core ou Edge). Se uma solução for instalada, por escolha ou por política, as práticas recomendadas e recomendações a seguir devem ser aplicadas. Para obter pacotes de antivírus comuns, consulte o Apêndice A "Guia do usuário do cache global de arquivos da NetApp"no .

Definições da firewall

- Firewall da Microsoft:
  - Guarde as definições de firewall como predefinição.
  - Recomendação: Deixe as configurações e os serviços do firewall da Microsoft na configuração padrão de OFF e não iniciado para instâncias padrão do Global File Cache Edge.
  - Recomendação: Deixe as configurações e os serviços do firewall da Microsoft na configuração padrão de ATIVADO e iniciado para instâncias do Edge que também executam a função controlador de domínio.
- Firewall corporativo:
  - A instância do Global File Cache Core escuta nas portas TCP 6618-6630, certifique-se de que as instâncias do Global File Cache Edge possam se conetar a essas portas TCP.
  - As instâncias de cache de arquivos globais exigem comunicações com o servidor de gerenciamento de cache de arquivos global na porta TCP 443 (HTTPS).
- As soluções/dispositivos de otimização de rede devem ser configurados para passar por portas específicas do Global File Cache.

Práticas recomendadas de antivírus

Esta seção ajuda você a entender os requisitos ao executar um software antivírus em uma instância do Windows Server executando o Global File Cache. O Global File Cache testou os produtos antivírus mais usados, incluindo Cylance, McAfee, Symantec, Sophos, Trend Micro, Kaspersky e Windows Defender, para uso em conjunto com o Global File Cache.

Adicionar antivírus a um dispositivo Edge pode introduzir um impactos de 10 a 20% no desempenho do usuário.

Para obter mais informações, consulte "Guia do usuário do cache global de arquivos da NetApp".

Configurar exclusões

O software antivírus ou outros utilitários de indexação ou verificação de terceiros nunca devem verificar a unidade D: Na instância do Edge. Essas verificações da unidade D do servidor Edge resultarão em inúmeras solicitações de abertura de arquivo para todo o namespace do cache. Isso resultará em buscas de arquivos pela WAN para que todos os servidores de arquivos sejam otimizados no data center. O alagamento de conexão WAN e a carga desnecessária na instância do Edge ocorrerão, resultando na degradação do desempenho.

Além da unidade D: ', o seguinte diretório e processos Global File Cache devem geralmente ser excluídos de todos os aplicativos antivírus:

- `C:\Program Files\TalonFAST\`
- `C:\Program Files\TalonFAST\Bin\LMClientService.exe`

- `C:\Program Files\TalonFAST\Bin\LMServerService.exe`
- `C:\Program Files\TalonFAST\Bin\Optimus.exe`
- `C:\Program Files\TalonFAST\Bin\tafsexport.exe`
- `C:\Program Files\TalonFAST\Bin\tafsutils.exe`
- `C:\Program Files\TalonFAST\Bin\tapp.exe`
- `C:\Program Files\TalonFAST\Bin\tfs.exe`
- `C:\Program Files\TalonFAST\Bin\TService.exe`
- `C:\Program Files\TalonFAST\Bin\tum.exe`
- `C:\Program Files\TalonFAST\FastDebugLogs\`
- `C:\Windows\System32\drivers\tfast.sys`
- `\\?\TafsMtPt:\ or \\?\TafsMtPt*`
- `\Device\TalonCacheFS\`
- `\\?\GLOBALROOT\Device\TalonCacheFS\`
- `\\?\GLOBALROOT\Device\TalonCacheFS\*`

Política de suporte da NetApp

As instâncias globais de Cache de arquivos são projetadas especificamente para Global File Cache como o aplicativo principal executado em uma plataforma Windows Server 2016 e 2019. O Global File Cache requer acesso prioritário aos recursos da plataforma, por exemplo, disco, memória, interfaces de rede, e pode colocar altas demandas sobre esses recursos. As implantações virtuais exigem reservas de memória/CPU e discos de alta performance.

- Para implantações de filiais do Global File Cache, os serviços e aplicativos suportados no servidor que executa o Global File Cache estão limitados a:
  - DNS/DHCP
  - Controlador de domínio do ative Directory (o Global File Cache deve estar em um volume separado)
  - Serviços de impressão
  - Microsoft System Center Configuration Manager (SCCM)
  - Agentes do sistema do lado do cliente e aplicativos antivírus aprovados pela Global File Cache
- O suporte e a manutenção da NetApp se aplicam somente ao cache global de arquivos.
- O software de produtividade de linha de negócios, que normalmente consome recursos, por exemplo, servidores de banco de dados, servidores de e-mail e assim por diante, não é suportado.
- O cliente é responsável por qualquer software não Global File Cache que possa ser instalado no servidor que executa o Global File Cache:
  - Se qualquer pacote de software de terceiros causar conflitos de software ou recursos com o Global File Cache ou o desempenho estiver comprometido, a organização de suporte do Global File Cache pode exigir que o cliente desative ou remova o software do servidor que executa o Global File Cache.
  - É responsabilidade do cliente por toda a instalação, integração, suporte e atualização de qualquer software adicionado ao servidor que executa o aplicativo Global File Cache.
- Utilitários/agentes de gerenciamento de sistemas, como ferramentas antivírus e agentes de licenciamento,

podem ser capazes de coexistir. No entanto, exceto para os serviços e aplicativos suportados listados acima, esses aplicativos não são suportados pelo Global File Cache e as mesmas diretrizes acima ainda devem ser seguidas:

- É responsabilidade do cliente por toda a instalação, integração, suporte e atualização de qualquer software adicionado.
- Se um cliente instalar qualquer pacote de software de terceiros que cause ou suspeite estar causando conflitos de software ou recursos com o Global File Cache ou o desempenho estiver comprometido, talvez haja um requisito da organização de suporte do Global File Cache para desativar/remover o software.

Implantar instâncias do Global File Cache Edge

Depois de verificar se o seu ambiente atende a todos os requisitos, instale o software Global File Cache Edge em cada escritório remoto.

Antes de começar

Para concluir as tarefas de configuração do Global File Cache Edge, você precisa das seguintes informações:

- Endereços IP estáticos para cada instância do Global File Cache
- Máscara de sub-rede
- Endereço IP do gateway
- O FQDN que você deseja atribuir a cada servidor Global File Cache
- O sufixo DNS (opcional)
- O nome de usuário e a senha de um usuário administrativo no domínio
- O FQDN e/ou o endereço IP dos servidores Core associados
- Um volume a ser usado como Intelligent File Cache. Recomenda-se que este seja pelo menos 2x do tamanho do conjunto de dados ativo. Isso deve ser formatado como NTFS e atribuído como `D:\`.

Portas TCP comumente usadas

Existem várias portas TCP usadas pelos serviços Global File Cache. É obrigatório que os dispositivos possam se comunicar nessas portas e eles sejam excluídos de quaisquer dispositivos de otimização de WAN ou políticas de restrição de firewall:

- Porta TCP de licenciamento de Cache de arquivos global: 443
- Portas TCP de Cache de arquivos globais: 6618-6630

Implante o modelo virtual Global File Cache

O modelo virtual `.OVA`e `.VHD` as imagens) contêm a versão mais recente do software Global File Cache. Se você estiver implantando o Global File Cache usando o `.OVA` modelo de máquina virtual (VM) ou `.VHD` o modelo de máquina virtual (VM), siga as etapas descritas nesta seção. Supõe-se que você entenda como implantar o `.OVA` modelo ou `.VHD` na plataforma de hypervisor designada.

Certifique-se de que as preferências de VM, incluindo reservas de recursos, estejam de acordo com os requisitos descritos na "Requisitos de implantação virtual".

Passos

1. Extraia o pacote do modelo que você baixou.
2. Implante o modelo virtual. Consulte os vídeos a seguir antes de iniciar a implantação:
   - "Implante o modelo virtual no VMware"
   - "Implante o modelo Virtual no Hyper-V."
3. Depois que o modelo virtual tiver sido implantado e você tiver configurado as configurações da VM, inicie a VM.
4. Durante a inicialização inicial, quando o sistema operacional Windows Server 2016 ou 2019 estiver se preparando para a primeira utilização, conclua a experiência pronta para uso instalando os drivers corretos e instalando os componentes necessários para o respetivo hardware.
5. Quando a instalação básica da instância do Global File Cache Edge for concluída, o sistema operacional Windows Server 2016 ou 2019 o guiará por meio de um assistente de configuração inicial para configurar especificações do sistema operacional, como localização e chave do produto.
6. Após a conclusão do assistente de configuração inicial, efetue login localmente no sistema operacional Windows Server 2016 ou 2019 com as seguintes credenciais:
   - Nome de usuário: **FASTAdmin**
   - Senha: **Tal0nFAST!**
7. Configure a VM do Windows Server, entre no domínio do ative Directory da organização e prossiga para a seção de configuração do Global File Cache Edge.

Configure a instância do Global File Cache Edge

A instância do Global File Cache Edge se coneta a um Global File Cache Core para fornecer aos usuários da filial acesso aos recursos do servidor de arquivos do data center.

> A instância do Edge deve ser licenciada como parte da implantação do Cloud Volumes ONTAP antes de iniciar a configuração. Consulte "Licenciamento" para obter mais informações sobre licenciamento.

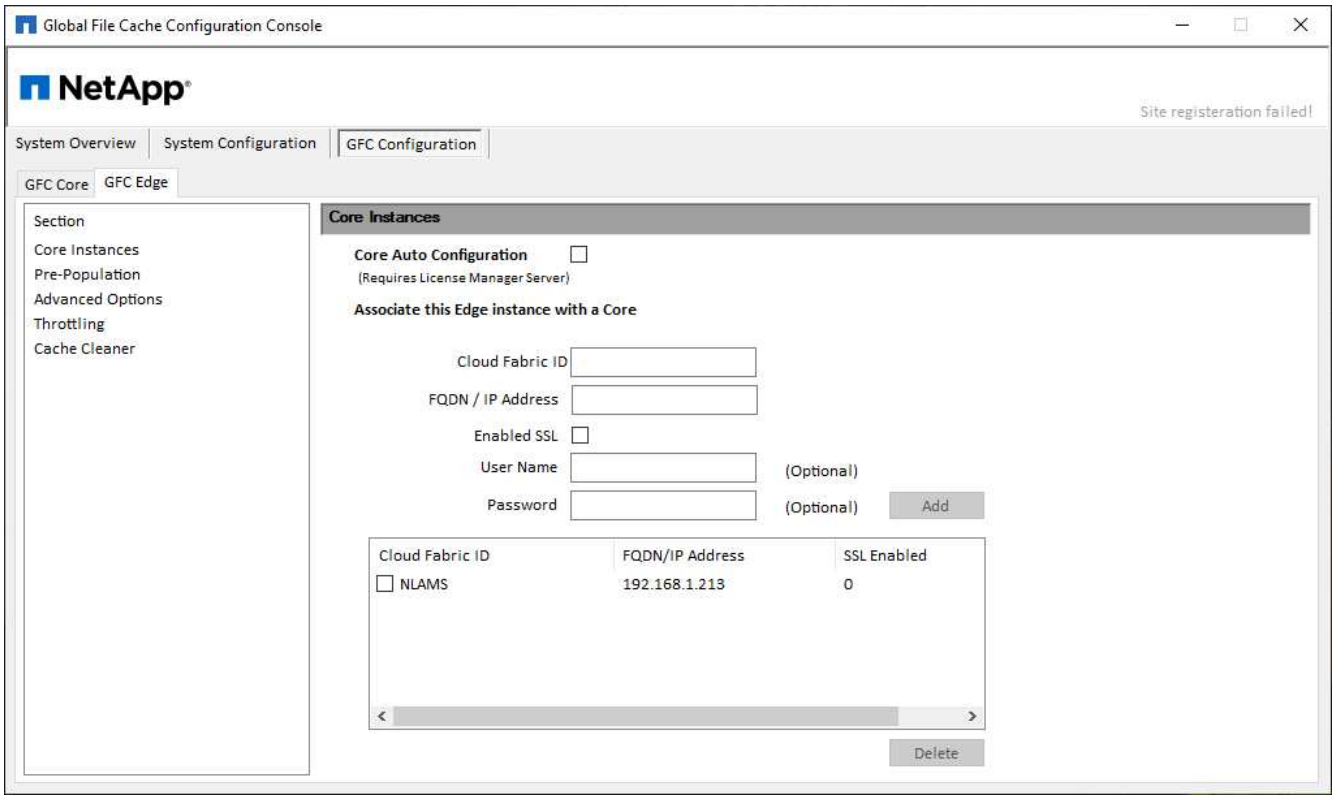
Se a sua configuração exigir que mais de um Global File Cache Core seja instalado devido a um grande número de instâncias do Edge, você configurará algumas instâncias do Edge para se conetar ao primeiro Core e outras para se conetar ao segundo Core. Verifique se você tem o FQDN ou o endereço IP e outras informações necessárias para a instância Core correta.

Para configurar a instância do Edge, execute as seguintes etapas:

Passos

1. Clique em **Perform** ao lado da etapa de Configuração do núcleo desmarcada listada na seção "etapas de configuração do Edge" do assistente de configuração inicial. Isso abre uma nova guia, o GFC Edge, e mostra a seção *Core Instances*.
2. Forneça o **ID do Cloud Fabric** do servidor Global File Cache Core. O ID do Cloud Fabric é normalmente o nome NetBIOS ou a localização geográfica do servidor de arquivos back-end.
3. Forneça o **Endereço FQDN/IP** do servidor Global File Cache Core:
   a. (Opcional) Marque a caixa **SSL** para habilitar o suporte SSL para criptografia aprimorada do Edge ao Core.
   b. Introduza o Nome de utilizador e a Palavra-passe, que são as credenciais da conta de serviço utilizada no núcleo.

4. Clique em **Add** para confirmar a adição do dispositivo Global File Cache Core. Será apresentada uma caixa de confirmação. Clique em **OK** para descartá-lo.



Atualize o software Global File Cache Edge

O Global File Cache frequentemente libera atualizações do software, seja patches, aprimoramentos ou novos recursos/funcionalidades. Embora o modelo virtual (`.OVA`e `.VHD` as imagens) contenham a versão mais recente do software Cache de arquivos global, é possível que uma versão mais recente esteja disponível no portal de download do suporte da NetApp.

Certifique-se de que suas instâncias do Global File Cache estão atualizadas com a versão mais recente.

Este pacote de software também pode ser usado para instalações impecáveis no Microsoft Windows Server 2016 Standard ou Datacenter Edition, ou Windows Server 2019 Standard ou Datacenter Edition, ou usado como parte de sua estratégia de atualização.

Abaixo você pode encontrar os passos necessários para atualizar o pacote de instalação do Global File Cache:

Passos

1. Depois de salvar o pacote de instalação mais recente na instância desejada do Windows Server, clique duas vezes nele para executar o executável de instalação.
2. Clique em **seguinte** para continuar o processo.
3. Clique em **seguinte** para continuar.
4. Aceite o Contrato de Licenciamento e clique em **seguinte**.
5. Selecione a localização de destino de instalação pretendida.

O NetApp recomenda que o local de instalação padrão seja usado.

6. Clique em **seguinte** para continuar.
7. Selecione a pasta do menu Iniciar.
8. Clique em **seguinte** para continuar.
9. Verifique os parâmetros de instalação desejados e clique em **Install** para iniciar a instalação.

   O processo de instalação será executado.

10. Após a conclusão da instalação, reinicie o servidor quando solicitado.

O que se segue?

Para obter detalhes sobre a configuração avançada do Global File Cache Edge, consulte "Guia do usuário do cache global de arquivos da NetApp".

Treinamento do usuário final

Você vai querer treinar seus usuários sobre as práticas recomendadas para acessar os arquivos compartilhados por meio do Global File Cache.

Esta é a fase final da implantação do Global File Cache, a fase de implementação do usuário final.

A fim de preparar e simplificar o processo de integração do usuário final, use o modelo de e-mail abaixo que irá ajudá-lo a educar os usuários finais sobre o que significa trabalhar em um ambiente de "dados centrais". Isso ajudará seus usuários a aproveitar todos os benefícios da solução Global File Cache. Nós também publicamos um vídeo que pode ser compartilhado para "treinar" usuários quando necessário.

Personalize e encaminhe os seguintes recursos aos usuários finais para prepará-los para implementação:

- Vídeo de formação do utilizador "Vídeo de formação do utilizador final"
- Modelo de e-mail "Modelo de e-mail do Mac (.emltpl)"

  "Modelo de e-mail do Windows (.msg)"

- Comunicações de integração "Documento do Word (.docx)"

Consulte o Capítulo 12 no "Guia do usuário do cache global de arquivos da NetApp"para obter material adicional.

Informações adicionais

Use os links a seguir para saber mais sobre o cache de arquivos global e outros produtos da NetApp:

- Perguntas frequentes sobre o Global File Cache
  - Veja uma lista de perguntas e respostas frequentes "aqui"
- "Guia do usuário do cache global de arquivos da NetApp"
- Documentação do produto NetApp
  - Consulte a documentação adicional para os produtos de nuvem da NetApp "aqui"

    - Consulte a documentação adicional para todos os produtos NetApp "aqui"
- O suporte ao cliente para usuários globais de cache de arquivos com Cloud Volumes ONTAP está disponível através destes canais:
    - Resolução de problemas guiada, gerenciamento de casos, base de conhecimento, downloads, ferramentas e muito mais GO "aqui"
    - Faça login no suporte da NetApp em https://mysupport.netapp.com com suas credenciais NSS
    - Para obter assistência imediata para um número de telefone P1: 856.481.3990 (opção 2)
- O suporte ao cliente para usuários de cache de arquivos global que utilizam o Cloud volumes Services e o Azure NetApp Files está disponível por meio do suporte padrão do seu fornecedor. Entre em Contato com o suporte ao cliente Google ou com o suporte ao cliente Microsoft, respetivamente.

Otimizar os custos de computação em nuvem

Saiba mais sobre o serviço Compute

Ao aproveitar "Serviço Cloud Analyzer da Spot"o , o Cloud Manager pode fornecer uma análise de custos de alto nível dos seus gastos com computação em nuvem e identificar possíveis economias.

O Cloud Analyzer é uma solução de gerenciamento de infraestrutura de nuvem que usa análises avançadas para fornecer visibilidade e insights sobre os custos da nuvem. Ele mostra onde você pode otimizar esses custos e permite implementar essa otimização usando o portfólio de produtos de otimização contínua da Spot em apenas alguns cliques.

Caraterísticas

- Uma análise de custos que mostra o custo atual do mês, os custos mensais projetados e as economias perdidas
- Uma visão da eficiência de gastos por conta, incluindo as economias adicionais estimadas
- Um link para o Cloud Analyzer do Spot para obter detalhes mais detalhados sobre os gastos de todas as contas

Fornecedores de nuvem compatíveis

Esse serviço é compatível com a AWS.

Custo

Não há nenhum custo para usar esse serviço por meio do Cloud Manager.

Como o Cloud Analyzer funciona com o Cloud Manager

Em um alto nível, a integração do Cloud Analyzer com o Cloud Manager funciona assim:

1. Você clica em **Compute** e coneta sua conta do pagador principal da AWS.
2. O NetApp configura seu ambiente da seguinte forma:
   a. Cria uma organização na plataforma Spot.
   b. Envia um e-mail para recebê-lo no Spot.

      Você pode fazer login no serviço Spot usando as mesmas credenciais de logon único usadas com o Cloud Central e o Cloud Manager.

   c. O Cloud Analyzer começa a processar os dados da sua conta da AWS.
3. No Cloud Manager, a página Compute é atualizada e você usa as informações para obter insights sobre os custos de nuvem passados, atuais e futuros.
4. Clique em **Obtenha análise completa** a qualquer momento para acessar o Spot's Cloud Analyzer, que fornece uma análise completa dos seus gastos em nuvem e oportunidades de economia.

Segurança dos dados

Os dados do Cloud Analyzer são criptografados em repouso e nenhuma credencial é armazenada em nenhuma conta.

Comece a otimizar seus custos de computação em nuvem

Conete sua conta da AWS e veja a análise para começar a otimizar seus custos de computação em nuvem.

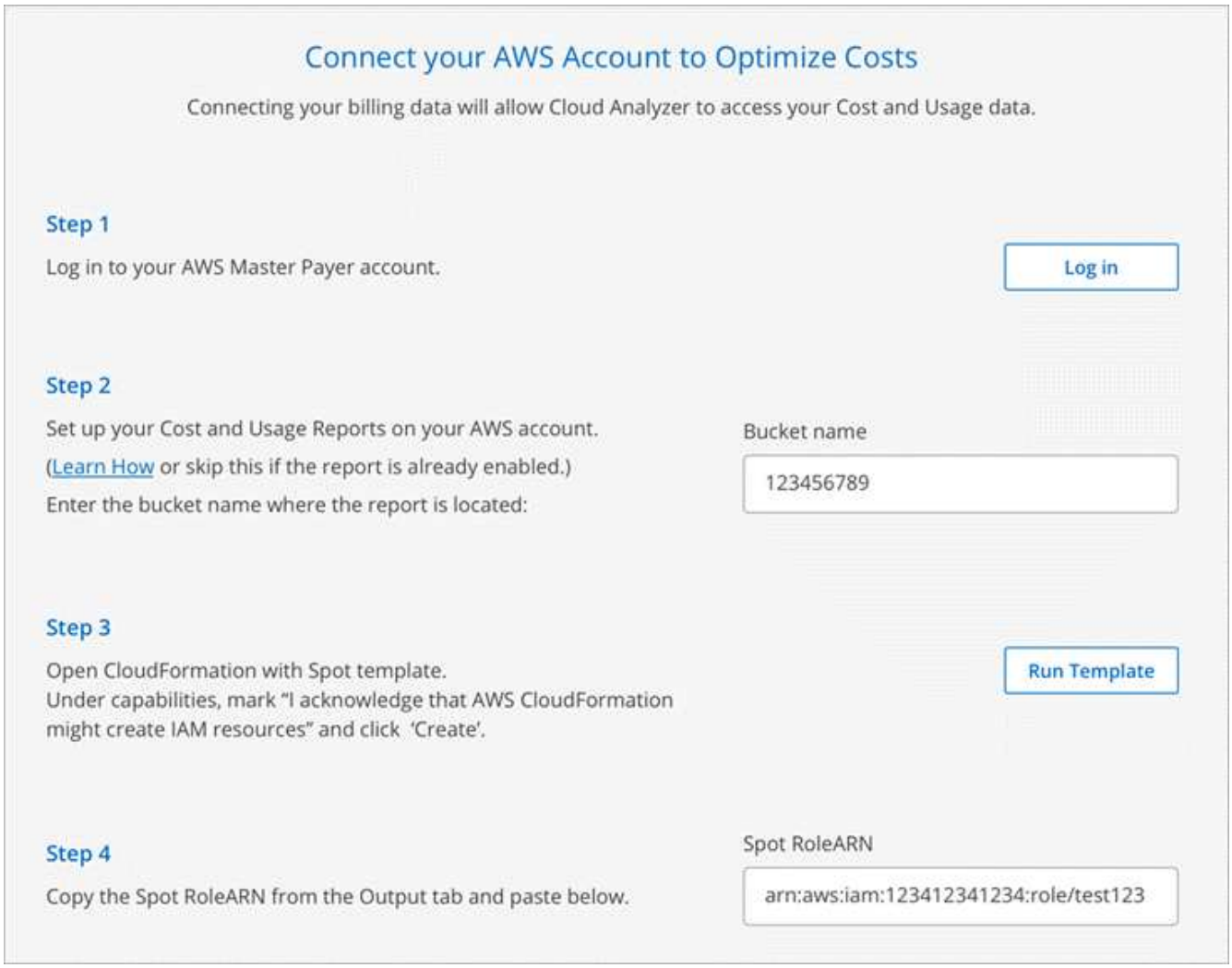
Conete o Cloud Analyzer à sua conta da AWS

Clique em **Compute** e conete sua conta do AWS Payer.

Passos

1. Clique em **Compute**.
2. Clique em **Adicionar credenciais da AWS ao Iniciar**.
3. Siga as etapas na página para conetar sua conta da AWS:
    a. Faça login na sua conta do pagador principal da AWS.
    b. Configure relatórios de custo e uso na conta da AWS.
    c. Execute o modelo do CloudFormation.
    d. Cole o Spot RoleARN.

    "Veja mais detalhes sobre estas etapas".

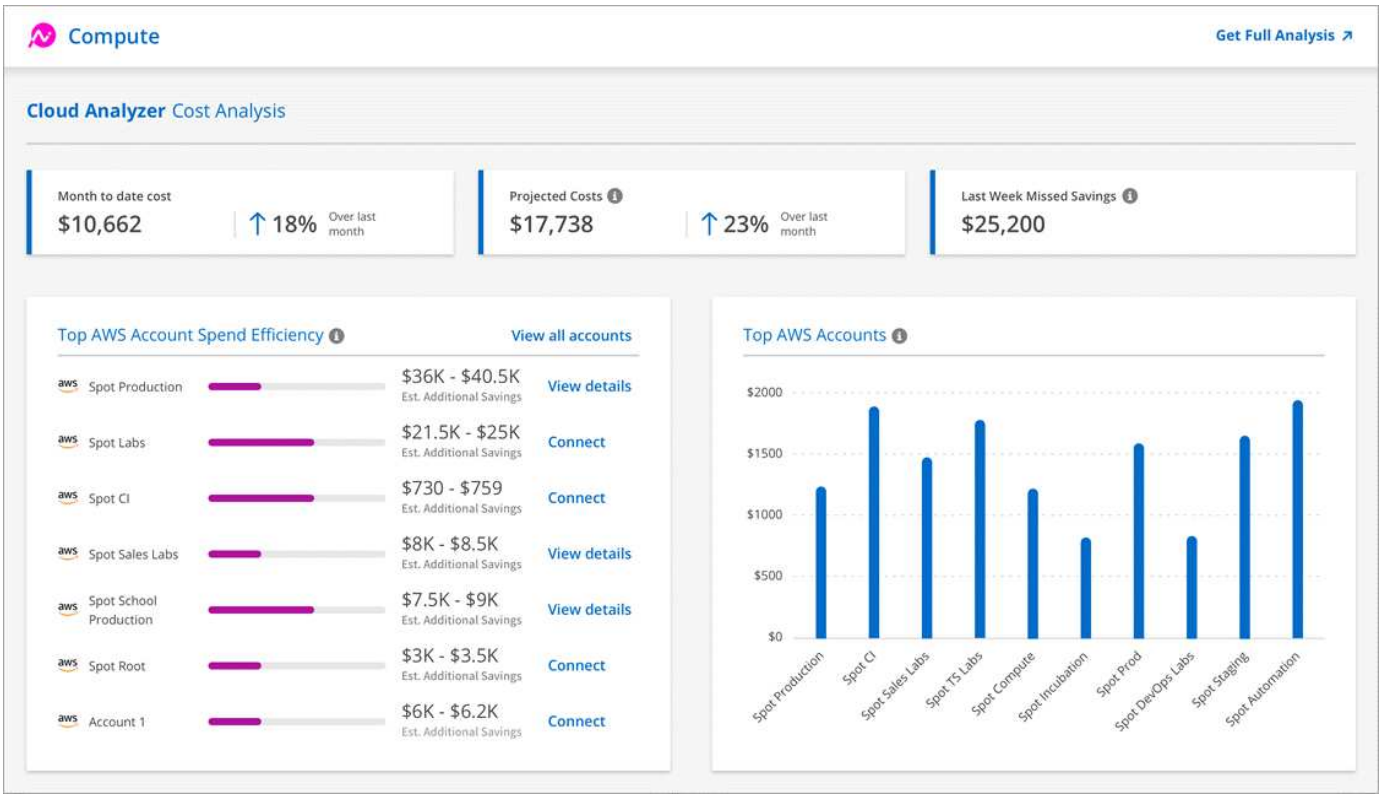


Resultado

O Cloud Analyzer começa a processar os dados da sua conta da AWS. Se você tiver várias contas, o Cloud Analyzer começa com recursos somente leitura para todas as contas vinculadas na conta do pagador principal. Se você quiser obter mais detalhes sobre as economias potenciais para essas contas, então você também precisará conectá-las. Você pode encontrar mais detalhes sobre esse processo na seção abaixo.

Analise seus custos de computação

Depois que o Cloud Analyzer processa os dados da sua conta, a guia Computação mostra informações sobre os custos da nuvem passados, atuais e futuros.



Custo mensal até à data

O custo total de suas cargas de trabalho desde o início do mês atual até o presente.

Custos projetados

O custo previsto no final do mês com base na análise do seu padrão de uso.

Poupanças perdidas na semana passada

Economias que poderiam ter sido obtidas nos últimos sete dias usando a otimização de instâncias spot e reservas.

Eficiência de gastos com contas da AWS

As 10 principais contas de acordo com o maior valor de poupança adicional estimada.

Cada conta recebe uma pontuação de eficiência com base em economias potenciais atuais e adicionais. A economia adicional estimada indica quanto pode ser economizado ainda mais com o uso de instâncias spot e reservadas.

Você pode executar as seguintes ações para otimizar ainda mais suas contas:

- **Veja detalhes**: Veja suas oportunidades de otimização de custos indo para o Cloud Analyzer do Spot.
- **Connect**: Conete uma conta que ainda não foi gerenciada. Você será direcionado para o assistente que coneta a conta.

Principais contas da AWS

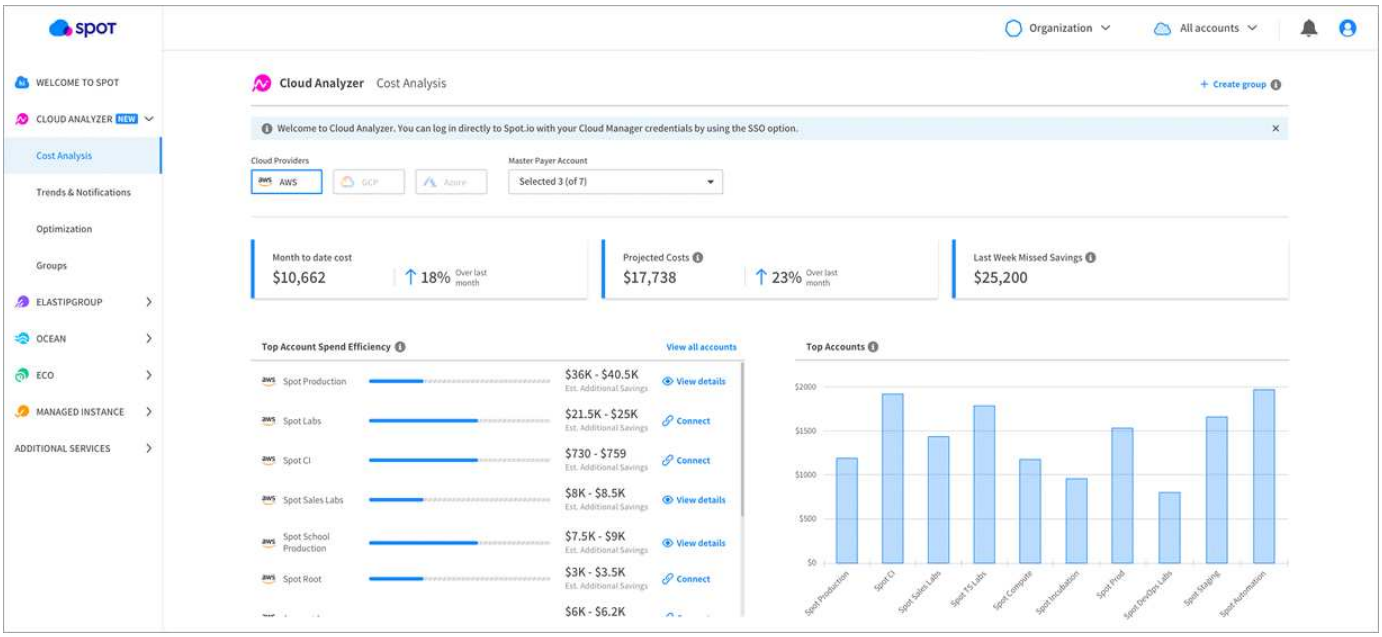
Este é um gráfico de barras mostrando suas dez principais contas por custo. O gráfico é baseado nos últimos 30 dias de atividade de gastos.

"Saiba mais sobre a página análise de custos disponível no Cloud Analyzer do Spot".

Vá para Cloud Analyzer para obter mais análises e recomendações

Clique em **Obtenha análise completa** a qualquer momento para acessar mais gráficos e análises, recomendações detalhadas, uma quebra de otimização de casos de uso (contentores, ElasticApps e reservas) e muito mais.

Aqui está um exemplo do que você verá no Cloud Analyzer:



- "Veja a página de produto do Cloud Analyzer para saber mais sobre seus recursos".
- "Veja a documentação do Spot para obter ajuda usando o Cloud Analyzer".

Categorize os dados na nuvem

Saiba mais sobre o Cloud Tiering

O serviço de disposição em camadas na nuvem do NetApp estende o data center para a nuvem ao dispor automaticamente em camadas os dados inativos de clusters ONTAP on-premises para o storage de objetos. Isso libera espaço valioso no cluster para mais workloads, sem fazer alterações na camada de aplicação. A disposição em camadas na nuvem pode reduzir custos no data center e permitir a mudança de um modelo CAPEX para um modelo OPEX.

O serviço disposição em camadas na nuvem aproveita os recursos do *FabricPool*. O FabricPool é uma tecnologia NetApp Data Fabric que permite a disposição automatizada em camadas de dados em storage de objetos de baixo custo. Os dados ativos permanecem em SSDs de alta performance, enquanto os dados inativos são dispostos em camadas em storage de objetos de baixo custo, preservando a eficiência de dados do ONTAP.

Caraterísticas

O Cloud Tiering oferece automação, monitoramento, relatórios e uma interface de gerenciamento comum:

- Com a automação, é mais fácil configurar e gerenciar a disposição de dados em camadas de clusters ONTAP no local para a nuvem
- Um único painel remove a necessidade de gerenciar o FabricPool de forma independente em vários clusters
- Os relatórios mostram a quantidade de dados ativos e inativos em cada cluster
- O status de integridade em categorias ajuda você a identificar e corrigir problemas conforme eles ocorrem
- Se você tiver sistemas Cloud Volumes ONTAP, encontrá-los-á no painel do cluster para ter uma visão completa da disposição de dados em sua infraestrutura de nuvem híbrida

Os sistemas Cloud Volumes ONTAP são somente leitura no Cloud Tiering. "Você configura a disposição em camadas do Cloud Volumes ONTAP a partir do ambiente de trabalho do Cloud Manager".

Para obter mais detalhes sobre o valor que o Cloud Tiering fornece, "Confira a página disposição em camadas na nuvem no NetApp".

Embora o Cloud Tiering possa reduzir significativamente o espaço físico do storage, ele não é uma solução de backup.

Fornecedores de storage de objetos compatíveis

É possível categorizar dados inativos de um cluster do ONTAP para Amazon S3, storage Microsoft Azure Blob, Google Cloud Storage ou StorageGRID (nuvem privada).

Preços e licenças

Pague pelo categorização de nuvem com uma subscrição com pagamento conforme o uso, uma licença de disposição em camadas do ONTAP chamada *FabricPool* ou uma combinação de ambos. Uma avaliação gratuita de 30 dias está disponível para o seu primeiro cluster se você não tiver uma licença.

Não há cobrança ao categorizar dados no StorageGRID. Nem uma licença BYOL ou Registro PAYGO são necessários.

"Ver detalhes de preços".

teste gratuito de 30 dias

Se você não tiver uma licença do FabricPool, uma avaliação gratuita de 30 dias do Cloud Tiering será iniciada quando você configurar a disposição em camadas no primeiro cluster. Depois que a avaliação gratuita de 30 dias terminar, você precisará pagar pelo Cloud Tiering por meio de uma assinatura com pagamento conforme o uso, uma licença FabricPool ou uma combinação de ambos.

Se a avaliação gratuita terminar e você não tiver assinado ou adicionado uma licença, o ONTAP não categorizará mais os dados inativos no storage de objetos, mas os dados existentes ainda estarão disponíveis para acesso.

Subscrição com pagamento conforme o uso

O Cloud Tiering oferece licenciamento baseado no consumo em um modelo de pagamento conforme o uso. Depois de se inscrever no marketplace do seu provedor de nuvem, você paga por GB pelos dados dispostos - não há pagamento inicial. Você é cobrado pelo seu provedor de nuvem por meio da sua fatura mensal.

Você deve se inscrever mesmo se você tiver uma avaliação gratuita ou se você trouxer sua própria licença (BYOL):

- A assinatura garante que não haja interrupção do serviço após o término da avaliação gratuita.

  Quando o teste terminar, você será cobrado de hora em hora de acordo com a quantidade de dados categorizados.

- Se você categorizar mais dados do que o permitido pela sua licença FabricPool, a categorização de dados continuará em sua assinatura de pagamento conforme o uso.

  Por exemplo, se você tiver uma licença de 10 TB, toda a capacidade além dos 10 TB será cobrada por meio da assinatura paga conforme o uso.

Você não será cobrado da sua assinatura paga conforme o uso durante a avaliação gratuita ou se você não tiver excedido sua licença FabricPool.

"Saiba como configurar uma assinatura paga conforme o uso".

Traga sua própria licença

Traga sua própria licença comprando uma licença ONTAP FabricPool da NetApp. Você pode comprar licenças perpétuas ou baseadas em termos de prazo.

Depois de adquirir uma licença do FabricPool, será necessário adicioná-la ao cluster, "O que você pode fazer diretamente do Cloud Tiering".

Depois de ativar a licença por meio do Cloud Tiering, se você adquirir capacidade adicional posteriormente, a licença no cluster será atualizada automaticamente com a nova capacidade. Não é necessário aplicar um novo ficheiro de licença NetApp (NLF) ao cluster.

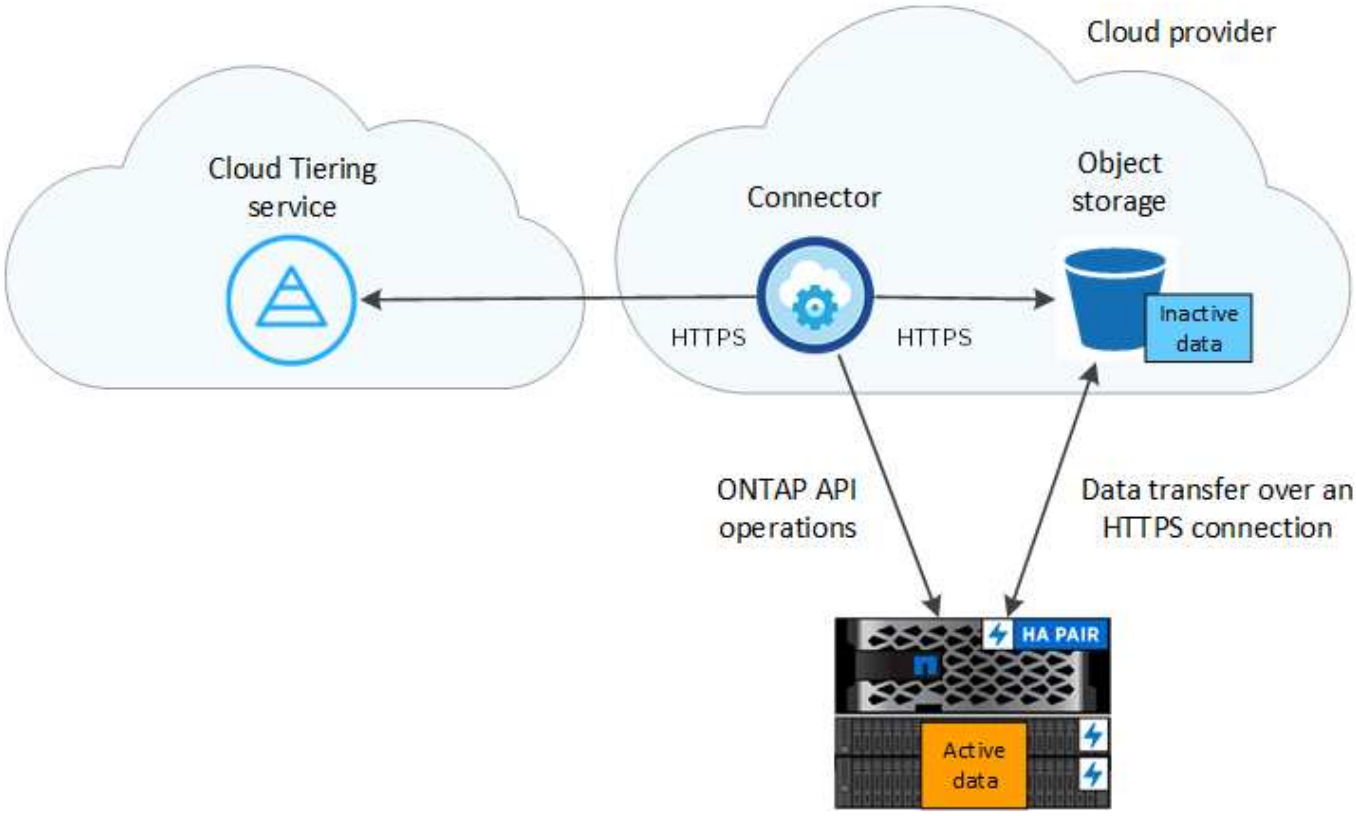
Como mencionado acima, recomendamos que você configure uma assinatura de pagamento conforme o uso, mesmo que seu cluster tenha uma licença BYOL.

Licença[Contacte-nos para comprar uma licença] NetApp.

Como o Cloud Tiering funciona

O Cloud Tiering é um serviço gerenciado pelo NetApp que usa a tecnologia FabricPool para categorizar automaticamente dados inativos (frios) dos seus clusters ONTAP no local para storage de objetos na nuvem pública ou privada. As ligações ao ONTAP ocorrem a partir de um conetor.

A imagem a seguir mostra a relação entre cada componente:



Em um alto nível, o Cloud Tiering funciona assim:

1. Descubra seu cluster no local usando o Cloud Manager.
2. Você configura a disposição em categorias fornecendo detalhes sobre seu storage de objetos, incluindo o bucket/contêiner e uma classe de storage ou camada de acesso.
3. O Cloud Manager configura o ONTAP para usar o fornecedor de storage de objetos e descobre a quantidade de dados ativos e inativos no cluster.
4. Você escolhe os volumes a categorizar e a política de disposição em camadas a serem aplicados a esses volumes.
5. O ONTAP começa a categorizar dados inativos no armazenamento de objetos, assim que os dados atingirem os limites para serem considerados inativos (Políticas de disposição em camadas de

volumeconsulte).

Storage de objetos

Cada cluster do ONTAP alinha dados inativos em um único armazenamento de objetos. Ao configurar a disposição de dados em categorias, você pode adicionar um novo bucket/contêiner ou selecionar um bucket/contêiner existente, juntamente com uma classe de storage ou uma categoria de acesso.

- "Saiba mais sobre as classes de armazenamento S3 suportadas"
- "Saiba mais sobre os níveis de acesso Blob do Azure compatíveis"
- "Saiba mais sobre as classes de armazenamento compatíveis do Google Cloud"

Políticas de disposição em camadas de volume

Quando você seleciona os volumes que deseja categorizar, você escolhe uma política de disposição em camadas *volume* para aplicar a cada volume. Uma política de disposição em categorias determina quando ou se os blocos de dados de usuário de um volume são movidos para a nuvem.

Nenhuma política de disposição em camadas

Mantém os dados em um volume na categoria de performance, impedindo que eles sejam movidos para a nuvem.

Snapshots inativos (somente Snapshot)

O ONTAP dispõe de blocos de Snapshot frio no volume que não são compartilhados com o sistema de arquivos ativo para o storage de objetos. Se lidos, os blocos de dados inativos na camada de nuvem ficam ativos e são movidos para a categoria de performance.

Os dados são dispostos somente depois que um agregado atingiu a capacidade de 50% e quando os dados alcançaram o período de resfriamento. O número padrão de dias de resfriamento é 2, mas você pode ajustar o número de dias.

> As gravações da categoria de nuvem para a categoria de performance serão desativadas se a capacidade da categoria de performance for superior a 70%. Se isso ocorrer, os blocos são acessados diretamente da camada de nuvem.

Dados inativos do utilizador (Auto)

O ONTAP coloca todos os blocos inativos no volume (não incluindo metadados) no storage de objetos. Os dados inativos incluem não apenas cópias Snapshot, mas também dados de usuários inativos do sistema de arquivos ativo.

Se forem lidos por leituras aleatórias, os blocos de dados inativos na camada de nuvem ficam ativos e são movidos para a camada de performance. Se forem lidos por leituras sequenciais, como as associadas a verificações de índice e antivírus, os blocos de dados inativos na camada de nuvem permanecem inativos e não são gravados na camada de performance.

Os dados são dispostos somente depois que um agregado atingiu a capacidade de 50% e quando os dados alcançaram o período de resfriamento. O período de resfriamento é o tempo em que os dados do usuário em um volume devem permanecer inativos para que os dados sejam considerados "frios" e movidos para o armazenamento de objetos. O número padrão de dias de resfriamento é 31, mas você pode ajustar o número de dias.

As gravações da categoria de nuvem para a categoria de performance serão desativadas se a capacidade da categoria de performance for superior a 70%. Se isso ocorrer, os blocos são acessados diretamente da camada de nuvem.

Todos os dados do utilizador (todos)

Todos os dados (não incluindo metadados) são imediatamente marcados como frios e dispostos em camadas no storage de objetos o mais rápido possível. Não há necessidade de esperar 48 horas para que novos blocos em um volume fiquem frios. Observe que os blocos localizados no volume antes da política tudo ser definida exigem 48 horas para ficarem frios.

Se lidos, os blocos de dados inativos na categoria de nuvem não são gravados de volta na categoria de performance. Esta política está disponível a partir do ONTAP 9.6.

Leve o seguinte em consideração antes de escolher essa política de disposição em categorias:

- A disposição de dados em categorias reduz imediatamente as eficiências de storage (somente inline).
- Você deve usar esta política somente se tiver certeza de que os dados inativos no volume não serão alterados.
- O armazenamento de objetos não é transacional e resultará em fragmentação significativa se sujeito a alterações.
- Considere o impacto das transferências SnapMirror antes de atribuir a política de todas as categorias aos volumes de origem em relacionamentos de proteção de dados.

  Como os dados são dispostos imediatamente, o SnapMirror lê os dados da camada de nuvem e não da camada de performance. Isso resultará em operações mais lentas do SnapMirror - possivelmente retardando outras operações do SnapMirror mais tarde na fila - mesmo que estejam usando políticas de disposição em camadas diferentes.

Todos os dados do usuário DP (Backup)

Todos os dados em um volume de proteção de dados (não incluindo metadados) são movidos imediatamente para a categoria de nuvem. Se lidos, os blocos de dados inativos na categoria de nuvem permanecem inativos e não são gravados de volta na categoria de performance (começando com ONTAP 9.4).

Esta política está disponível para o ONTAP 9.5 ou anterior. Ela foi substituída pela política de disposição em camadas **All** a partir do ONTAP 9.6.

Comece agora

Disposição em camadas de dados de clusters ONTAP on-premises para o Amazon S3

Liberar espaço nos clusters do ONTAP no local ao dispor os dados em camadas no Amazon S3. A disposição em camadas de dados é baseada no serviço de disposição em camadas na nuvem do NetApp.

Início rápido

Comece rapidamente seguindo estas etapas ou role para baixo até as seções restantes para obter detalhes completos.

Prepare-se para categorizar dados no Amazon S3

Você precisa do seguinte:

- Um sistema AFF ou FAS com agregados all-SSD que está executando o ONTAP 9.2 ou posterior e tem uma conexão HTTPS com o Amazon S3.
- Uma conta da AWS com uma chave de acesso e as permissões necessárias assim o cluster do ONTAP pode categorizar dados inativos dentro e fora do S3.
- Um conetor instalado em uma VPC da AWS ou no local.
- Rede para o conetor que habilita uma conexão HTTPS de saída ao cluster ONTAP, ao storage S3 e ao serviço de disposição em camadas na nuvem.

Configurar a disposição em camadas

No Cloud Manager, selecione um ambiente de trabalho local, clique em **Configuração de categorias** e siga as instruções para colocar dados em camadas no Amazon S3.

Configure o licenciamento

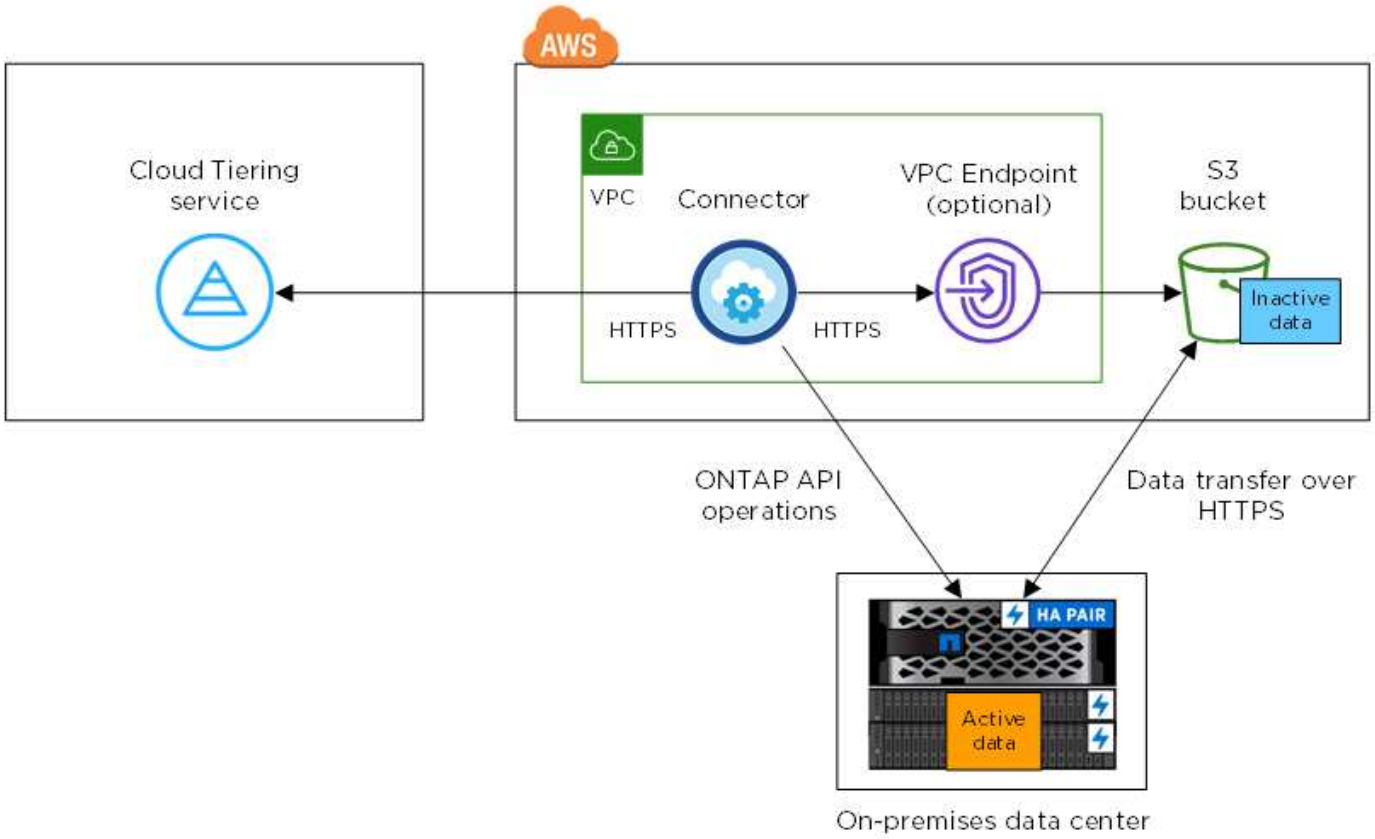
Após o término da avaliação gratuita, pague pelo Cloud Tiering por meio de uma assinatura com pagamento conforme o uso, de uma licença de disposição em camadas do ONTAP ou de uma combinação de ambos:

- Para se inscrever no AWS Marketplace, clique em **Categorização > Licenciamento**, clique em **Subscribe** e siga os prompts.
- Para pagar usando uma licença de disposição em camadas, mailto:ng-cloud-Tiering em NetApp.com?subject:Licensing [entre em Contato conosco se precisar comprar uma] e, em seguida"Adicione-o ao cluster a partir do Cloud Tiering", .

Requisitos

Verifique o suporte para o cluster ONTAP, configure a rede e prepare o armazenamento de objetos.

A imagem a seguir mostra cada componente e as conexões que você precisa preparar entre eles:



A comunicação entre um conetor e S3 destina-se apenas à configuração de armazenamento de objetos. O conector pode residir no local, em vez da nuvem.

Preparando os clusters do ONTAP

Os clusters do ONTAP precisam atender aos requisitos a seguir ao categorizar dados no Amazon S3.

Plataformas ONTAP compatíveis

O Cloud Tiering dá suporte a sistemas AFF e agregados all-SSD em sistemas FAS.

Versão ONTAP suportada

ONTAP 9 .2 ou posterior

Requisitos de rede de cluster

- O cluster do ONTAP inicia uma conexão HTTPS pela porta 443 para o Amazon S3.

  O ONTAP lê e grava dados no storage de objetos. O armazenamento de objetos nunca inicia, ele apenas responde.

  Embora o AWS Direct Connect ofereça melhor desempenho e menores taxas de transferência de dados, isso não é necessário entre o cluster ONTAP e o S3. Como o desempenho é significativamente melhor ao usar o AWS Direct Connect, isso é a melhor prática recomendada.

- Uma conexão de entrada é necessária a partir do conetor, que pode residir em uma VPC da AWS ou no local.

  Não é necessária uma conexão entre o cluster e o serviço Cloud Tiering.

- É necessário um LIF entre clusters em cada nó do ONTAP que hospeda volumes dispostos em camadas. O LIF deve estar associado ao *IPspace* que o ONTAP deve usar para se conetar ao armazenamento de objetos.

  Os IPspaces permitem a segregação de tráfego de rede, permitindo a separação do tráfego de clientes para privacidade e segurança. "Saiba mais sobre IPspaces".

  Quando você configura a disposição de dados em categorias, o Cloud Tiering solicita que você use o espaço IPspace. Você deve escolher o espaço IPspace ao qual cada LIF está associado. Esse pode ser o espaço IPspace "padrão" ou um espaço IPspace personalizado que você criou.

Volumes e agregados compatíveis

O número total de volumes em que o Cloud Tiering pode ser menor que o número de volumes no sistema ONTAP. Isso porque os volumes não podem ser dispostos em camadas de alguns agregados. Por exemplo, você não pode categorizar dados de volumes do SnapLock ou de configurações do MetroCluster. Consulte a documentação do ONTAP para obter "Funcionalidade ou recursos não suportados pelo FabricPool"informações sobre .

O Cloud Tiering é compatível com volumes FlexGroup, a partir do ONTAP 9.5. A configuração funciona da mesma forma que qualquer outro volume.

Criação ou comutação de conetores

Um conector é necessário para categorizar dados na nuvem. Ao categorizar dados no AWS S3, você pode usar um conetor em uma VPC da AWS ou no local. Você precisará criar um novo conetor ou garantir que o conetor selecionado atualmente reside na AWS ou no local.

- "Saiba mais sobre conetores"
- "Criando um conetor na AWS"
- "Requisitos do host do conetor"
- "Instalar o conetor em um host Linux existente"
- "Comutação entre conetores"

Preparar a rede para o conetor

Certifique-se de que o conetor tem as ligações de rede necessárias. Um conetor pode ser instalado no local ou na AWS.

Passos

1. Certifique-se de que a rede onde o conetor está instalado permite as seguintes ligações:
   - Uma conexão de saída à Internet para o serviço Cloud Tiering pela porta 443 (HTTPS)
   - Uma conexão HTTPS pela porta 443 a S3
   - Uma conexão HTTPS pela porta 443 aos clusters do ONTAP
2. Se necessário, habilite um endpoint VPC para S3.

   Um endpoint de VPC para S3 é recomendado se você tiver uma conexão de conexão direta ou VPN do cluster do ONTAP para a VPC e quiser que a comunicação entre o conetor e o S3 permaneça na rede interna da AWS.

Preparando o Amazon S3

Ao configurar a disposição de dados em categorias em um novo cluster, você será solicitado a criar um bucket do S3 ou a selecionar um bucket do S3 existente na conta da AWS onde o conetor está configurado.

A conta da AWS deve ter permissões e uma chave de acesso que você possa inserir no Cloud Tiering. O cluster do ONTAP usa a chave de acesso para agrupar dados em camadas dentro e fora do S3.

Passos

1. Forneça as seguintes permissões ao usuário do IAM:

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetBucketLocation",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject"
```

   "Documentação da AWS: Criando uma função para delegar permissões a um usuário do IAM"

2. Crie ou localize uma chave de acesso.

   O Cloud Tiering passa a chave de acesso ao cluster do ONTAP. As credenciais não são armazenadas no serviço Cloud Tiering.

   "Documentação da AWS: Gerenciando chaves de acesso para usuários do IAM"

Disposição em camadas dos dados inativos do primeiro cluster para o Amazon S3

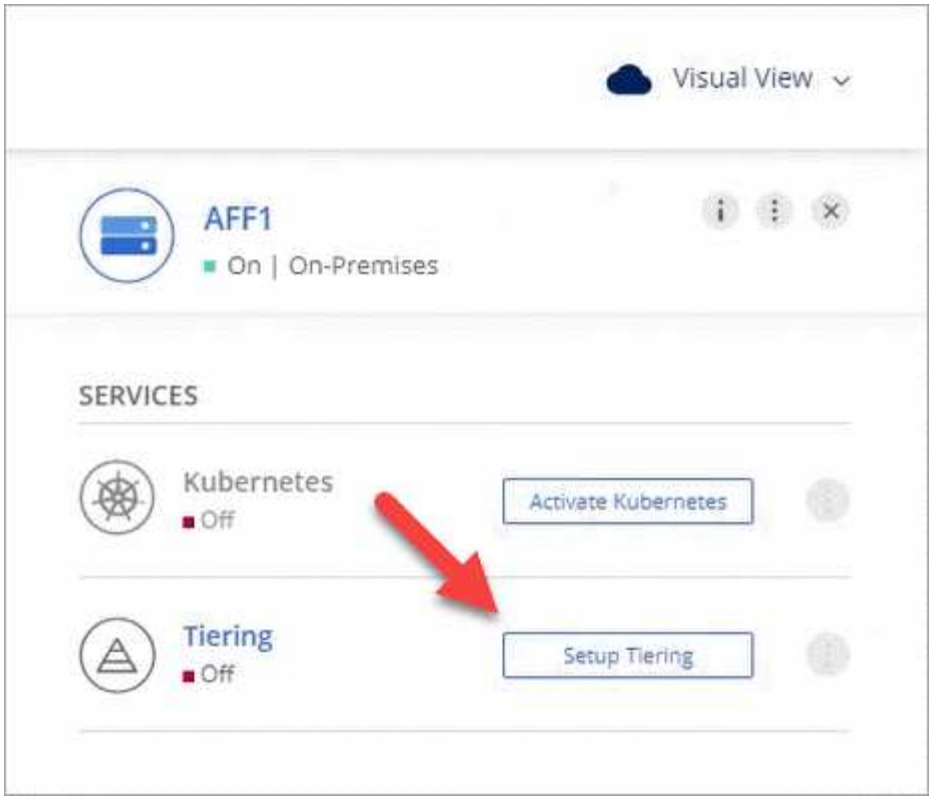
Depois de preparar seu ambiente AWS, comece a categorizar os dados inativos do primeiro cluster.

O que você vai precisar

- "Um ambiente de trabalho no local".
- Uma chave de acesso da AWS para um usuário do IAM que tenha as permissões S3 necessárias.

Passos

1. Selecione um cluster no local.
2. Clique em **Configuração em categorias**.



Agora você está no painel de disposição em camadas.

3. Clique em **Configurar disposição em camadas** ao lado do cluster.
4. Conclua as etapas na página **Configuração de categorias**:

   a. **S3 Bucket**: Adicione um novo bucket S3 ou selecione um bucket S3 existente que comece com o prefixo *Fabric-pool* e clique em **Continue**.

      O prefixo *Fabric-pool* é necessário porque a política do IAM para o conetor permite que a instância execute ações S3 em buckets nomeados com esse prefixo exato.

   Por exemplo, você pode nomear o bucket do S3 fabric-pool-AFF1, onde AFF1 é o nome do cluster.

   a. **Classe de armazenamento**: Selecione a classe de armazenamento S3 para a qual deseja transferir os dados após 30 dias e clique em **continuar**.

      Se você escolher padrão, os dados permanecerão nessa classe de storage.

   b. **Credenciais**: Insira a ID da chave de acesso e a chave secreta para um usuário do IAM que tenha as permissões S3 necessárias.

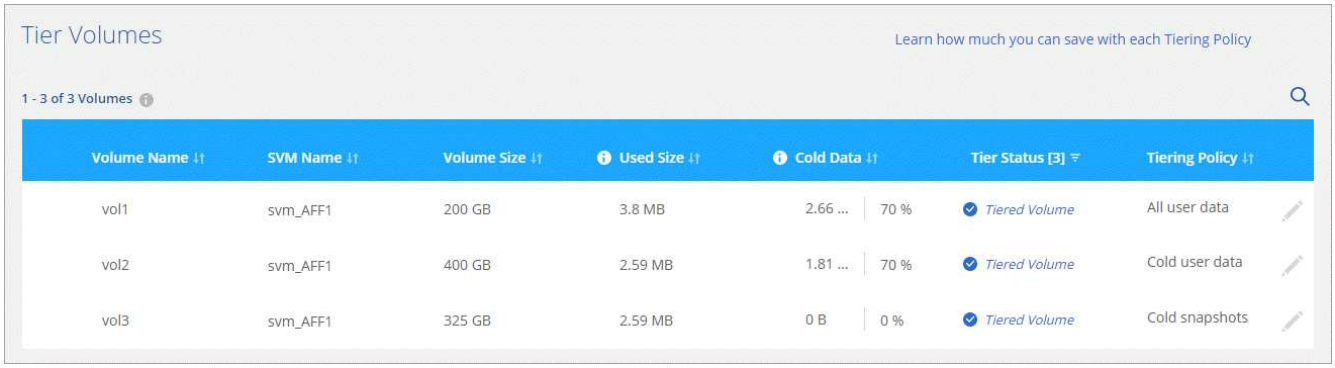
      O usuário do IAM deve estar na mesma conta da AWS que o intervalo selecionado ou criado na página **S3 Bucket**.

   c. **Rede de cluster**: Selecione o espaço IPspace que o ONTAP deve usar para se conetar ao armazenamento de objetos e clique em **continuar**.

      A seleção do espaço de IPspace correto garante que a disposição em camadas na nuvem possa configurar uma conexão do ONTAP ao armazenamento de objetos do seu provedor de nuvem.

5. Clique em **continuar** para selecionar os volumes que deseja categorizar.
6. Na página **volumes de nível**, configure a disposição em categorias para cada volume. Clique no ícone, selecione uma política de disposição em camadas, ajuste opcionalmente os dias de resfriamento e clique em **aplicar**.

   "Saiba mais sobre as políticas de disposição em camadas de volume".



Resultado

Você configurou com sucesso a disposição de dados em camadas de volumes no cluster para o storage de objetos S3.

O que se segue?

"Certifique-se de se inscrever no serviço Cloud Tiering".

Você também pode adicionar clusters adicionais ou analisar informações sobre os dados ativos e inativos no cluster. Para obter detalhes, "Gerenciamento de categorização de dados nos clusters"consulte .

Disposição em camadas de dados de clusters ONTAP on-premises para o storage Azure Blob

Libere espaço em seus clusters ONTAP no local ao dispor em camadas os dados no storage Blob do Azure. A disposição em camadas de dados é baseada no serviço de disposição em camadas na nuvem do NetApp.

Início rápido

Comece rapidamente seguindo estas etapas ou role para baixo até as seções restantes para obter detalhes completos.

Prepare-se para categorizar dados no storage Azure Blob

Você precisa do seguinte:

- Um sistema AFF ou FAS com agregados all-SSD que esteja executando o ONTAP 9.4 ou posterior e que tenha uma conexão HTTPS com o storage Blob do Azure.
- Um conetor instalado em um Azure VNet.
- Rede para um conetor que habilita uma conexão HTTPS de saída para o cluster do ONTAP no data

center, para o storage do Blob do Azure e para o serviço de disposição em camadas na nuvem.

Configurar a disposição em camadas

No Cloud Manager, selecione um ambiente de trabalho local, clique em **Configuração de disposição em camadas** e siga as instruções para categorizar dados no armazenamento de Blob do Azure.

Configure o licenciamento

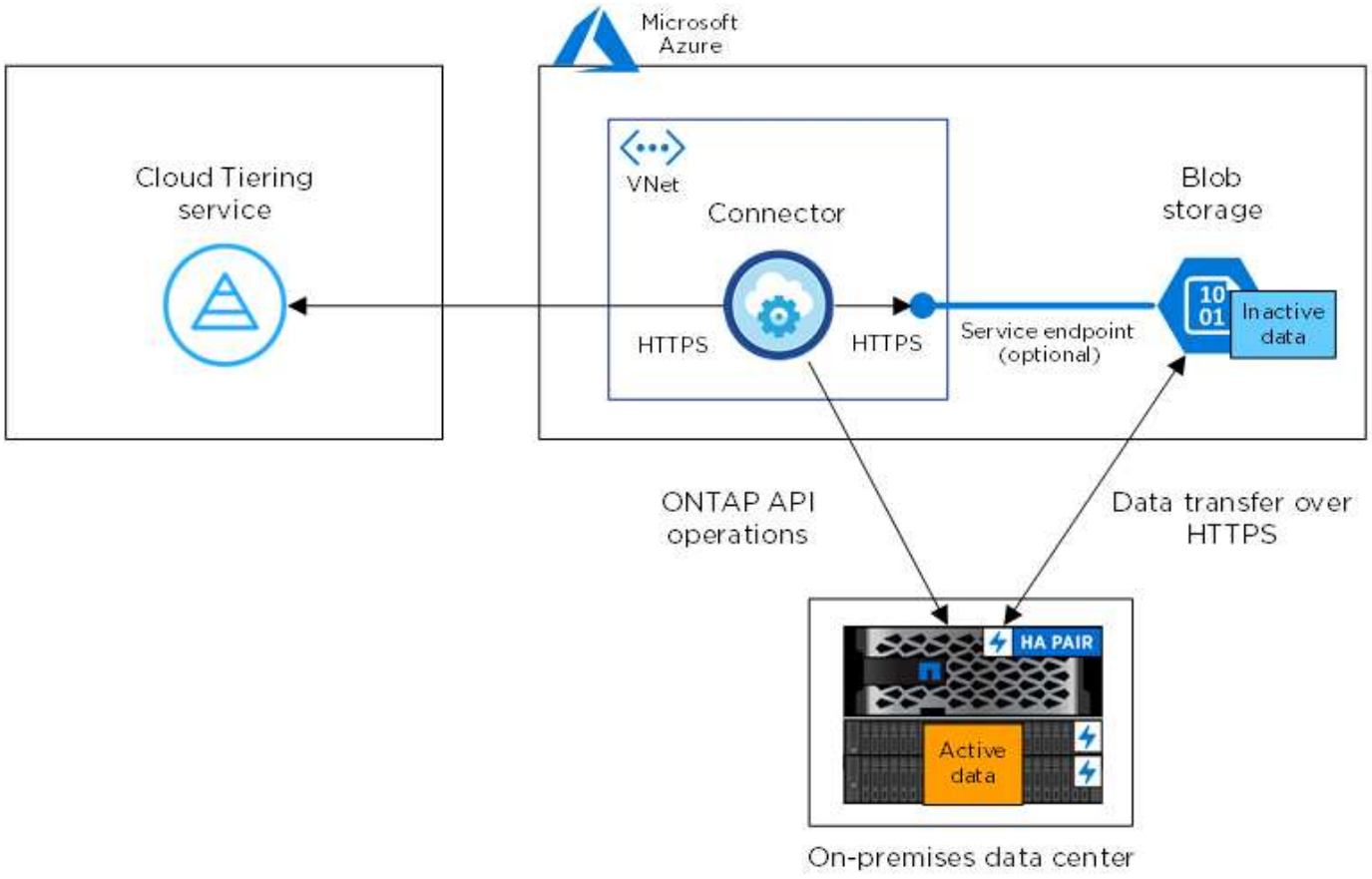
Após o término da avaliação gratuita, pague pelo Cloud Tiering por meio de uma assinatura com pagamento conforme o uso, de uma licença de disposição em camadas do ONTAP ou de uma combinação de ambos:

- Para se inscrever no Azure Marketplace, clique em **Categorização > Licenciamento**, clique em **Subscribe** e siga as instruções.
- Para adicionar uma licença de disposição em camadas, mailto:ng-cloud-Tiering em NetApp.com?subject:Licensing [entre em Contato conosco se precisar comprar uma] e, em seguida"Adicione-o ao cluster a partir do Cloud Tiering", .

Requisitos

Verifique o suporte para o cluster ONTAP, configure a rede e prepare o armazenamento de objetos.

A imagem a seguir mostra cada componente e as conexões que você precisa preparar entre eles:



A comunicação entre o conetor e o armazenamento Blob destina-se apenas à configuração de armazenamento de objetos.

Preparando os clusters do ONTAP

Os clusters do ONTAP devem atender aos requisitos a seguir ao categorizar dados no storage de Blob do Azure.

Plataformas ONTAP compatíveis

O Cloud Tiering dá suporte a sistemas AFF e agregados all-SSD em sistemas FAS.

Versão ONTAP suportada

ONTAP 9 .4 ou posterior

Requisitos de rede de cluster

- O cluster do ONTAP inicia uma conexão HTTPS pela porta 443 para o armazenamento de Blobs do Azure.

  O ONTAP lê e grava dados no storage de objetos. O armazenamento de objetos nunca inicia, ele apenas responde.

  Embora o ExpressRoute forneça melhor desempenho e menores custos de transferência de dados, isso não é necessário entre o cluster ONTAP e o armazenamento de Blobs do Azure. Como o desempenho é significativamente melhor ao usar o ExpressRoute, isso é a melhor prática recomendada.

- Uma conexão de entrada é necessária a partir do NetApp Service Connector, que reside em um Azure VNet.

  Não é necessária uma conexão entre o cluster e o serviço Cloud Tiering.

- É necessário um LIF entre clusters em cada nó do ONTAP que hospeda volumes dispostos em camadas. O LIF deve estar associado ao *IPspace* que o ONTAP deve usar para se conetar ao armazenamento de objetos.

  Os IPspaces permitem a segregação de tráfego de rede, permitindo a separação do tráfego de clientes para privacidade e segurança. "Saiba mais sobre IPspaces".

  Quando você configura a disposição de dados em categorias, o Cloud Tiering solicita que você use o espaço IPspace. Você deve escolher o espaço IPspace ao qual cada LIF está associado. Esse pode ser o espaço IPspace "padrão" ou um espaço IPspace personalizado que você criou.

Volumes e agregados compatíveis

O número total de volumes em que o Cloud Tiering pode ser menor que o número de volumes no sistema ONTAP. Isso porque os volumes não podem ser dispostos em camadas de alguns agregados. Por exemplo, você não pode categorizar dados de volumes do SnapLock ou de configurações do MetroCluster. Consulte a documentação do ONTAP para obter "Funcionalidade ou recursos não suportados pelo FabricPool"informações sobre .

O Cloud Tiering é compatível com volumes FlexGroup, a partir do ONTAP 9.5. A configuração funciona da mesma forma que qualquer outro volume.

Criação ou comutação de conetores

Um conector é necessário para categorizar dados na nuvem. Ao categorizar dados no armazenamento de Blob do Azure, um conector deve estar disponível em um Azure VNet. Você precisará criar um novo conetor ou certificar-se de que o conetor atualmente selecionado reside no Azure.

- "Saiba mais sobre conetores"
- "Criando um conetor no Azure"
- "Comutação entre conetores"

Preparar a rede para o conetor

Certifique-se de que o conetor tem as ligações de rede necessárias.

Passos

1. Certifique-se de que a VNet onde o conetor está instalado permite as seguintes ligações:
   - Uma conexão de saída à Internet para o serviço Cloud Tiering pela porta 443 (HTTPS)
   - Uma conexão HTTPS pela porta 443 para o storage Azure Blob
   - Uma conexão HTTPS pela porta 443 aos clusters do ONTAP
2. Se necessário, ative um ponto de extremidade do serviço VNet para o armazenamento Azure.

   Recomenda-se um ponto de extremidade do serviço VNet para o armazenamento Azure se tiver uma ligação ExpressRoute ou VPN do seu cluster ONTAP para o VNet e pretender que a comunicação entre o conetor e o armazenamento Blob permaneça na sua rede privada virtual.

Disposição em camadas dos dados inativos do primeiro cluster para o storage Azure Blob

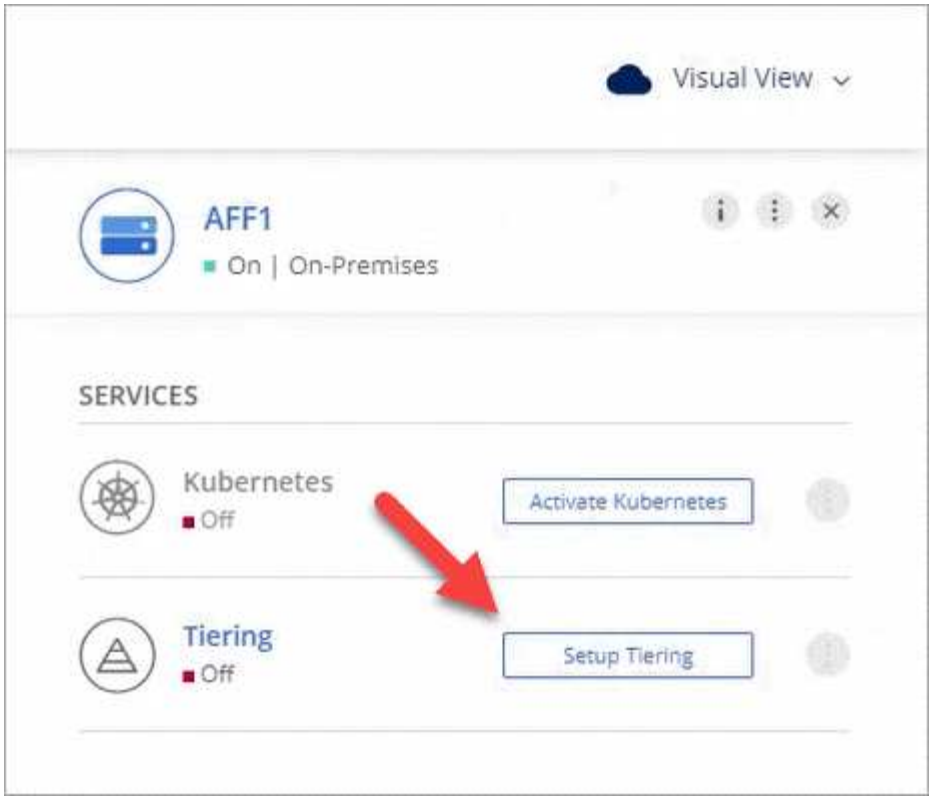
Depois de preparar seu ambiente Azure, comece a categorizar os dados inativos do primeiro cluster.

O que você vai precisar

"Um ambiente de trabalho no local".

Passos

1. Selecione um cluster no local.
2. Clique em **Configuração em categorias**.



Agora você está no painel de disposição em camadas.

3. Clique em **Configurar disposição em camadas** ao lado do cluster.
4. Conclua as etapas na página **Configuração de categorias**:
   a. **Grupo de recursos**: Selecione um grupo de recursos onde um contentor existente é gerenciado ou onde você gostaria de criar um novo contentor para dados em camadas.
   b. **Contentor Azure**: Adicione um novo contentor Blob a uma conta de armazenamento ou selecione um contentor existente e clique em **continuar**.

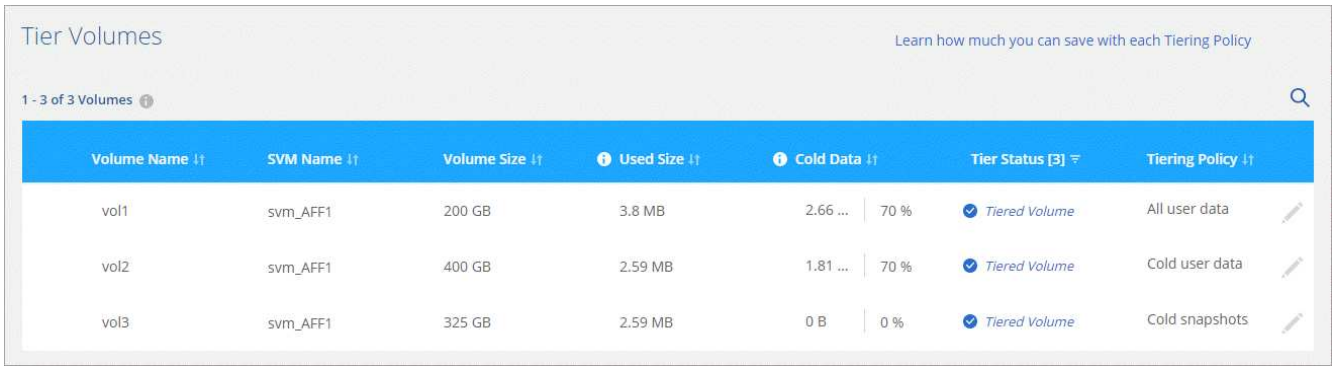
      A conta de armazenamento e os contentores que aparecem nesta etapa pertencem ao grupo de recursos selecionado na etapa anterior.

   c. **Nível de acesso**: Selecione o nível de acesso que deseja usar para os dados em camadas e clique em **continuar**.
   d. **Rede de cluster**: Selecione o espaço IPspace que o ONTAP deve usar para se conetar ao armazenamento de objetos e clique em **continuar**.

      A seleção do espaço de IPspace correto garante que a disposição em camadas na nuvem possa configurar uma conexão do ONTAP ao armazenamento de objetos do seu provedor de nuvem.

5. Clique em **continuar** para selecionar os volumes que deseja categorizar.
6. Na página **volumes de nível**, configure a disposição em categorias para cada volume. Clique no ícone, selecione uma política de disposição em camadas, ajuste opcionalmente os dias de resfriamento e clique em **aplicar**.

   "Saiba mais sobre as políticas de disposição em camadas de volume".



Resultado

Você configurou com sucesso a disposição de dados em categorias de volumes no cluster para o storage de objetos Azure Blob.

O que se segue?

"Certifique-se de se inscrever no serviço Cloud Tiering".

Você também pode adicionar clusters adicionais ou analisar informações sobre os dados ativos e inativos no cluster. Para obter detalhes, "Gerenciamento de categorização de dados nos clusters"consulte .

Disposição de dados em camadas de clusters ONTAP on-premises para o Google Cloud Storage

Libere espaço nos clusters do ONTAP no local ao dispor os dados em camadas no Google Cloud Storage. A disposição em camadas de dados é baseada no serviço de disposição em camadas na nuvem do NetApp.

Início rápido

Comece rapidamente seguindo estas etapas ou role para baixo até as seções restantes para obter detalhes completos.

1 Prepare-se para categorizar dados no Google Cloud Storage

Você precisa do seguinte:

- Um sistema AFF ou FAS com agregados all-SSD executando o ONTAP 9.6 ou posterior e com conexão HTTPS ao Google Cloud Storage.
- Uma conta de serviço que tem a função de administrador de armazenamento predefinida e as chaves de acesso ao armazenamento.
- Um conetor instalado em uma VPC do Google Cloud Platform.
- Rede para o conetor que permite uma conexão HTTPS de saída ao cluster do ONTAP no data center, ao Google Cloud Storage e ao serviço de disposição em camadas na nuvem.

2 Configurar a disposição em camadas

No Cloud Manager, selecione um ambiente de trabalho local, clique em **Configuração de categorias** e siga as instruções para colocar dados em camadas no Google Cloud Storage.

Configure o licenciamento

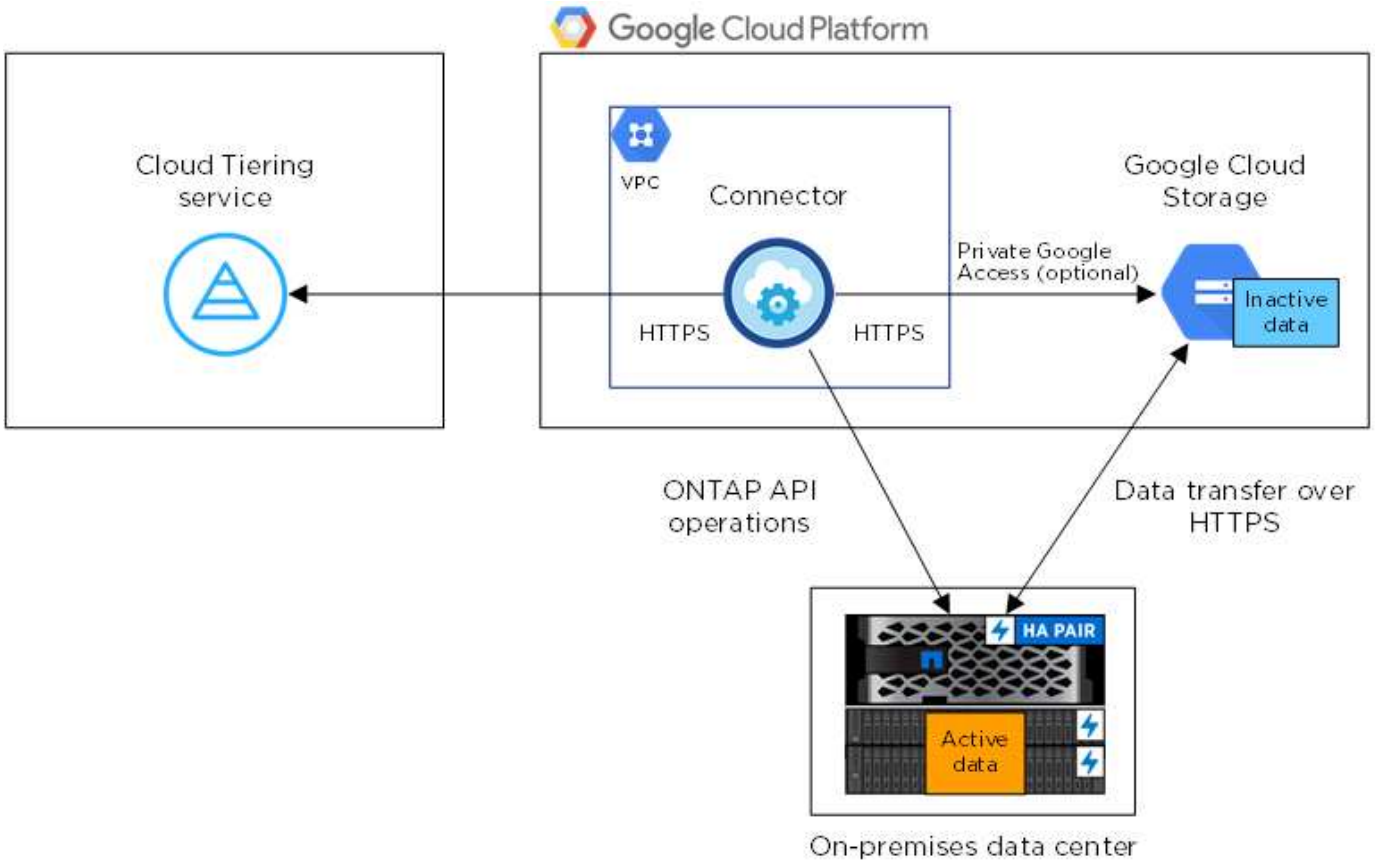
Após o término da avaliação gratuita, pague pelo Cloud Tiering por meio de uma assinatura com pagamento conforme o uso, de uma licença de disposição em camadas do ONTAP ou de uma combinação de ambos:

- Para se inscrever no GCP Marketplace, clique em **Categorização > Licenciamento**, clique em **Subscrever** e siga as instruções.
- Para adicionar uma licença de disposição em camadas, mailto:ng-cloud-Tiering em NetApp.com?subject:Licensing [entre em Contato conosco se precisar comprar uma] e, em seguida"Adicione-o ao cluster a partir do Cloud Tiering", .

Requisitos

Verifique o suporte para o cluster ONTAP, configure a rede e prepare o armazenamento de objetos.

A imagem a seguir mostra cada componente e as conexões que você precisa preparar entre eles:



A comunicação entre o conetor e o Google Cloud Storage destina-se apenas à configuração de armazenamento de objetos.

Preparando os clusters do ONTAP

Os clusters do ONTAP precisam atender aos requisitos a seguir ao categorizar dados no Google Cloud Storage.

Plataformas ONTAP compatíveis

O Cloud Tiering dá suporte a sistemas AFF e agregados all-SSD em sistemas FAS.

Versões de ONTAP compatíveis

ONTAP 9 .6 ou posterior

Requisitos de rede de cluster

- O cluster do ONTAP inicia uma conexão HTTPS pela porta 443 para o Google Cloud Storage.

  O ONTAP lê e grava dados no storage de objetos. O armazenamento de objetos nunca inicia, ele apenas responde.

  Embora o Google Cloud Interconnect ofereça melhor desempenho e menores taxas de transferência de dados, isso não é necessário entre o cluster do ONTAP e o Google Cloud Storage. Como o desempenho é significativamente melhor ao usar o Google Cloud Interconnect, isso é a melhor prática recomendada.

- Uma conexão de entrada é necessária no NetApp Service Connector, que reside em uma VPC do Google Cloud Platform.

  Não é necessária uma conexão entre o cluster e o serviço Cloud Tiering.

- É necessário um LIF entre clusters em cada nó do ONTAP que hospeda volumes dispostos em camadas. O LIF deve estar associado ao *IPspace* que o ONTAP deve usar para se conetar ao armazenamento de objetos.

  Os IPspaces permitem a segregação de tráfego de rede, permitindo a separação do tráfego de clientes para privacidade e segurança. "Saiba mais sobre IPspaces".

  Quando você configura a disposição de dados em categorias, o Cloud Tiering solicita que você use o espaço IPspace. Você deve escolher o espaço IPspace ao qual cada LIF está associado. Esse pode ser o espaço IPspace "padrão" ou um espaço IPspace personalizado que você criou.

Volumes e agregados compatíveis

O número total de volumes em que o Cloud Tiering pode ser menor que o número de volumes no sistema ONTAP. Isso porque os volumes não podem ser dispostos em camadas de alguns agregados. Por exemplo, você não pode categorizar dados de volumes do SnapLock ou de configurações do MetroCluster. Consulte a documentação do ONTAP para obter "Funcionalidade ou recursos não suportados pelo FabricPool"informações sobre .

O Cloud Tiering é compatível com FlexGroup volumes. A configuração funciona da mesma forma que qualquer outro volume.

Criação ou comutação de conetores

Um conector é necessário para categorizar dados na nuvem. Ao categorizar dados no Google Cloud Storage, um conetor deve estar disponível em uma VPC do Google Cloud Platform. Você precisará criar um novo conetor ou certificar-se de que o conetor selecionado atualmente reside no GCP.

- "Saiba mais sobre conetores"
- "Criando um conetor no GCP"
- "Comutação entre conetores"

Preparar a rede para o conetor

Certifique-se de que o conetor tem as ligações de rede necessárias.

Passos

1. Verifique se a VPC onde o conetor está instalado habilita as seguintes conexões:
   - Uma conexão de saída à Internet para o serviço Cloud Tiering pela porta 443 (HTTPS)
   - Uma conexão HTTPS pela porta 443 ao Google Cloud Storage
   - Uma conexão HTTPS pela porta 443 aos clusters do ONTAP
2. Opcional: Ative o acesso privado do Google na sub-rede onde pretende implementar o Service Connector.

   "Acesso privado ao Google" O é recomendado se você tiver uma conexão direta do cluster do ONTAP com a VPC e quiser que a comunicação entre o conetor e o Google Cloud Storage permaneça em sua rede virtual privada. Observe que o Private Google Access funciona com instâncias de VM que possuem apenas endereços IP internos (privados) (sem endereços IP externos).

Preparação do Google Cloud Storage para categorização de dados

Ao configurar a disposição em camadas, você precisa fornecer chaves de acesso ao storage para uma conta de serviço que tenha permissões de administrador do storage. Uma conta de serviço permite que o Cloud Tiering autentique e acesse buckets do Cloud Storage usados para categorização de dados. As chaves são necessárias para que o Google Cloud Storage saiba quem está fazendo a solicitação.

Passos

1. "Crie uma conta de serviço que tenha a função de administrador de storage predefinida".
2. Vá para "Configurações de armazenamento do GCP" e crie chaves de acesso para a conta de serviço:
   a. Selecione um projeto e clique em **interoperabilidade**. Se ainda não o fez, clique em **Ativar acesso à interoperabilidade**.
   b. Em **chaves de acesso para contas de serviço**, clique em **criar uma chave para uma conta de serviço**, selecione a conta de serviço que acabou de criar e clique em **criar chave**.

      Você precisará "Insira as chaves no Cloud Tiering" mais tarde quando configurar a disposição em camadas.

Disposição em camadas dos dados inativos do primeiro cluster para o Google Cloud Storage

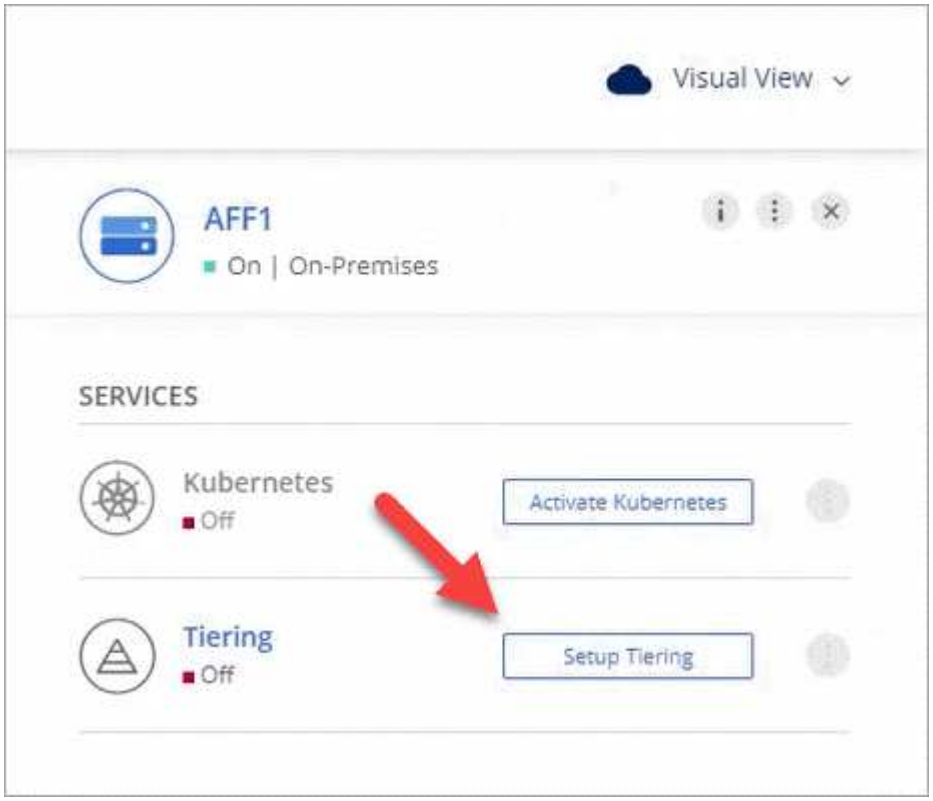
Depois de preparar seu ambiente do Google Cloud, comece a categorizar os dados inativos no primeiro cluster.

O que você vai precisar

- "Um ambiente de trabalho no local".
- Chaves de acesso de armazenamento para uma conta de serviço que tem a função Administrador de armazenamento.

Passos

1. Selecione um cluster no local.
2. Clique em **Configuração em categorias**.

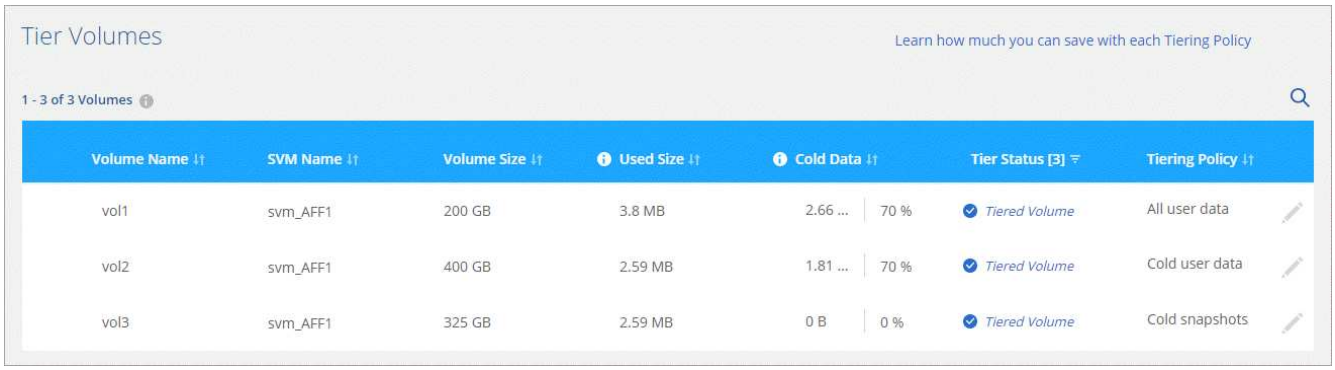


Agora você está no painel de disposição em camadas.

3. Clique em **Configurar disposição em camadas** ao lado do cluster.
4. Conclua as etapas na página **Configuração de categorias**:
   a. **Bucket**: Adicione um novo bucket do Google Cloud Storage ou selecione um bucket existente e clique em **continuar**.
   b. **Classe de armazenamento**: Selecione a classe de armazenamento que deseja usar para os dados em camadas e clique em **continuar**.
   c. **Credenciais**: Insira a chave de acesso ao armazenamento e a chave secreta para uma conta de serviço que tenha a função Administrador do armazenamento.
   d. **Rede de cluster**: Selecione o espaço IPspace que o ONTAP deve usar para se conetar ao armazenamento de objetos e clique em **continuar**.

      A seleção do espaço de IPspace correto garante que a disposição em camadas na nuvem possa configurar uma conexão do ONTAP ao armazenamento de objetos do seu provedor de nuvem.
5. Clique em **continuar** para selecionar os volumes que deseja categorizar.
6. Na página **volumes de nível**, configure a disposição em categorias para cada volume. Clique no ícone, selecione uma política de disposição em camadas, ajuste opcionalmente os dias de resfriamento e clique em **aplicar**.

   "Saiba mais sobre as políticas de disposição em camadas de volume".



Resultado

Você configurou com sucesso a disposição de dados em categorias de volumes no cluster para o storage de objetos do Google Cloud.

O que se segue?

"Certifique-se de se inscrever no serviço Cloud Tiering".

Você também pode adicionar clusters adicionais ou analisar informações sobre os dados ativos e inativos no cluster. Para obter detalhes, "Gerenciamento de categorização de dados nos clusters"consulte .

Disposição de dados em camadas de clusters ONTAP on-premises para o StorageGRID

Liberar espaço nos clusters do ONTAP no local ao dispor dados em camadas no StorageGRID. A disposição em camadas de dados é baseada no serviço de disposição em camadas na nuvem do NetApp.

Início rápido

Comece rapidamente seguindo estas etapas ou role para baixo até as seções restantes para obter detalhes completos.

1 Prepare-se para categorizar dados no StorageGRID

Você precisa do seguinte:

- Um sistema AFF ou FAS com agregados all-SSD que está executando o ONTAP 9.4 ou posterior e uma conexão em uma porta especificada pelo usuário para o StorageGRID.
- StorageGRID 10,3 ou posterior com chaves de acesso AWS que têm permissões S3.
- Um conetor instalado nas suas instalações.
- Rede para o conetor que habilita uma conexão HTTPS de saída ao cluster ONTAP, ao StorageGRID e ao serviço de disposição em camadas na nuvem.

2 Configurar a disposição em camadas

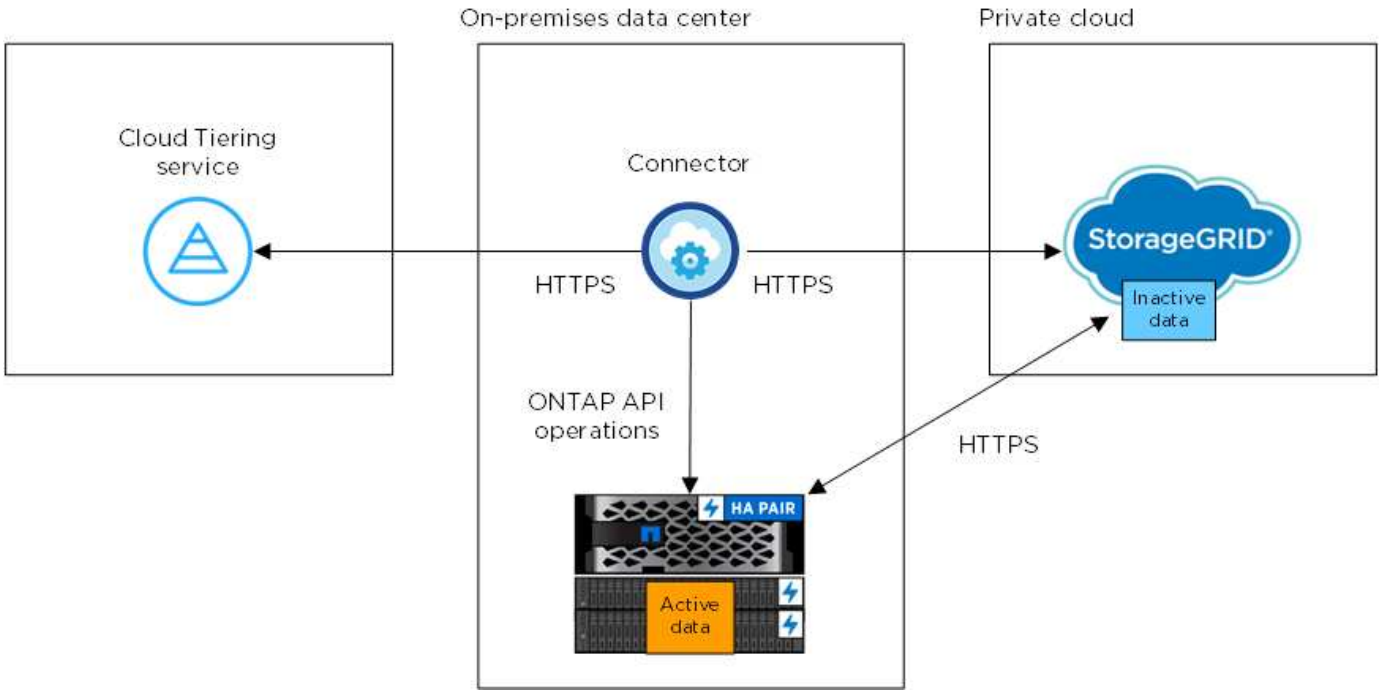
Selecione um ambiente de trabalho local, clique em **Configuração de disposição em camadas** e siga as

instruções para colocar dados em camadas no StorageGRID.

Requisitos

Verifique o suporte para o cluster ONTAP, configure a rede e prepare o armazenamento de objetos.

A imagem a seguir mostra cada componente e as conexões que você precisa preparar entre eles:



A comunicação entre o conetor e o StorageGRID destina-se apenas à configuração de armazenamento de objetos.

Preparando os clusters do ONTAP

Os clusters do ONTAP precisam atender aos requisitos a seguir ao categorizar dados no StorageGRID.

Plataformas ONTAP compatíveis

O Cloud Tiering dá suporte a sistemas AFF e agregados all-SSD em sistemas FAS.

Versão ONTAP suportada

ONTAP 9 .4 ou posterior

Licenciamento

Não é necessária uma licença do FabricPool no cluster do ONTAP ao categorizar dados no StorageGRID.

Requisitos de rede de cluster

- O cluster do ONTAP inicia uma conexão HTTPS por uma porta especificada pelo usuário para o StorageGRID (a porta é configurável durante a configuração de disposição em camadas).

  O ONTAP lê e grava dados no storage de objetos. O armazenamento de objetos nunca inicia, ele apenas responde.

- Uma conexão de entrada é necessária a partir do conetor, que deve residir em suas instalações.

Não é necessária uma conexão entre o cluster e o serviço Cloud Tiering.

- É necessário um LIF entre clusters em cada nó do ONTAP que hospeda volumes dispostos em camadas. O LIF deve estar associado ao *IPspace* que o ONTAP deve usar para se conetar ao armazenamento de objetos.

  Os IPspaces permitem a segregação de tráfego de rede, permitindo a separação do tráfego de clientes para privacidade e segurança. "Saiba mais sobre IPspaces".

  Quando você configura a disposição de dados em categorias, o Cloud Tiering solicita que você use o espaço IPspace. Você deve escolher o espaço IPspace ao qual cada LIF está associado. Esse pode ser o espaço IPspace "padrão" ou um espaço IPspace personalizado que você criou.

Volumes e agregados compatíveis

O número total de volumes em que o Cloud Tiering pode ser menor que o número de volumes no sistema ONTAP. Isso porque os volumes não podem ser dispostos em camadas de alguns agregados. Por exemplo, você não pode categorizar dados de volumes do SnapLock ou de configurações do MetroCluster. Consulte a documentação do ONTAP para obter "Funcionalidade ou recursos não suportados pelo FabricPool"informações sobre .

O Cloud Tiering é compatível com volumes FlexGroup, a partir do ONTAP 9.5. A configuração funciona da mesma forma que qualquer outro volume.

Preparando o StorageGRID

O StorageGRID deve atender aos seguintes requisitos.

Versões suportadas do StorageGRID

StorageGRID 10,3 e posterior são suportados.

S3 credenciais

Ao configurar a disposição em camadas no StorageGRID, você precisa fornecer ao Cloud Tiering uma chave de acesso ao S3 e uma chave secreta. O Cloud Tiering usa as chaves para acessar seus buckets.

Essas chaves de acesso devem estar associadas a um usuário que tenha as seguintes permissões:

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket"
```

Controle de versão de objetos

Você não deve habilitar o controle de versão de objetos do StorageGRID no bucket do armazenamento de objetos.

Criação ou comutação de conetores

Um conector é necessário para categorizar dados na nuvem. Ao colocar os dados em categorias no

StorageGRID, um conector precisa estar disponível no local. Você precisará instalar um novo conetor ou certificar-se de que o conetor selecionado atualmente reside no local.

- "Saiba mais sobre conetores"
- "Requisitos do host do conetor"
- "Instalar o conetor em um host Linux existente"
- "Comutação entre conetores"

Preparar a rede para o conetor

Certifique-se de que o conetor tem as ligações de rede necessárias.

Passos

1. Certifique-se de que a rede onde o conetor está instalado permite as seguintes ligações:
    - Uma conexão de saída à Internet para o serviço Cloud Tiering pela porta 443 (HTTPS)
    - Uma conexão HTTPS pela porta 443 para o StorageGRID
    - Uma conexão HTTPS pela porta 443 aos clusters do ONTAP

Disposição em camadas dos dados inativos do primeiro cluster no StorageGRID

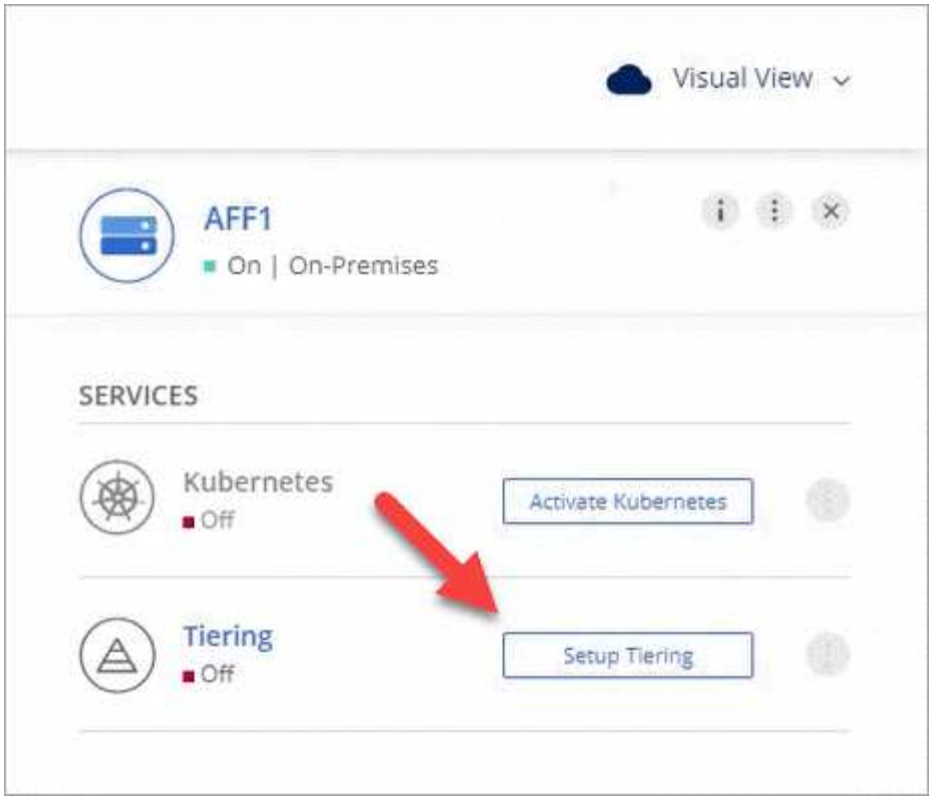
Depois de preparar seu ambiente, comece a categorizar os dados inativos do primeiro cluster.

O que você vai precisar

- "Um ambiente de trabalho no local".
- Uma chave de acesso da AWS que tem as permissões S3 necessárias.

Passos

1. Selecione um cluster no local.
2. Clique em **Configuração em categorias**.

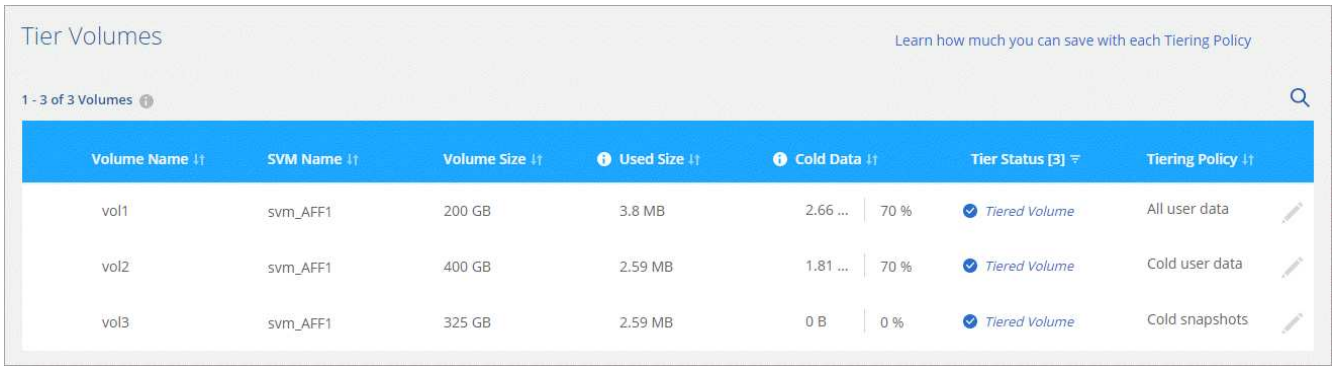


Agora você está no painel de disposição em camadas.

3. Clique em **Configurar disposição em camadas** ao lado do cluster.
4. Conclua as etapas na página **Configuração de categorias**:
   a. **Escolha seu provedor**: Selecione StorageGRID.
   b. **Servidor**: Insira o FQDN do servidor StorageGRID, insira a porta que o ONTAP deve usar para comunicação HTTPS com o StorageGRID e insira a chave de acesso e a chave secreta para uma conta AWS que tenha as permissões S3 necessárias.
   c. **Bucket**: Adicione um novo bucket ou selecione um bucket existente para os dados em camadas.
   d. **Rede de cluster**: Selecione o espaço IPspace que o ONTAP deve usar para se conetar ao armazenamento de objetos e clique em **continuar**.

      A seleção do espaço de IPspace correto garante que a disposição em camadas na nuvem possa configurar uma conexão do ONTAP ao armazenamento de objetos do seu provedor de nuvem.
5. Clique em **continuar** para selecionar os volumes que deseja categorizar.
6. Na página **volumes de nível**, configure a disposição em categorias para cada volume. Clique no ícone, selecione uma política de disposição em camadas, ajuste opcionalmente os dias de resfriamento e clique em **aplicar**.

   "Saiba mais sobre as políticas de disposição em camadas de volume".



Resultado

Você configurou com sucesso a disposição de dados em categorias de volumes no cluster para o StorageGRID.

O que se segue?

Você pode adicionar clusters adicionais ou analisar informações sobre os dados ativos e inativos no cluster. Para obter detalhes, "Gerenciamento de categorização de dados nos clusters"consulte .

Configurar o licenciamento para o Cloud Tiering

Pague pelo categorização de nuvem com uma subscrição com pagamento conforme o uso, uma licença de disposição em camadas do ONTAP chamada *FabricPool* ou uma combinação de ambos. Se você quiser pagar conforme o uso, precisará se inscrever no mercado do fornecedor de nuvem ao qual deseja categorizar dados inativos. Não há necessidade de se inscrever em todos os mercados.

Algumas notas antes de ler mais:

- Se uma licença do FabricPool já estiver instalada no cluster, tudo estará pronto. Não há mais nada que você precise fazer.
- Se você já se inscreveu na assinatura do Cloud Manager no mercado do seu provedor de nuvem, também será automaticamente inscrito no Cloud Tiering. Você verá uma assinatura ativa na guia Cloud Tiering **Licenciamento**. Você não precisará se inscrever novamente.
- Não há cobrança ao categorizar dados no StorageGRID. Nem uma licença BYOL ou Registro PAYGO são necessários.

"Saiba mais sobre como o licenciamento funciona para o Cloud Tiering".

Subscrever a partir do AWS Marketplace

Inscreva-se no AWS Marketplace para configurar uma assinatura de pagamento conforme o uso para categorização de dados dos clusters do ONTAP para o AWS S3.

Passos

1. No Cloud Manager, clique em **Categorização > Licenciamento**.
2. Clique em **Subscribe** no AWS Marketplace e clique em **Continue**.
3. Inscreva-se no AWS Marketplace e faça login novamente no Cloud Central para concluir o Registro.

O vídeo a seguir mostra o processo:

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

Subscrever a partir do Azure Marketplace

Inscreva-se no Cloud Tiering no Azure Marketplace para configurar uma assinatura de pagamento conforme o uso para categorização de dados dos clusters ONTAP para o storage Azure Blob.

Passos

1. No Cloud Manager, clique em **Categorização > Licenciamento**.
2. Clique em **Subscribe** no Azure Marketplace e, em seguida, clique em **Continue**.
3. Assine a partir do Azure Marketplace e, em seguida, faça login novamente no Cloud Central para concluir o Registro.

   O vídeo a seguir mostra o processo:

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

Subscrever a partir do GCP Marketplace

Inscreva-se no Cloud Tiering no mercado do GCP para configurar uma assinatura de pagamento conforme o uso para categorização de dados dos clusters do ONTAP ao storage do Google Cloud.

Passos

1. No Cloud Manager, clique em **Categorização > Licenciamento**.
2. Clique em **Inscrever-se** no GCP Marketplace e clique em **continuar**.
3. Assine no GCP Marketplace e faça login novamente no Cloud Central para concluir o Registro.

   o vídeo a seguir mostra o processo:

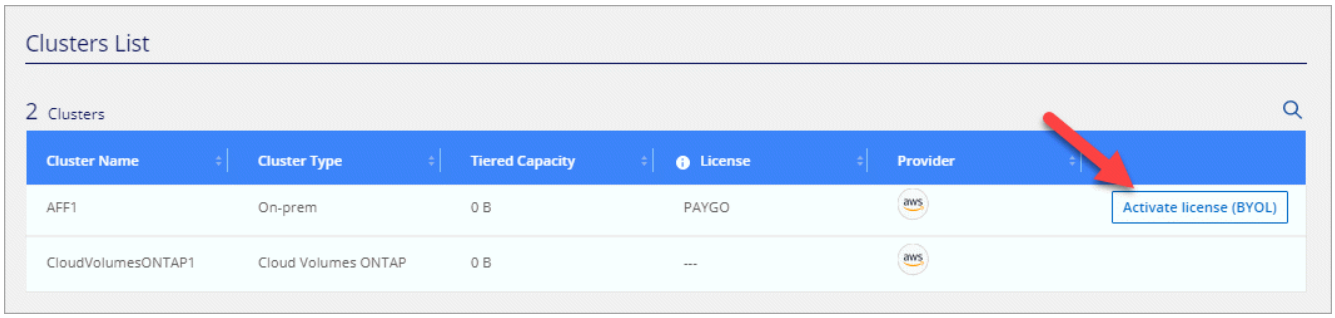
   ► https://docs.netapp.com/pt-br/occm38//media/video_subscribing_gcp_tiering.mp4 *(video)*

Adição de uma licença de disposição em camadas ao ONTAP

Traga sua própria licença comprando uma licença ONTAP FabricPool da NetApp.

Passos

1. Se você não tem uma licença FabricPool, mailto:ng-cloud-Tiering em NetApp.com?subject-Licensing [entre em Contato conosco para comprar uma].
2. No Cloud Manager, clique em **Categorização > Licenciamento**.
3. Na tabela Lista de clusters, clique em **Ativar licença (BYOL)** para um cluster ONTAP on-premise.



4. Introduza o número de série da licença e, em seguida, introduza a conta do site de suporte da NetApp associada ao número de série.
5. Clique em **Ativar licença**.

Resultado

O Cloud Tiering Registra a licença e a instala no cluster.

Depois de terminar

Se você adquirir capacidade adicional posteriormente, a licença no cluster será atualizada automaticamente com a nova capacidade. Não é necessário aplicar um novo ficheiro de licença NetApp (NLF) ao cluster.

Gerenciamento de categorização de dados nos clusters

Agora que você configurou a disposição de dados em categorias dos clusters do ONTAP, pode categorizar dados de volumes adicionais, alterar a política de disposição em categorias de um volume e muito mais.

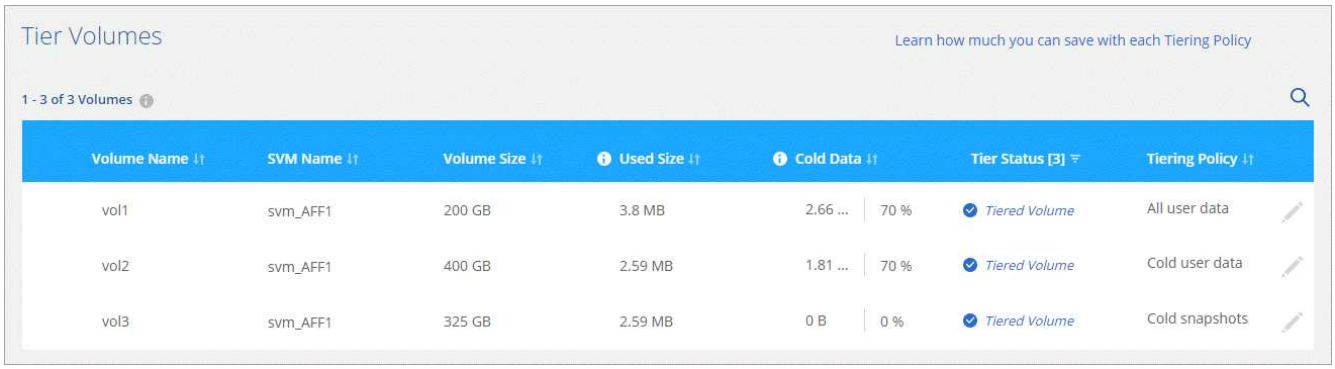
Disposição em camadas de dados de volumes adicionais

Configure a disposição de dados em categorias para volumes adicionais a qualquer momento, por exemplo, depois de criar um novo volume.

Passos

1. Na parte superior do Cloud Manager, clique em **Categorização**.
2. No **Painel de cluster**, clique em **volumes de nível** para o cluster.
3. Para cada volume, clique no  ícone, selecione uma política de disposição em camadas, ajuste opcionalmente os dias de resfriamento e clique em **aplicar**.

   "Saiba mais sobre as políticas de disposição em camadas de volume".



Não é necessário configurar o armazenamento de objetos porque ele já estava configurado quando você configurou a disposição em camadas inicialmente para o cluster. O ONTAP categorizará os dados inativos desses volumes no mesmo armazenamento de objetos.

4. Quando terminar, clique em **Fechar**.

Alteração da política de disposição em camadas de um volume

A alteração da política de disposição em camadas de um volume altera a forma como o ONTAP classifica os dados inativos no storage de objetos. A alteração começa a partir do momento em que você altera a política - ela altera apenas o comportamento de disposição em camadas subsequente para o volume.

Passos

1. Na parte superior do Cloud Manager, clique em **Categorização**.
2. No **Painel de cluster**, clique em **volumes de nível** para o cluster.
3. Clique no  ícone, selecione uma política de disposição em camadas, ajuste opcionalmente os dias de resfriamento e clique em **aplicar**.

   "Saiba mais sobre as políticas de disposição em camadas de volume".

Gerenciamento de configurações de disposição em camadas em agregados

Cada agregado tem duas configurações que você pode ajustar: O limite de preenchimento de categorias e se o relatório de dados inativos está ativado.

Disposição em camadas no limite de plenitude

Definir o limite para um número menor reduz a quantidade de dados necessária para ser armazenada na camada de performance antes da disposição em categorias. Isso pode ser útil para grandes agregados que contêm poucos dados ativos.

Definir o limite para um número maior aumenta a quantidade de dados necessários para serem armazenados na camada de performance antes da disposição em camadas. Isso pode ser útil para soluções projetadas para categorizar somente quando os agregados estiverem próximos da capacidade máxima.

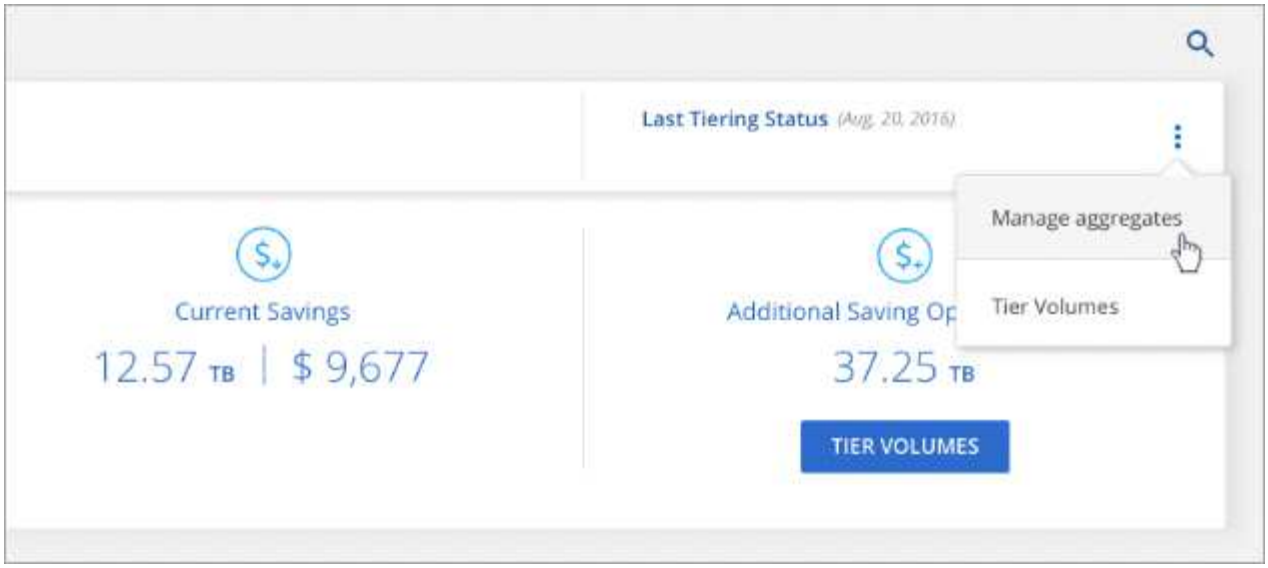
Relatórios de dados inativos

O relatório de dados inativos (IDR) usa um período de resfriamento de 31 dias para determinar quais dados são considerados inativos. A quantidade de dados inativos em camadas depende das políticas de disposição em camadas definidas nos volumes. Essa quantidade pode ser diferente da quantidade de dados frios detetados pelo IDR usando um período de resfriamento de 31 dias.

É melhor manter o IDR ativado porque ajuda a identificar seus dados inativos e oportunidades de economia. O IDR deve permanecer habilitado se a disposição de dados tiver sido ativada em um agregado.

Passos

1. Na parte superior do Cloud Manager, clique em **Categorização**.
2. Na página **disposição em camadas na nuvem**, clique no ícone de menu de um cluster e selecione **Gerenciar agregados**.



3. Na página **Gerenciar agregados**, clique no ícone de um agregado na tabela.
4. Modifique o limite de preenchimento e escolha se deseja ativar ou desativar o relatório de dados inativos.

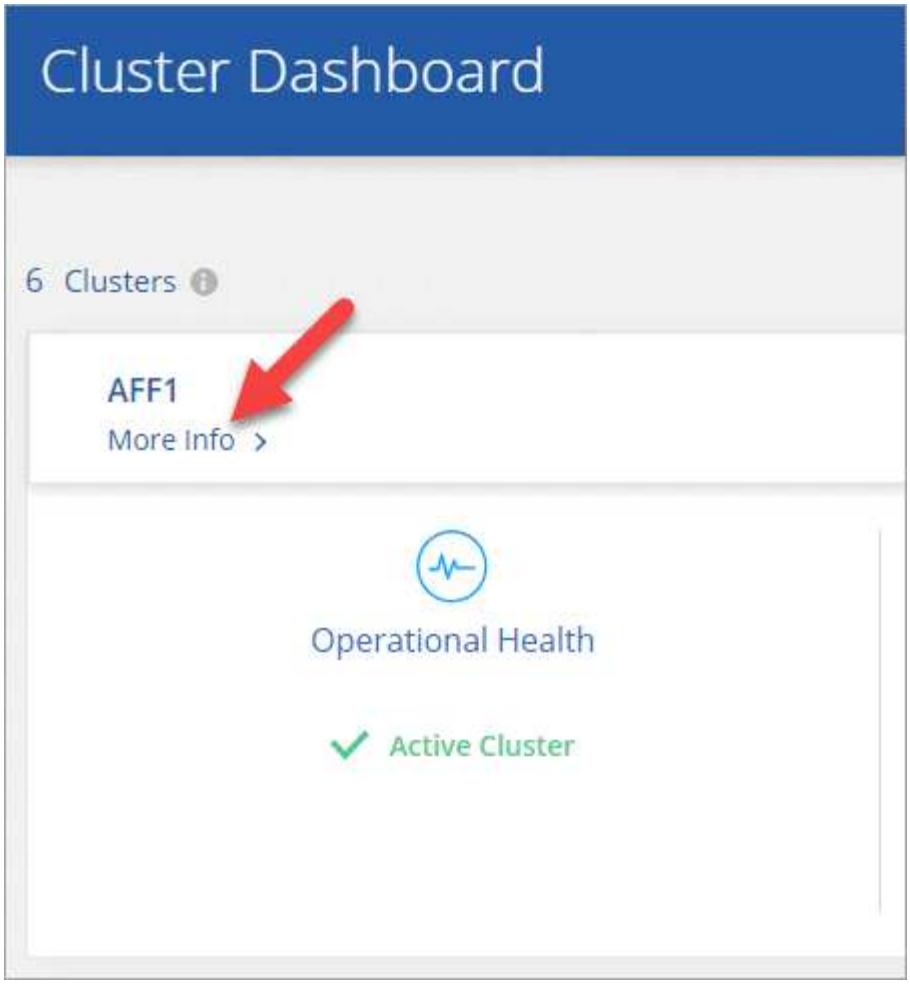
5. Clique em **aplicar**.

Analisar as informações de disposição em camadas de um cluster

Talvez você queira ver a quantidade de dados na camada de nuvem e a quantidade de dados nos discos. Ou, talvez você queira ver a quantidade de dados ativos e inativos nos discos do cluster. O Cloud Tiering fornece essas informações para cada cluster.

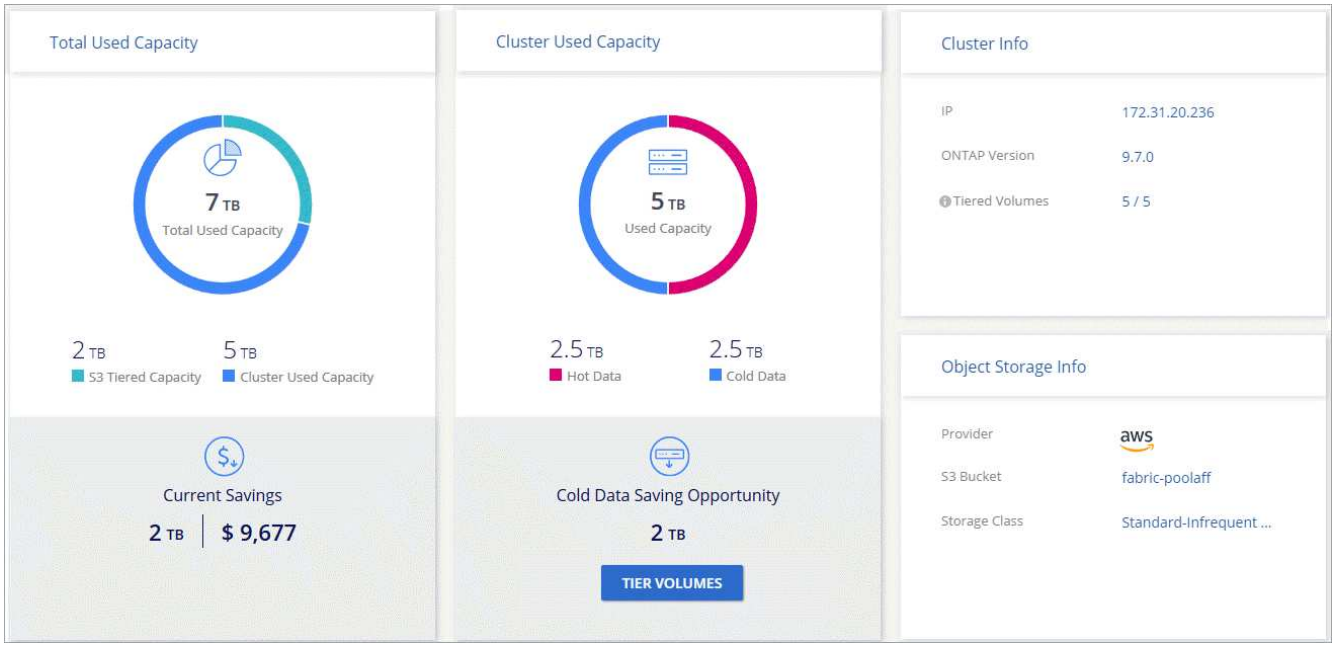
Passos

1. Na parte superior do Cloud Manager, clique em **Categorização**.
2. No **Painel de cluster**, clique em **mais informações** para um cluster.



3. Reveja os detalhes sobre o cluster.

   Aqui está um exemplo:

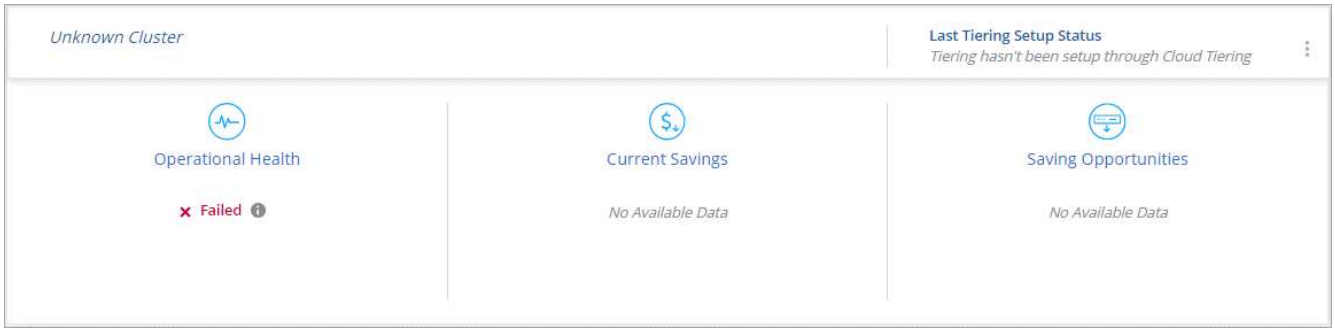


Fixação da saúde operacional

Falhas podem acontecer. Quando isso acontece, o Cloud Tiering exibe um status de integridade operacional "Falha" no Painel de cluster. A integridade reflete o status do sistema ONTAP e do Cloud Manager.

Passos

1. Identifique quaisquer clusters que tenham uma integridade operacional de "Falha".



2. Passe o Mouse sobre o ícone para ver o motivo da falha.
3. Corrija o problema:
   a. Verifique se o cluster do ONTAP está operacional e se ele tem uma conexão de entrada e saída para seu provedor de storage de objetos.
   b. Verifique se o Cloud Manager tem conexões de saída para o serviço Cloud Tiering, para o armazenamento de objetos e para os clusters ONTAP detetados.

FAQ técnico do Cloud Tiering

Este FAQ pode ajudar se você está apenas procurando uma resposta rápida para uma pergunta.

ONTAP

As seguintes perguntas dizem respeito ao ONTAP.

Quais são os requisitos para o meu cluster ONTAP?

Depende de onde você categoriza os dados inativos. Consulte o seguinte:

- "Disposição em camadas de dados de clusters ONTAP on-premises para o Amazon S3"
- "Disposição em camadas de dados de clusters ONTAP on-premises para o storage Azure Blob"
- "Disposição de dados em camadas de clusters ONTAP on-premises para o Google Cloud Storage"
- "Disposição de dados em camadas de clusters ONTAP on-premises para o StorageGRID"

O Cloud Tiering permite relatórios de dados inativos?

Sim, o Cloud Tiering permite que você crie relatórios de dados inativos em cada agregado. Essa configuração nos permite identificar a quantidade de dados inativos que podem ser dispostos em camadas em armazenamento de objetos de baixo custo.

Posso categorizar dados de volumes nas e volumes SAN?

Você pode usar o Cloud Tiering para categorizar dados de volumes nas para a nuvem pública e de volumes SAN para uma nuvem privada usando o StorageGRID.

E o Cloud Volumes ONTAP?

Se você tiver sistemas Cloud Volumes ONTAP, encontrá-los-á no painel do cluster para que você veja uma visão completa da disposição de dados em categorias na sua infraestrutura de nuvem híbrida.

No Dashboard do cluster, você pode visualizar informações em categorias semelhantes a um cluster do ONTAP no local: Integridade operacional, economia atual, oportunidades de economia, detalhes sobre volumes e agregados e muito mais.

Os sistemas Cloud Volumes ONTAP são somente leitura no Cloud Tiering. Não é possível configurar a disposição de dados em categorias no Cloud Volumes ONTAP a partir do Cloud Tiering. Você ainda configurará a disposição em camadas da mesma maneira: Do ambiente de trabalho no Cloud Manager.

Storage de objetos

As perguntas a seguir estão relacionadas ao armazenamento de objetos.

Quais fornecedores de storage de objetos são compatíveis?

O Amazon S3, o storage Azure Blob, o Google Cloud Storage e o StorageGRID usando o protocolo S3 são compatíveis.

Posso usar meu próprio balde/recipiente?

Sim, você pode. Ao configurar a disposição de dados em categorias, você pode adicionar um novo bucket/contêiner ou selecionar um bucket/contêiner existente.

Quais regiões são suportadas?

- "Regiões AWS compatíveis"
- "Regiões Azure compatíveis"
- "Regiões compatíveis do Google Cloud"

Quais classes de armazenamento S3 são suportadas?

O Cloud Tiering oferece suporte à disposição em camadas de dados para as classes de armazenamento *Standard*, *Standard-Uncasable Access*, *One Zone-IA* ou *Intelligent*. "Classes de armazenamento S3 suportadas"Consulte para obter mais detalhes.

Quais camadas de acesso do Blob do Azure são compatíveis?

O Cloud Tiering usa automaticamente o nível *Hot* Access para seus dados inativos.

Quais classes de armazenamento são compatíveis com o Google Cloud Storage?

O Cloud Tiering usa a classe de armazenamento *Standard* para dados inativos.

O Cloud Tiering usa um armazenamento de objetos para todo o cluster ou um por agregado?

Um armazenamento de objetos para todo o cluster.

Posso aplicar políticas ao meu armazenamento de objetos para mover dados independentemente da disposição em camadas?

Não, o Cloud Tiering não é compatível com regras de gerenciamento do ciclo de vida do objeto que movem ou excluem dados de armazenamentos de objetos.

Conetores

As seguintes questões dizem respeito aos conetores.

Onde o conetor precisa ser instalado?

- Ao categorizar os dados no S3, um conector pode residir em uma VPC da AWS ou no local.
- Ao categorizar dados no storage Blob, um conector deve residir em um Azure VNet.
- Ao categorizar dados no Google Cloud Storage, um conector deve residir em uma VPC do Google Cloud Platform.
- Ao categorizar dados no StorageGRID, um conector deve residir em um host Linux no local.

Rede

As seguintes perguntas dizem respeito à rede.

Quais são os requisitos de rede?

- O cluster do ONTAP inicia uma conexão HTTPS pela porta 443 ao seu provedor de storage de objetos.

  O ONTAP lê e grava dados no storage de objetos. O armazenamento de objetos nunca inicia, ele apenas responde.

- Para o StorageGRID, o cluster do ONTAP inicia uma conexão HTTPS por uma porta especificada pelo usuário para o StorageGRID (a porta é configurável durante a configuração de disposição em camadas).
- Um conector precisa de uma conexão HTTPS de saída pela porta 443 para os clusters do ONTAP, para o armazenamento de objetos e para o serviço de disposição em camadas na nuvem.

Para obter mais detalhes, consulte:

- "Disposição em camadas de dados de clusters ONTAP on-premises para o Amazon S3"
- "Disposição em camadas de dados de clusters ONTAP on-premises para o storage Azure Blob"
- "Disposição de dados em camadas de clusters ONTAP on-premises para o Google Cloud Storage"
- "Disposição de dados em camadas de clusters ONTAP on-premises para o StorageGRID"

Permissões

As perguntas a seguir se referem às permissões.

Quais permissões são necessárias na AWS?

As permissões são "Para gerir o balde S3"necessárias .

Quais permissões são necessárias no Azure?

Não são necessárias permissões extras fora das permissões que você precisa fornecer ao Cloud Manager.

Quais permissões são necessárias no Google Cloud Platform?

As permissões de administrador de armazenamento são necessárias para uma conta de serviço que tenha chaves de acesso ao armazenamento.

Quais permissões são necessárias para o StorageGRID?

"S3 permissões são necessárias".

Referência

Classes e regiões de armazenamento S3 compatíveis

O Cloud Tiering é compatível com várias classes de storage S3 e a maioria das regiões.

Classes de armazenamento S3 suportadas

O Cloud Tiering pode aplicar uma regra de ciclo de vida para que os dados transitem da classe de armazenamento *Standard* para outra classe de armazenamento após 30 dias. Você pode escolher entre as seguintes classes de armazenamento:

- Acesso padrão-infrequente
- Uma zona-IA
- Inteligente

Se você escolher padrão, os dados permanecerão nessa classe de storage.

"Saiba mais sobre as classes de armazenamento S3".

Regiões AWS compatíveis

O Cloud Tiering é compatível com as seguintes regiões da AWS.

Ásia-Pacífico

- Mumbai
- Seul
- Singapura
- Sydney
- Tóquio

Europa

- Frankfurt
- Irlanda
- Londres
- Paris
- Estocolmo

América do Norte

- Canadá Central
- GovCloud (US-West) – começando com ONTAP 9.3
- Leste DOS EUA (Norte da Virgínia)
- Leste DOS EUA (Ohio)
- Oeste DOS EUA (Norte da Califórnia)
- Oeste DOS EUA (Oregon)

América do Sul

- São Paulo

Camadas e regiões de acesso Blob do Azure compatíveis

O Cloud Tiering é compatível com o nível de acesso *Hot* e a maioria das regiões.

Camadas de acesso Azure Blob compatíveis

Quando você configura a disposição de dados em categorias no Azure, o Cloud Tiering usa automaticamente o nível *Hot* Access para seus dados inativos.

Regiões Azure compatíveis

O Cloud Tiering é compatível com as seguintes regiões do Azure.

África

- África do Sul Norte

Ásia-Pacífico

- Leste da Austrália
- Sudeste da Austrália
- Leste da Ásia
- Leste do Japão
- Oeste do Japão
- Coreia Central
- Coreia do Sul

- Sudeste da Ásia

Europa

- França Central
- Alemanha Central
- Alemanha Nordeste
- Norte da Europa
- Sul do Reino Unido
- Oeste do Reino Unido
- Europa Ocidental

América do Norte

- Canadá Central
- Leste do Canadá
- Central US
- Leste dos EUA
- East US 2
- North Central US
- South Central US
- Oeste dos EUA
- West US 2
- West Central US

América do Sul

- Brasil Sul

Regiões e classes de armazenamento do Google Cloud compatíveis

O Cloud Tiering é compatível com a classe de storage padrão e a maioria das regiões do Google Cloud.

Camadas de acesso compatíveis

O Cloud Tiering usa o nível *Standard* Access para seus dados inativos.

Regiões compatíveis do Google Cloud

O Cloud Tiering é compatível com as seguintes regiões.

Américas

- Iowa
- Los Angeles

- Montreal
- N. Virginia
- Oregon
- Sao Paulo
- Carolina do Sul

Ásia-Pacífico

- Hong Kong
- Mumbai
- Osaka
- Singapura
- Sydney
- Taiwan
- Tóquio

Europa

- Bélgica
- Finlândia
- Frankfurt
- Londres
- Países Baixos
- Zurique

Visualização dos buckets do Amazon S3

Depois de instalar um conetor na AWS, o Cloud Manager poderá descobrir automaticamente informações sobre os buckets do Amazon S3 que residem na conta da AWS onde ele é instalado.

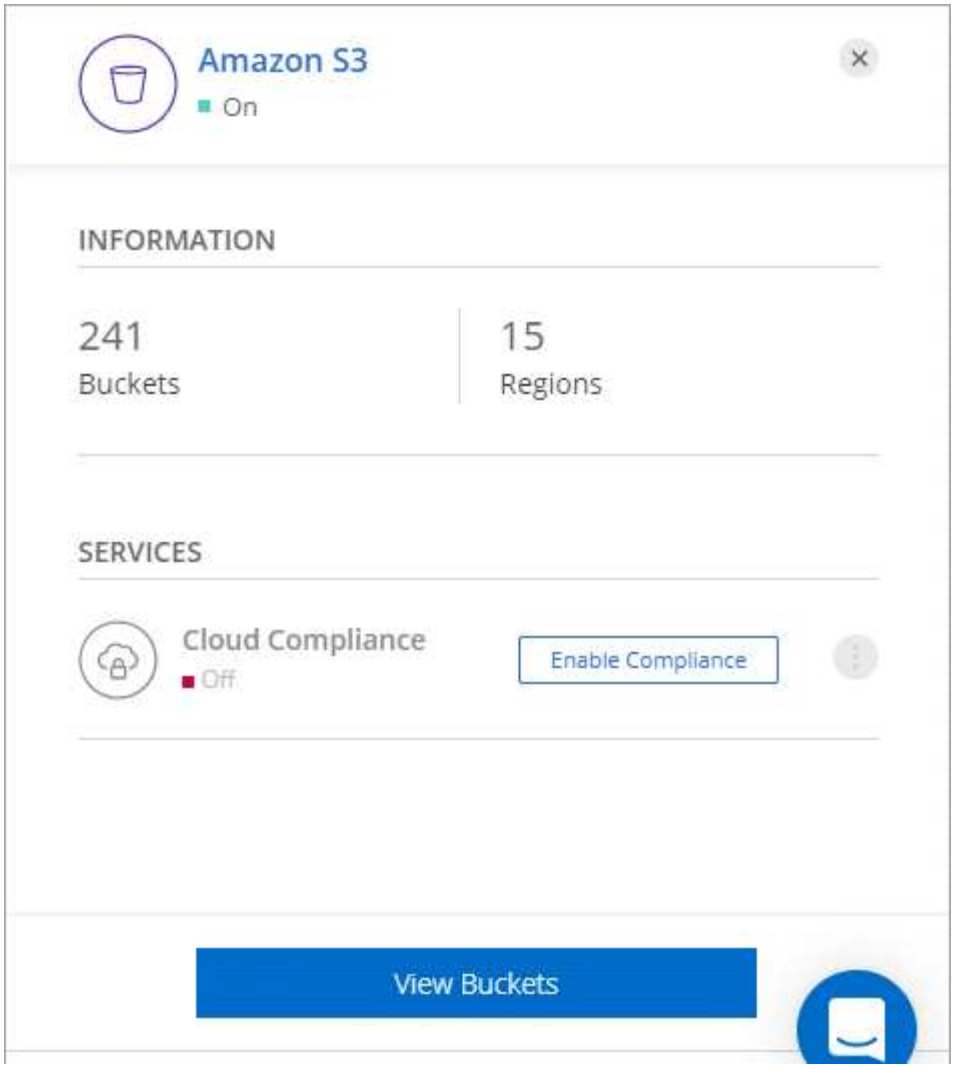
Você pode ver detalhes sobre os buckets do S3, incluindo a região, nível de acesso, classe de storage e se o bucket é usado com o Cloud Volumes ONTAP para backups ou categorização de dados. E você pode verificar os buckets do S3 com o Cloud Compliance.

Passos

1. "Instale um conetor" Na conta da AWS onde você deseja exibir seus buckets do Amazon S3.

   Você deve ver automaticamente um ambiente de trabalho do Amazon S3 logo depois.

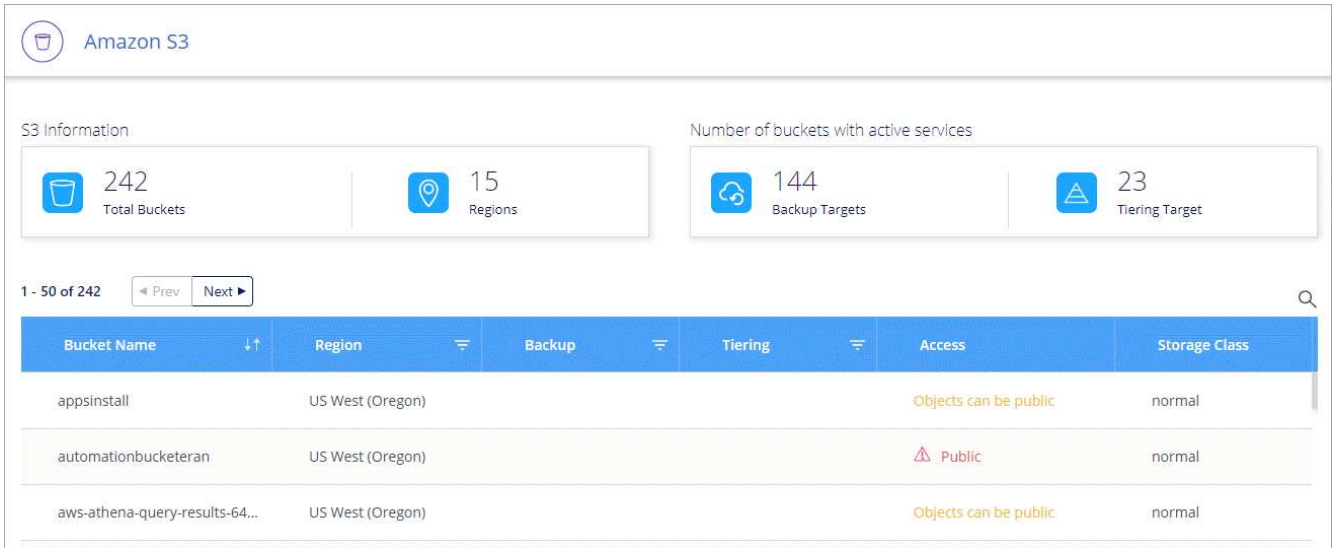
2. Clique no ambiente de trabalho e selecione uma ação no painel direito.



3. Clique em **Ativar conformidade** para verificar os buckets do S3 em busca de dados pessoais e confidenciais.

   Para obter mais detalhes, "Introdução ao Cloud Compliance para Amazon S3"consulte .

4. Clique em **Exibir buckets** para ver detalhes sobre os buckets do S3 na sua conta da AWS.



Administrar o Cloud Manager

Encontrando a ID do sistema do Cloud Manager

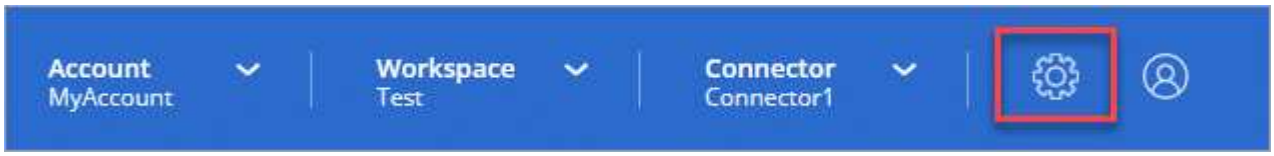
Para ajudá-lo a começar, seu representante da NetApp pode pedir a ID do sistema do Cloud Manager. O ID é normalmente utilizado para fins de licenciamento e resolução de problemas.

O que você vai precisar

Você precisa criar um conetor antes de alterar as configurações do Cloud Manager. "Saiba como".

Passos

1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações.



2. Clique em **Painel de suporte**.

   A ID do sistema aparece no canto superior direito.

   Exemplo

Gerenciar conetores

Gerenciamento de conetores existentes

Depois de criar um ou mais conetores, você pode gerenciá-los alternando entre conetores, conetando-se à interface de usuário local em execução em um conetor e muito mais.

Comutação entre conetores

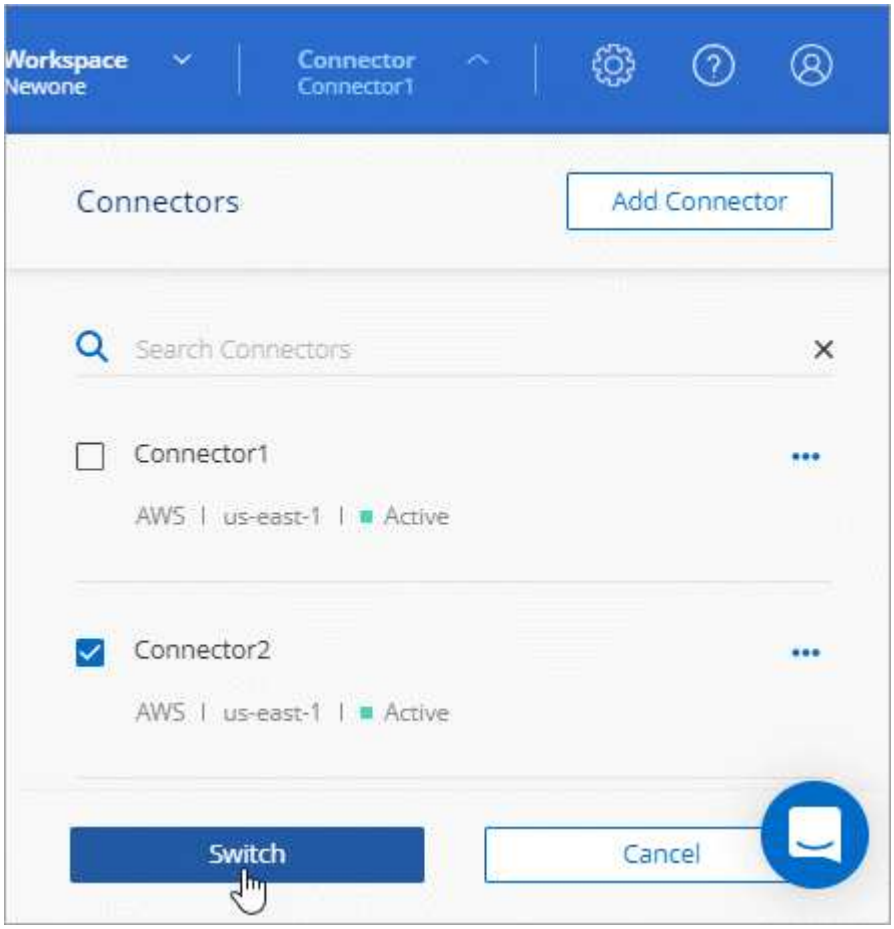
Se você tiver vários conetores, pode alternar entre eles para ver os ambientes de trabalho associados a um conetor específico.

Por exemplo, digamos que você está trabalhando em um ambiente multicloud. Você pode ter um conetor na

AWS e outro no Google Cloud. Você precisa alternar entre esses conetores para gerenciar os sistemas Cloud Volumes ONTAP executados nessas nuvens.

Passo

1. Clique no menu suspenso **Connector**, selecione outro conetor e clique em **Switch**.



O Cloud Manager atualiza e mostra os ambientes de trabalho associados ao conector selecionado.

Acessando a IU local

Embora você deva executar quase todas as tarefas a partir da interface de usuário SaaS, uma interface de usuário local ainda está disponível no conetor. Esta interface é necessária para algumas tarefas que precisam ser executadas a partir do próprio conetor:

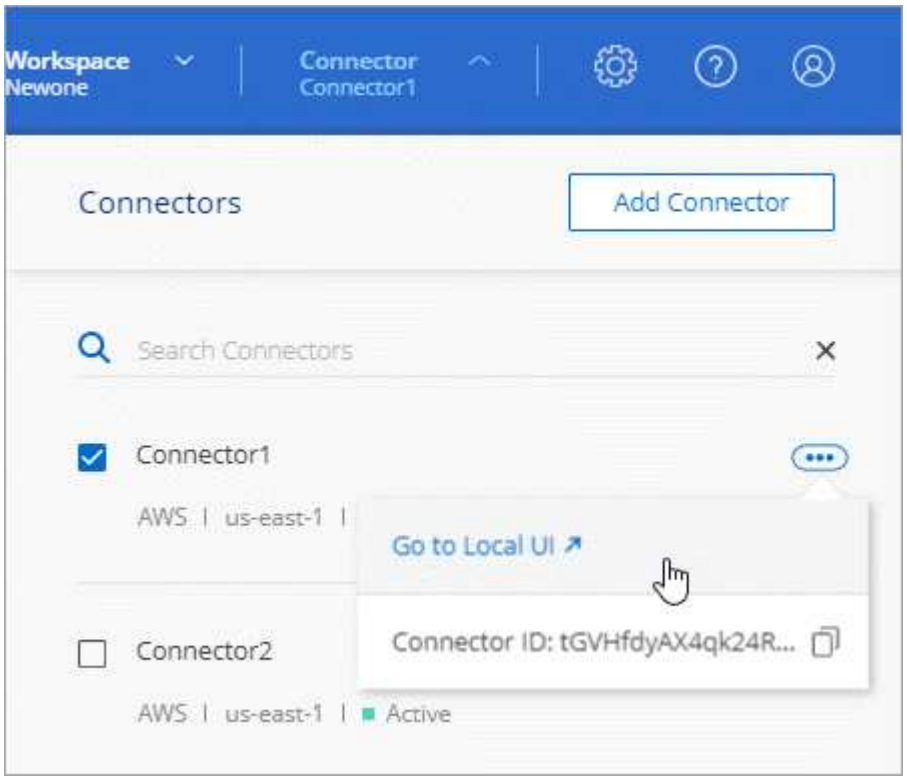
- "Configurando um servidor proxy"
- Instalando um patch (você normalmente trabalhará com o pessoal do NetApp para instalar um patch)
- Download de mensagens do AutoSupport (geralmente direcionadas pelo pessoal do NetApp quando você tiver problemas)

Passos

1. "Faça login na interface SaaS do Cloud Manager" De uma máquina que tenha uma conexão de rede com a instância do conetor.

   Se o conetor não tiver um endereço IP público, você precisará de uma conexão VPN ou precisará se conetar a partir de um host de salto que esteja na mesma rede que o conetor.

2. Clique no menu suspenso **Connector**, clique no menu de ação de um conetor e, em seguida, clique em **Go to local UI**.



A interface do Cloud Manager em execução no conetor é carregada em uma nova guia do navegador.

Removendo conetores do Cloud Manager

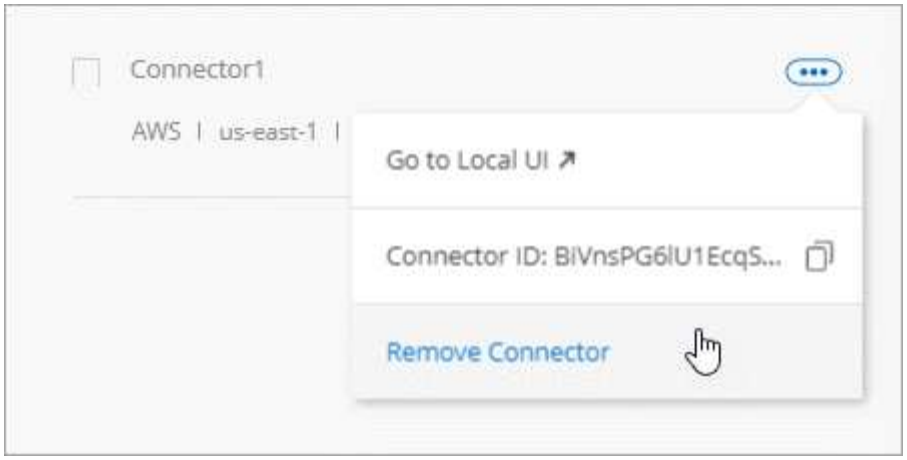
Se um conetor estiver inativo, você poderá removê-lo da lista de conetores no Cloud Manager. Pode fazê-lo se tiver eliminado a máquina virtual do conetor ou se tiver desinstalado o software do conetor.

Observe o seguinte sobre como remover um conetor:

- Esta ação não exclui a máquina virtual.
- Esta ação não pode ser revertida - uma vez que você remove um conetor do Cloud Manager, você não pode adicioná-lo de volta ao Cloud Manager.

Passos

1. Clique no menu suspenso conetor no cabeçalho do Cloud Manager.
2. Clique no menu de ação para um conetor inativo e clique em **Remove Connector**.



3. Introduza o nome do conetor para confirmar e, em seguida, clique em Remover.

Resultado

O Cloud Manager remove o conetor de seus Registros.

Desinstalar o software do conetor

O conetor inclui um script de desinstalação que você pode usar para desinstalar o software para solucionar problemas ou remover permanentemente o software do host.

Passo

1. A partir do host Linux, execute o script de desinstalação:

   /opt/application/NetApp/cloudmanager/bin/uninstall.sh [silent]

   silent executa o script sem solicitar confirmação.

E quanto às atualizações de software?

O conetor atualiza automaticamente o software para a versão mais recente, desde que seja "acesso de saída à internet" necessário obter a atualização de software.

Mais formas de criar conetores

Requisitos do host do conetor

O software do conetor deve ser executado em um host que atenda a requisitos específicos do sistema operacional, requisitos de RAM, requisitos de porta, etc.

Um host dedicado é necessário

O conetor não é suportado em um host que é compartilhado com outros aplicativos. O host deve ser um host dedicado.

CPU

4 núcleos ou 4 vCPUs

RAM

14 GB

Tipo de instância do AWS EC2

Um tipo de instância que atende aos requisitos de CPU e RAM acima. Recomendamos o T3.xlarge e use esse tipo de instância quando você implantar o conetor diretamente do Cloud Manager.

Tamanho da VM do Azure

Um tipo de instância que atende aos requisitos de CPU e RAM acima. Recomendamos o DS3 v2 e usar esse tamanho de VM quando você implantar o conetor diretamente do Cloud Manager.

Tipo de máquina GCP

Um tipo de instância que atende aos requisitos de CPU e RAM acima. Recomendamos o padrão n1-4 e usar esse tipo de máquina quando você implantar o conetor diretamente do Cloud Manager.

Sistemas operacionais suportados

- CentOS 7,6
- CentOS 7,7
- Red Hat Enterprise Linux 7,6
- Red Hat Enterprise Linux 7,7

  O sistema Red Hat Enterprise Linux deve ser registrado no Red Hat Subscription Management. Se não estiver registado, o sistema não poderá aceder aos repositórios para atualizar o software de 3rd partes necessário durante a instalação do conetor.

  O conetor é suportado em versões em inglês destes sistemas operativos.

Hipervisor

Um hypervisor bare metal ou hospedado certificado para executar o CentOS ou o Red Hat Enterprise Linux "Solução Red Hat: Quais hipervisores são certificados para executar o Red Hat Enterprise Linux?"

Espaço em disco em /opt

100 GB de espaço devem estar disponíveis

Acesso de saída à Internet

O acesso de saída à Internet é necessário para instalar o conetor e para que o conetor gerencie recursos e processos em seu ambiente de nuvem pública. Para obter uma lista de endpoints, "Requisitos de rede para o conetor"consulte .

Criando um conetor no AWS Marketplace

É melhor criar um conetor diretamente do Cloud Manager, mas você pode iniciar um conetor no AWS Marketplace, se preferir não especificar chaves de acesso da AWS. Depois de criar e configurar o conetor, o Cloud Manager o usará automaticamente quando você criar novos ambientes de trabalho.

Passos

1. Crie uma política e função do IAM para a instância do EC2:
   a. Faça o download da política do IAM do Cloud Manager a partir do seguinte local:

"Gerenciador de nuvem do NetApp: Políticas da AWS, Azure e GCP"

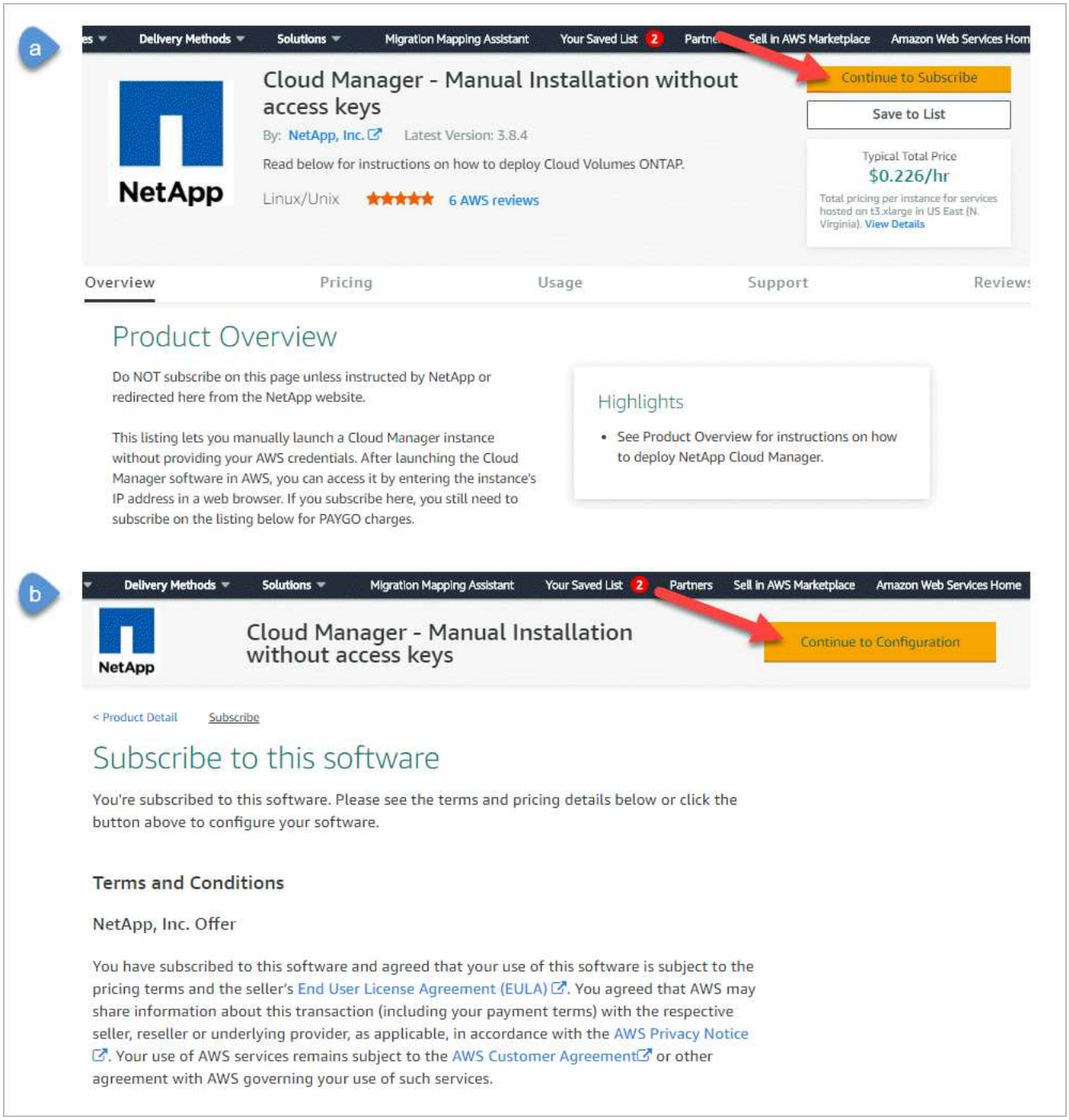
b. No console do IAM, crie sua própria política copiando e colando o texto da política do IAM do Cloud Manager.

c. Crie uma função do IAM com o tipo de função Amazon EC2 e anexe a política criada na etapa anterior à função.

2. Agora vá para o "Página do Cloud Manager no AWS Marketplace" para implantar o Cloud Manager a partir de uma AMI.

   O usuário do IAM deve ter permissões do AWS Marketplace para se inscrever e cancelar a assinatura.

3. Na página Marketplace, clique em **Continue to Subscribe** e clique em **Continue to Configuration**.



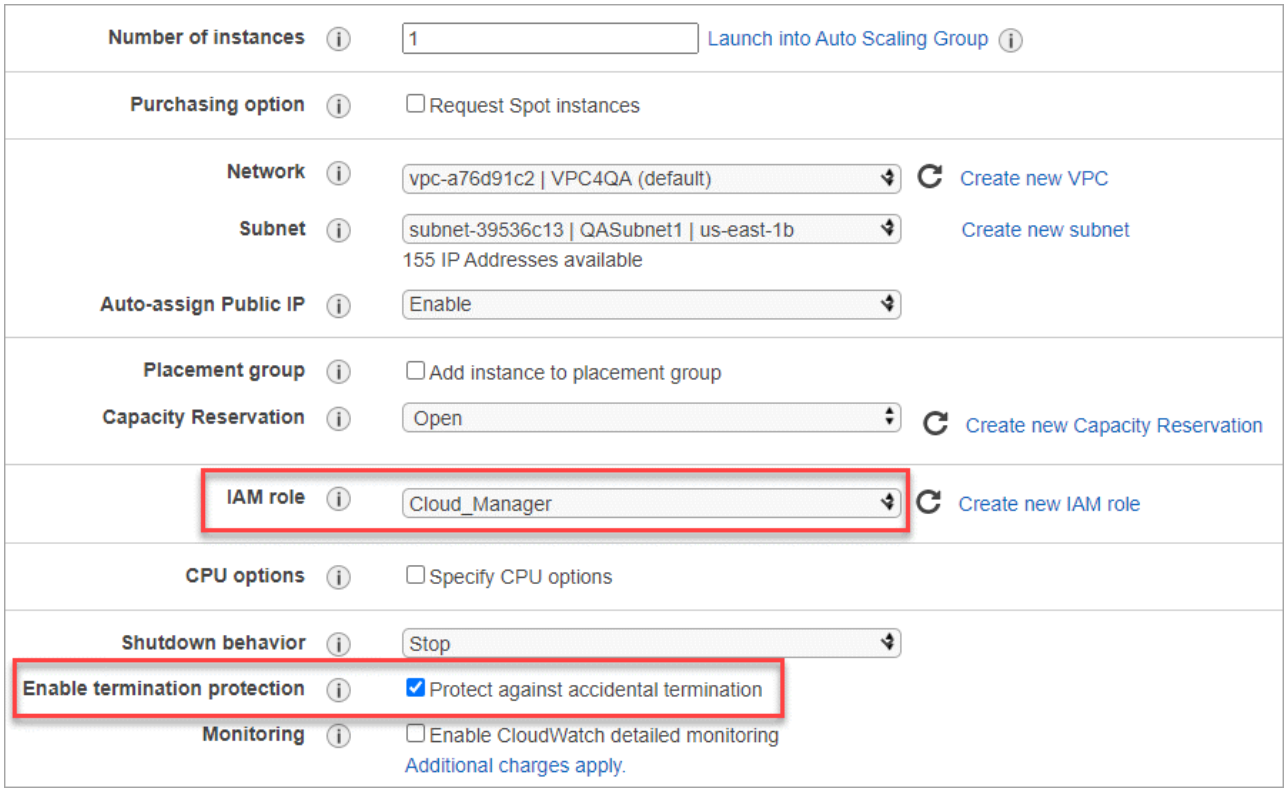
4. Altere qualquer uma das opções padrão e clique em **Continue to Launch**.
5. Em **escolha Ação**, selecione **Iniciar através de EC2** e, em seguida, clique em **Iniciar**.

   Estas etapas descrevem como iniciar a instância a partir do Console EC2 porque o console permite que você anexe uma função do IAM à instância do Cloud Manager. Isso não é possível usando a ação **Launch from Website**.

6. Siga as instruções para configurar e implantar a instância:
   - **Escolha tipo de instância**: Dependendo da disponibilidade da região, escolha um dos tipos de instância compatíveis (recomenda-se T3.xlarge).

     "Revise os requisitos da instância".

   - **Configurar instância**: Selecione uma VPC e uma sub-rede, escolha a função do IAM que você criou na etapa 1, ative a proteção de terminação (recomendada) e escolha qualquer outra opção de configuração que atenda aos seus requisitos.



   - **Adicionar armazenamento**: Mantenha as opções de armazenamento padrão.
   - **Add Tags**: Insira tags para a instância, se desejado.
   - **Configurar grupo de segurança**: Especifique os métodos de conexão necessários para a instância do conetor: SSH, HTTP e HTTPS.
   - **Revisão**: Revise suas seleções e clique em **Lançamento**.

     A AWS inicia o software com as configurações especificadas. A instância do conetor e o software devem estar sendo executados em aproximadamente cinco minutos.

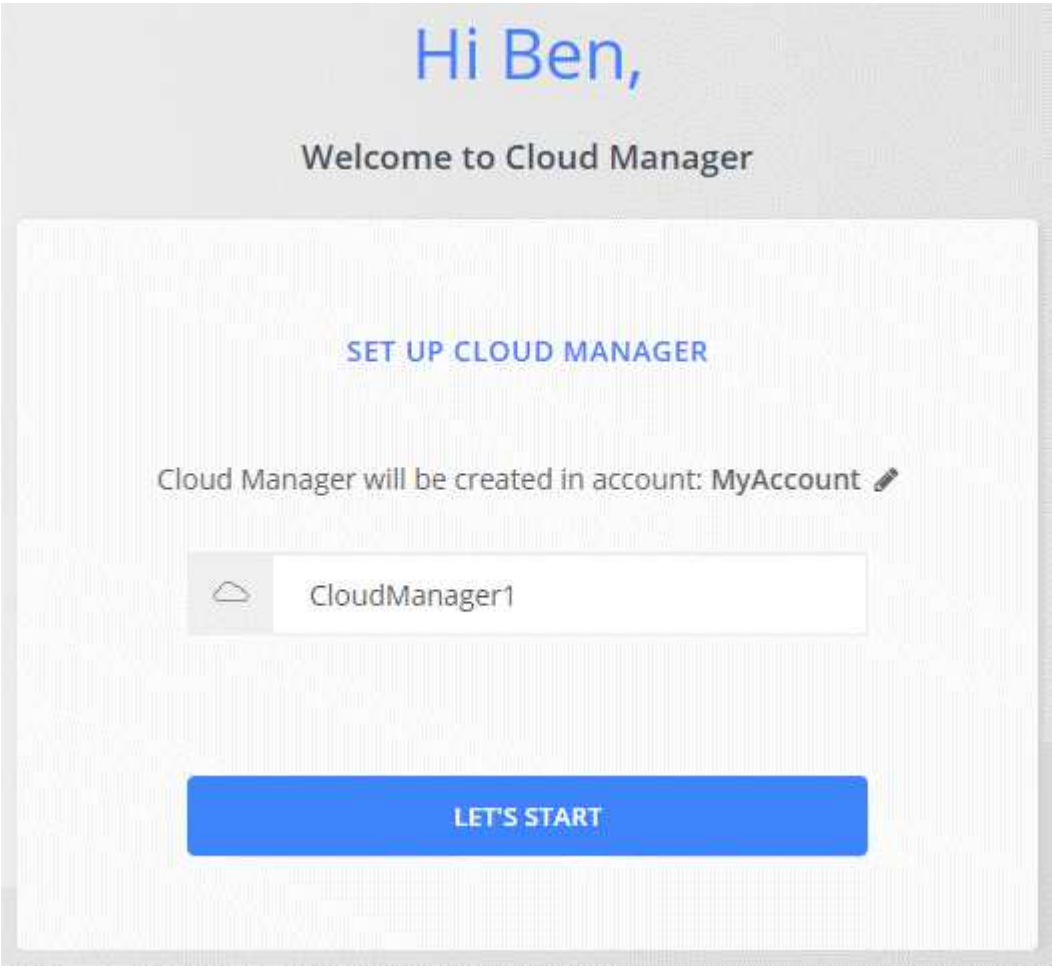
7. Abra um navegador da Web a partir de um host que tenha uma conexão com a instância do conetor e insira o seguinte URL:

http://ipaddress:80

8. Depois de iniciar sessão, configure o conetor:
   a. Especifique a conta do Cloud Central a ser associada ao conetor.

      "Saiba mais sobre as contas do Cloud Central".

   b. Introduza um nome para o sistema.



Resultado

O conetor agora está instalado e configurado com sua conta do Cloud Central. O Cloud Manager usará automaticamente esse conetor quando você criar novos ambientes de trabalho. Mas se você tiver mais de um conetor, você precisará "alterne entre eles".

Criando um conetor a partir do Azure Marketplace

É melhor criar um conetor diretamente do Cloud Manager, mas você pode iniciar um conetor do Azure Marketplace, se preferir. Depois de criar e configurar o conetor, o Cloud Manager o usará automaticamente quando você criar novos ambientes de trabalho.

Criando um conetor no Azure

Implante o conetor no Azure usando a imagem no Azure Marketplace e faça login no conetor para especificar sua conta do Cloud Central.

Passos

1. "Vá para a página do Azure Marketplace para o Cloud Manager".
2. Clique em **Obtenha-o agora** e, em seguida, clique em **continuar**.
3. No portal do Azure, clique em **criar** e siga as etapas para configurar a máquina virtual.

   Observe o seguinte ao configurar a VM:

   - O Cloud Manager pode ter um desempenho ideal com discos HDD ou SSD.
   - Escolha um tamanho de VM que atenda aos requisitos de CPU e RAM. Recomendamos DS3 v2.

     "Revise os requisitos da VM".

   - Para o grupo de segurança de rede, o conetor requer conexões de entrada usando SSH, HTTP e HTTPS.

     "Saiba mais sobre as regras do grupo de segurança para o conetor".

   - Em **Gerenciamento**, ative **identidade gerenciada atribuída ao sistema** para o conetor selecionando **On**.

     Essa configuração é importante porque uma identidade gerenciada permite que a máquina virtual Connector se identifique no Azure ative Directory sem fornecer credenciais. "Saiba mais sobre identidades gerenciadas para recursos do Azure".

4. Na página **Revisão e criação**, revise suas seleções e clique em **criar** para iniciar a implantação.

   O Azure implanta a máquina virtual com as configurações especificadas. A máquina virtual e o software do conetor devem estar funcionando em aproximadamente cinco minutos.

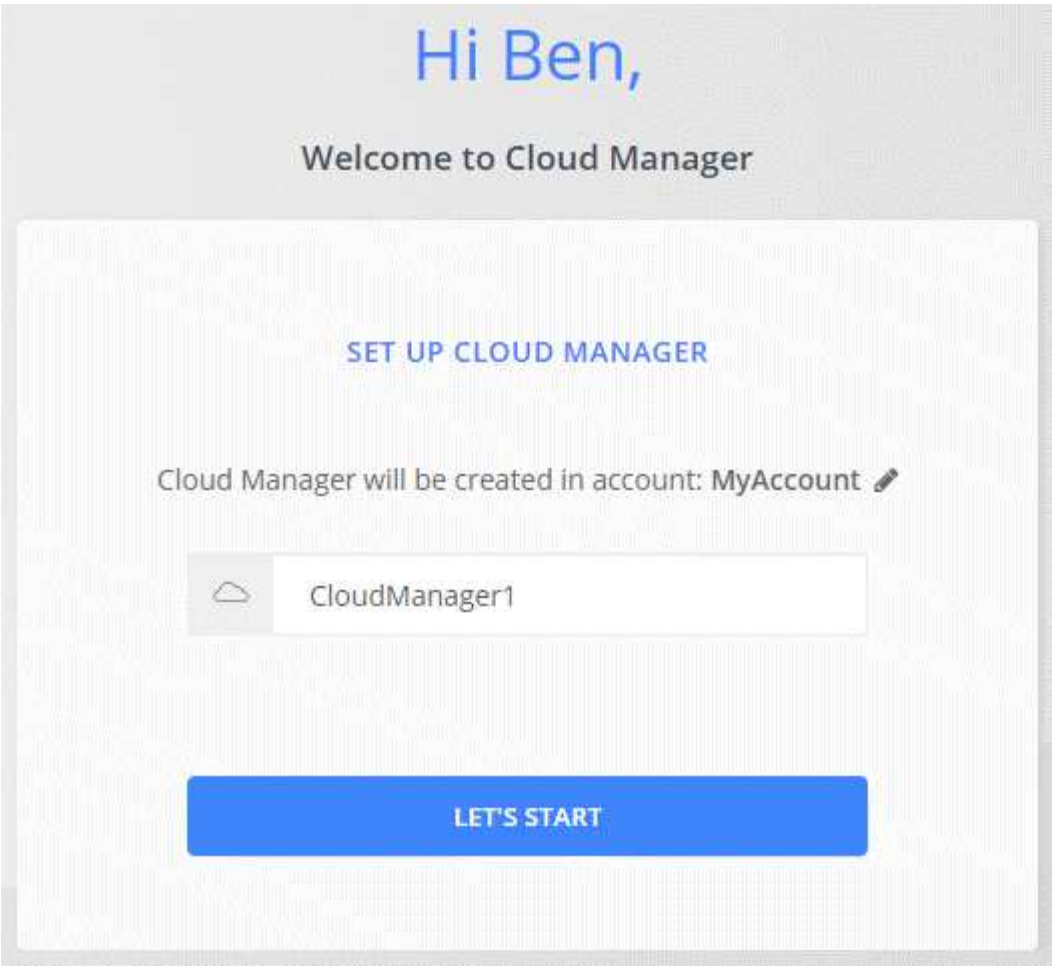
5. Abra um navegador da Web a partir de um host que tenha uma conexão com a máquina virtual do conetor e insira o seguinte URL:

   http://ipaddress:80

6. Depois de iniciar sessão, configure o conetor:
   a. Especifique a conta do Cloud Central a ser associada ao conetor.

      "Saiba mais sobre as contas do Cloud Central".

   b. Introduza um nome para o sistema.



Resultado

O conetor está agora instalado e configurado. Você deve conceder permissões do Azure antes que os usuários possam implantar o Cloud Volumes ONTAP no Azure.

Concessão de permissões do Azure

Quando você implantou o conetor no Azure, você deve ter habilitado um "identidade gerenciada atribuída ao sistema". agora você deve conceder as permissões necessárias do Azure criando uma função personalizada e atribuindo a função à máquina virtual do conetor para uma ou mais assinaturas.

Passos

1. Crie uma função personalizada usando a política do Cloud Manager:

   a. Faça download do "Política do Azure do Cloud Manager".

   b. Modifique o arquivo JSON adicionando IDs de assinatura do Azure ao escopo atribuível.

      Você deve adicionar o ID para cada assinatura do Azure a partir da qual os usuários criarão sistemas Cloud Volumes ONTAP.

      Exemplo

      "AssignableScopes": ["/Subscrições/d333af45-0d07-4154-943d-c25fbzzzzzzz", "/Subscrições/54b91999-b3e6-4599-908e-416e0zzzzzzz", "/Subscrições/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"

c. Use o arquivo JSON para criar uma função personalizada no Azure.

   O exemplo a seguir mostra como criar uma função personalizada usando a CLI do Azure 2,0:

   ```
   az role definition create --role-definition
   C:\Policy_for_cloud_Manager_Azure_3.8.7.json
   ```

Agora você deve ter uma função personalizada chamada Operador do Cloud Manager que você pode atribuir à máquina virtual do conetor.

2. Atribua a função à máquina virtual Connector para uma ou mais subscrições:
   a. Abra o serviço **assinaturas** e selecione a assinatura na qual deseja implantar sistemas Cloud Volumes ONTAP.
   b. Clique em **Access Control (IAM)**.
   c. Clique em **Adicionar** > **Adicionar atribuição de função** e, em seguida, adicione as permissões:
      - Selecione a função **Operador do Cloud Manager**.

        Operador do Cloud Manager é o nome padrão fornecido no "Política do Cloud Manager". Se você escolher um nome diferente para a função, selecione esse nome em vez disso.

      - Atribua acesso a uma **Máquina Virtual**.
      - Selecione a assinatura na qual a máquina virtual do conetor foi criada.
      - Selecione a máquina virtual do conetor.
      - Clique em **Salvar**.
   d. Se você quiser implantar o Cloud Volumes ONTAP a partir de assinaturas adicionais, mude para essa assinatura e repita essas etapas.

Resultado

O conetor agora tem as permissões necessárias para gerenciar recursos e processos em seu ambiente de nuvem pública. O Cloud Manager usará automaticamente esse conetor quando você criar novos ambientes de trabalho. Mas se você tiver mais de um conetor, você precisará "alterne entre eles".

Instalar o software Connector em um host Linux existente

A maneira mais comum de criar um conetor é diretamente do Cloud Manager ou do mercado de um provedor de nuvem. Mas você tem a opção de baixar e instalar o software Connector em um host Linux existente em sua rede ou na nuvem.

Se você quiser criar um sistema Cloud Volumes ONTAP no Google Cloud, também precisa ter um conetor em execução no Google Cloud. Não é possível usar um conetor que esteja sendo executado em outro local.

Requisitos

- O host deve atender "Requisitos para o conetor"o .
- Um sistema Red Hat Enterprise Linux deve ser registrado no Red Hat Subscription Management. Se não estiver registado, o sistema não poderá aceder aos repositórios para atualizar o software de 3rd partes necessário durante a instalação.

- O instalador do conetor acessa vários URLs durante o processo de instalação. Você deve garantir que o acesso de saída à Internet é permitido a esses endpoints:
  - http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm
  - https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
  - https://s3.amazonaws.com/aws-cli/awscli-bundle.zip

    O host pode tentar atualizar os pacotes do sistema operacional durante a instalação. O host pode entrar em Contato com diferentes sites de espelhamento para esses pacotes do sistema operacional.

Sobre esta tarefa

- Não são necessários Privileges raiz para instalar o conetor.
- A instalação instala as ferramentas de linha de comando da AWS (awscli) para habilitar procedimentos de recuperação do suporte ao NetApp.

  Se você receber uma mensagem informando que a instalação do awscli falhou, você pode ignorar a mensagem com segurança. O conetor pode funcionar com sucesso sem as ferramentas.

- O instalador disponível no site de suporte da NetApp pode ser uma versão anterior. Após a instalação, o conetor se atualiza automaticamente se uma nova versão estiver disponível.

Passos

1. Faça o download do software Cloud Manager no "Site de suporte da NetApp"e copie-o para o host Linux.

   Para obter ajuda para conetar e copiar o arquivo para uma instância do EC2 na AWS, "Documentação da AWS: Conexão com sua instância Linux usando SSH" consulte .

2. Atribua permissões para executar o script.

   Exemplo

   ```
    chmod +x OnCommandCloudManager-V3.8.4.sh
   . Execute o script de instalação:
   ```

   ```
   ./OnCommandCloudManager-V3.8.4.sh [silent] [proxy=ipaddress]
   [proxyport=port] [proxyuser=user_name] [proxypwd=password]
   ```

   silent executa a instalação sem solicitar informações.

   proxy é necessário se o host estiver atrás de um servidor proxy.

   proxyport é a porta para o servidor proxy.

   proxyuser é o nome de usuário do servidor proxy, se a autenticação básica for necessária.

   proxypwd é a senha para o nome de usuário que você especificou.

3. A menos que você especificou o parâmetro silencioso, digite **Y** para continuar o script e insira as portas HTTP e HTTPS quando solicitado.

O Cloud Manager agora está instalado. No final da instalação, o serviço do Cloud Manager (occm) será reiniciado duas vezes se você tiver especificado um servidor proxy.

4. Abra um navegador da Web e insira o seguinte URL:

   https://ipaddress:port

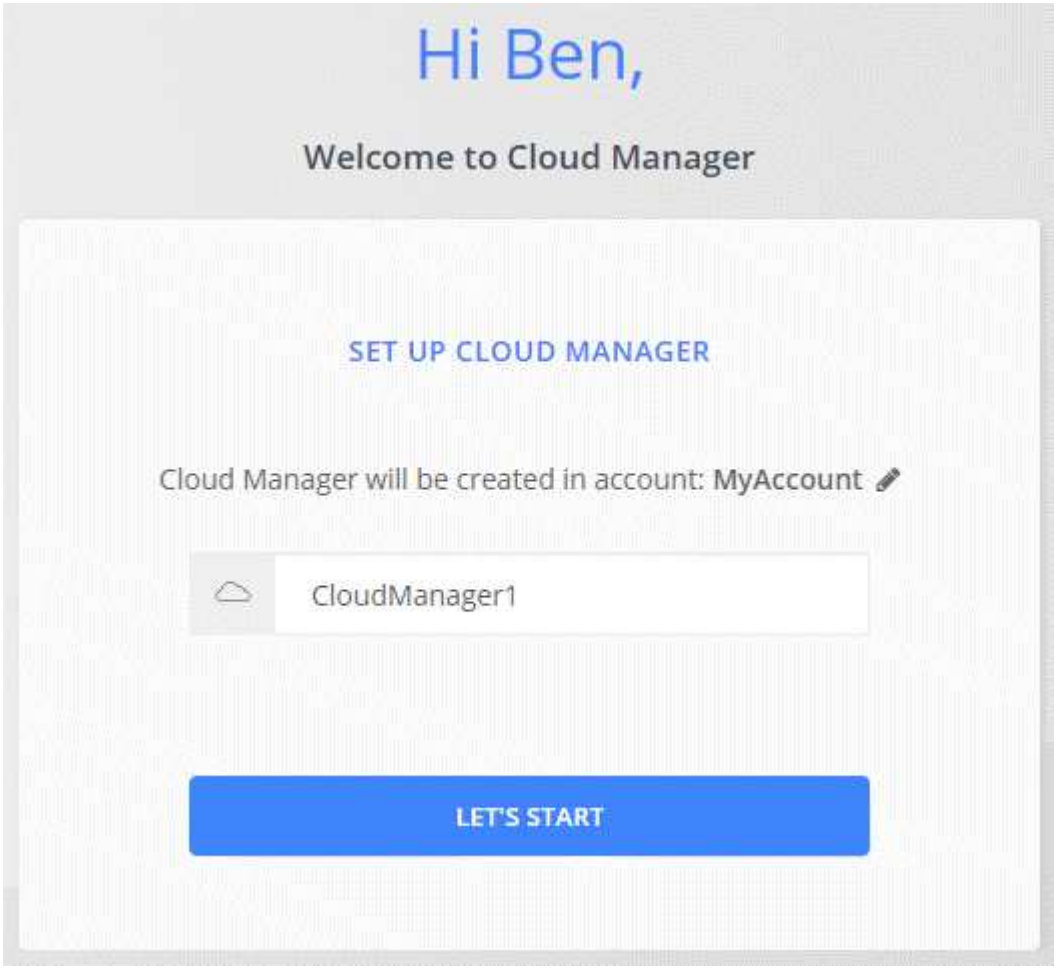
   Ipaddress pode ser localhost, um endereço IP privado ou um endereço IP público, dependendo da configuração do host. Por exemplo, se o conetor estiver na nuvem pública sem um endereço IP público, você deverá inserir um endereço IP privado de um host que tenha uma conexão com o host do conetor.

   Port é necessário se você alterou as portas HTTP (80) ou HTTPS (443) padrão. Por exemplo, se a porta HTTPS foi alterada para 8443, você digitaria https://ipaddress:8443

5. Inscreva-se no NetApp Cloud Central ou faça login.
6. Depois de fazer login, configure o Cloud Manager:
   a. Especifique a conta do Cloud Central a ser associada ao conetor.

      "Saiba mais sobre as contas do Cloud Central".

   b. Introduza um nome para o sistema.



Resultado

O conetor agora está instalado e configurado com sua conta do Cloud Central. O Cloud Manager usará automaticamente esse conetor quando você criar novos ambientes de trabalho.

Depois de terminar

Configure permissões para que o Cloud Manager possa gerenciar recursos e processos em seu ambiente de nuvem pública:

- AWS: "Configure uma conta da AWS e adicione-a ao Cloud Manager".
- Azure: "Configure uma conta do Azure e, em seguida, adicione-a ao Cloud Manager".
- GCP: Configure uma conta de serviço que tenha as permissões necessárias para criar e gerenciar sistemas Cloud Volumes ONTAP em projetos.
  a. "Crie uma função no GCP" isso inclui as permissões definidas no "Política do Cloud Manager para GCP".
  b. "Crie uma conta de serviço do GCP e aplique a função personalizada que você acabou de criar".
  c. "Associe esta conta de serviço à VM Connector".
  d. Se você quiser implantar o Cloud Volumes ONTAP em outros projetos "Conceda acesso adicionando a conta de serviço com a função Cloud Manager a esse projeto", . Você precisará repetir esta etapa para cada projeto.

Configuração padrão para o conetor

Se você precisar solucionar problemas do conetor, ele pode ajudar a entender como ele está configurado.

- Se você implantou o conetor do Cloud Manager (ou diretamente do mercado de um provedor de nuvem), observe o seguinte:
  - Na AWS, o nome de usuário da instância do EC2 Linux é EC2-user.
  - O sistema operativo da imagem é o seguinte:
    - AWS: Red Hat Enterprise Linux 7,5 (HVM)
    - Azure: Red Hat Enterprise Linux 7,6 (HVM)
    - GCP: CentOS 7,6

      O sistema operacional não inclui uma GUI. Tem de utilizar um terminal para aceder ao sistema.
- A pasta de instalação do conetor reside no seguinte local:

  /opt/application/NetApp/cloudmanager
- Os arquivos de log estão contidos na seguinte pasta:

  /opt/application/NetApp/cloudmanager/log
- O serviço Cloud Manager é chamado occm.
- O serviço occm depende do serviço MySQL.

  Se o serviço MySQL estiver inativo, o serviço occm também estará inativo.
- O Cloud Manager instala os seguintes pacotes no host Linux, se eles ainda não estiverem instalados:

- 7Zip
- AWSCLI
- Docker
- Java
- Kubectl
- MySQL
- Tridentctl
- Puxa
- Wget

- O conetor usa as seguintes portas no host Linux:
  - 80 para acesso HTTP
  - 443 para acesso HTTPS
  - 3306 para o banco de dados do Cloud Manager
  - 8080 para o proxy da API do Cloud Manager
  - 8666 para a API Service Manager
  - 8777 para a Health-Checker Container Service API

Gerenciar credenciais

AWS

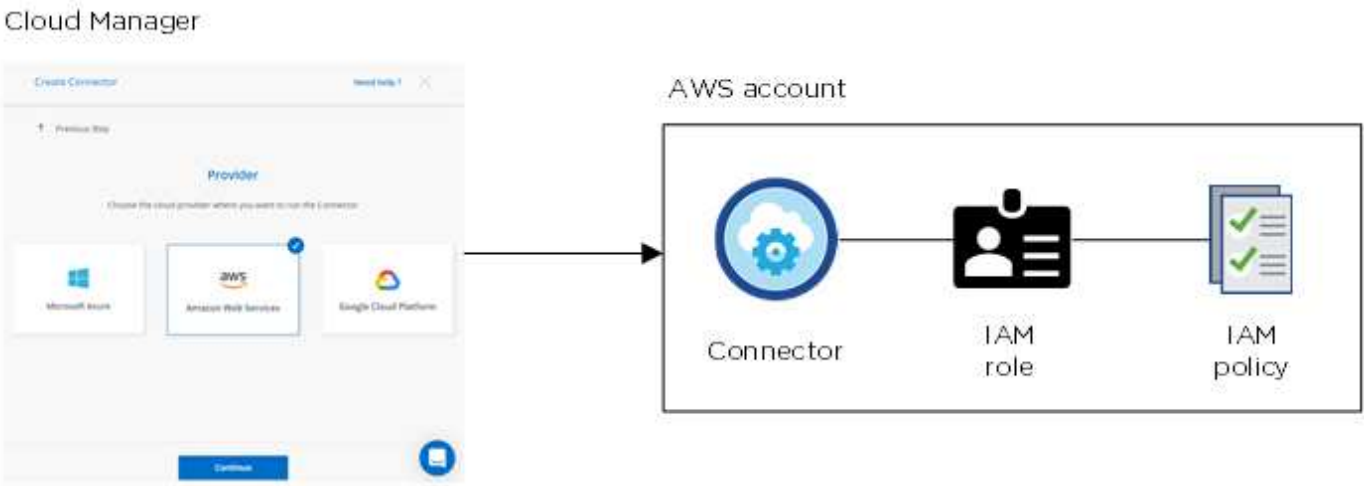
Credenciais e permissões da AWS

O Cloud Manager permite que você escolha as credenciais da AWS a serem usadas ao implantar o Cloud Volumes ONTAP. Você pode implantar todos os seus sistemas Cloud Volumes ONTAP usando as credenciais iniciais da AWS ou adicionar credenciais adicionais.

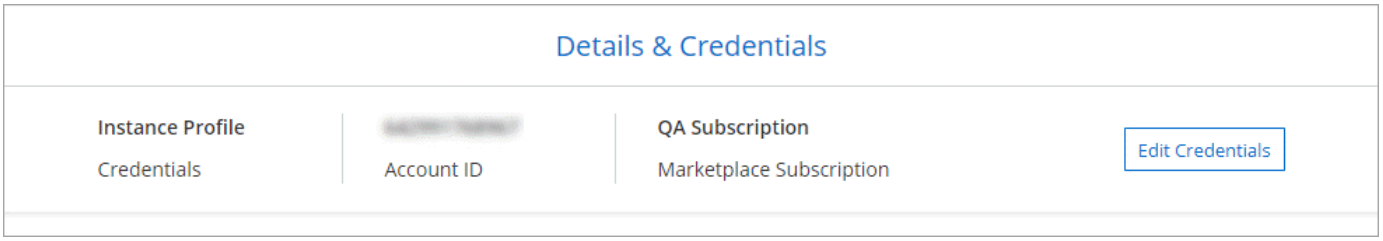
Credenciais iniciais da AWS

Ao implantar um conetor do Cloud Manager, você precisa usar uma conta da AWS que tenha permissões para iniciar a instância do Connector. As permissões necessárias estão listadas no "Política de implantação do Connector para AWS".

Quando o Cloud Manager inicia a instância do Connector na AWS, ele cria uma função do IAM e um perfil de instância para a instância. Ele também anexa uma política que fornece ao Cloud Manager permissões para gerenciar recursos e processos dentro dessa conta da AWS. "Veja como o Cloud Manager usa as permissões".

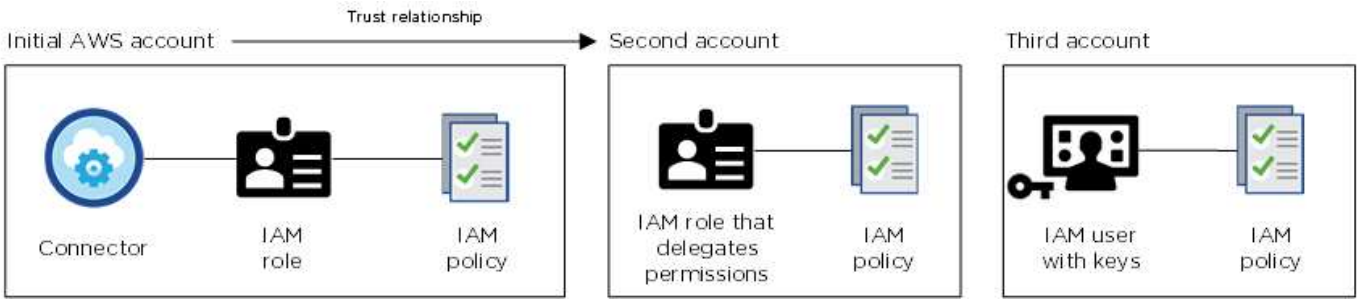


O Cloud Manager seleciona essas credenciais da AWS por padrão quando você cria um novo ambiente de trabalho para o Cloud Volumes ONTAP:



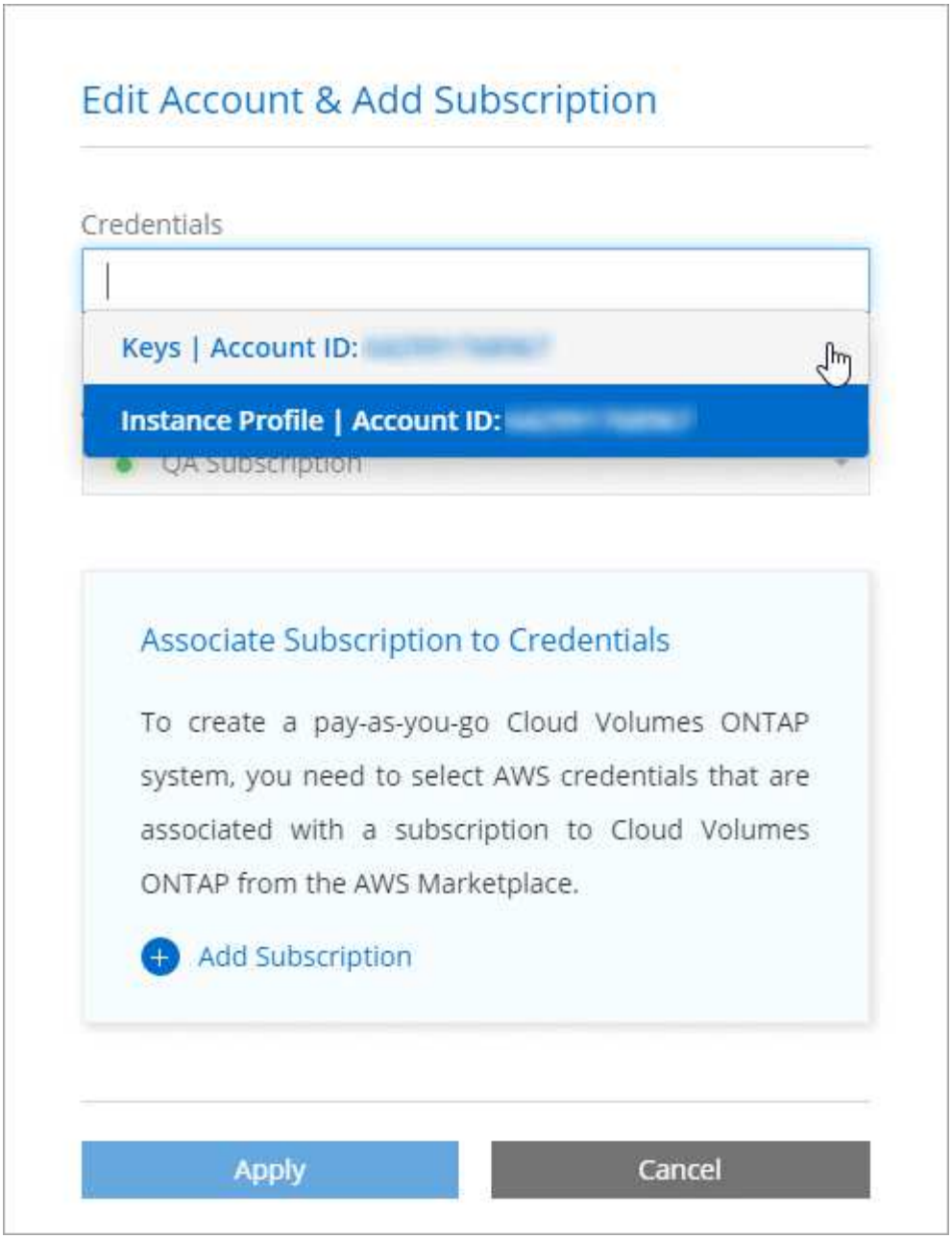
Credenciais adicionais da AWS

Se você quiser iniciar o Cloud Volumes ONTAP em diferentes contas da AWS, poderá usar "Forneça chaves da AWS para um usuário do IAM ou o ARN de uma função em uma conta confiável"o . A imagem a seguir mostra duas contas adicionais, uma fornecendo permissões por meio de uma função do IAM em uma conta confiável e outra por meio das chaves da AWS de um usuário do IAM:



Você deve "Adicione as credenciais da conta ao Cloud Manager"especificar o nome do recurso Amazon (ARN) da função do IAM ou as chaves da AWS para o usuário do IAM.

Depois de adicionar outro conjunto de credenciais, você pode alternar para elas ao criar um novo ambiente de trabalho:



E quanto às implantações do Marketplace e às implantações locais?

As seções acima descrevem o método de implantação recomendado para o conetor, que é do Cloud Manager. Também é possível implantar um conetor na AWS a partir do "AWS Marketplace" e "Instale o conetor no local"do .

Se você usar o Marketplace, as permissões serão fornecidas da mesma maneira. Você só precisa criar e configurar manualmente a função do IAM e, em seguida, fornecer permissões para quaisquer contas adicionais.

Para implantações locais, não é possível configurar uma função do IAM para o sistema do Cloud Manager, mas você pode fornecer permissões da mesma forma que faria para contas adicionais da AWS.

Como posso girar com segurança minhas credenciais da AWS?

Como descrito acima, o Cloud Manager permite que você forneça credenciais da AWS de algumas maneiras:

Uma função do IAM associada à instância do Connector, assumindo uma função do IAM em uma conta confiável ou fornecendo chaves de acesso da AWS.

Com as duas primeiras opções, o Cloud Manager usa o AWS Security Token Service para obter credenciais temporárias que rodam constantemente. Este processo é a melhor prática - é automático e seguro.

Se você fornecer ao Cloud Manager chaves de acesso da AWS, gire as chaves atualizando-as no Cloud Manager em um intervalo regular. Este é um processo completamente manual.

Gerenciamento de credenciais e assinaturas da AWS para o Cloud Manager

Ao criar um sistema Cloud Volumes ONTAP, você precisa selecionar as credenciais e a assinatura da AWS para usar com esse sistema. Se você gerenciar várias assinaturas da AWS, poderá atribuir cada uma delas a diferentes credenciais da AWS na página credenciais.

Antes de adicionar credenciais da AWS ao Cloud Manager, você precisa fornecer as permissões necessárias para essa conta. As permissões permitem que o Cloud Manager gerencie recursos e processos dentro dessa conta da AWS. A forma como você fornece as permissões depende se deseja fornecer ao Cloud Manager chaves AWS ou o ARN de uma função em uma conta confiável.

Quando você implantou um conetor do Cloud Manager, o Cloud Manager adicionou automaticamente credenciais da AWS para a conta na qual implantou o conetor. Esta conta inicial não é adicionada se você instalou manualmente o software Connector em um sistema existente. "Saiba mais sobre as credenciais e permissões da AWS".

Escolhas

- Concessão de permissões fornecendo chaves da AWS
- Concessão de permissões assumindo funções do IAM em outras contas

Como posso girar com segurança minhas credenciais da AWS?

O Cloud Manager permite que você forneça credenciais da AWS de algumas maneiras: Uma função do IAM associada à instância do Connector, assumindo uma função do IAM em uma conta confiável ou fornecendo chaves de acesso da AWS. "Saiba mais sobre as credenciais e permissões da AWS".

Com as duas primeiras opções, o Cloud Manager usa o AWS Security Token Service para obter credenciais temporárias que rodam constantemente. Este processo é a melhor prática, é automático e seguro.

Se você fornecer ao Cloud Manager chaves de acesso da AWS, gire as chaves atualizando-as no Cloud Manager em um intervalo regular. Este é um processo completamente manual.

Concessão de permissões fornecendo chaves da AWS

Se você quiser fornecer ao Cloud Manager chaves da AWS para um usuário do IAM, precisará conceder as permissões necessárias a esse usuário. A política do IAM do Cloud Manager define as ações e recursos da AWS que o Cloud Manager pode usar.

Passos

1. Faça download da política do IAM do Cloud Manager no "Página de políticas do Cloud Manager".
2. No console do IAM, crie sua própria política copiando e colando o texto da política do IAM do Cloud Manager.

   "Documentação da AWS: Criando políticas do IAM"

3. Anexe a política a uma função do IAM ou a um usuário do IAM.
   - "Documentação da AWS: Criando funções do IAM"
   - "Documentação da AWS: Adicionando e removendo políticas do IAM"

Resultado

A conta agora tem as permissões necessárias. Agora você pode adicioná-lo ao Cloud Manager.

Concessão de permissões assumindo funções do IAM em outras contas

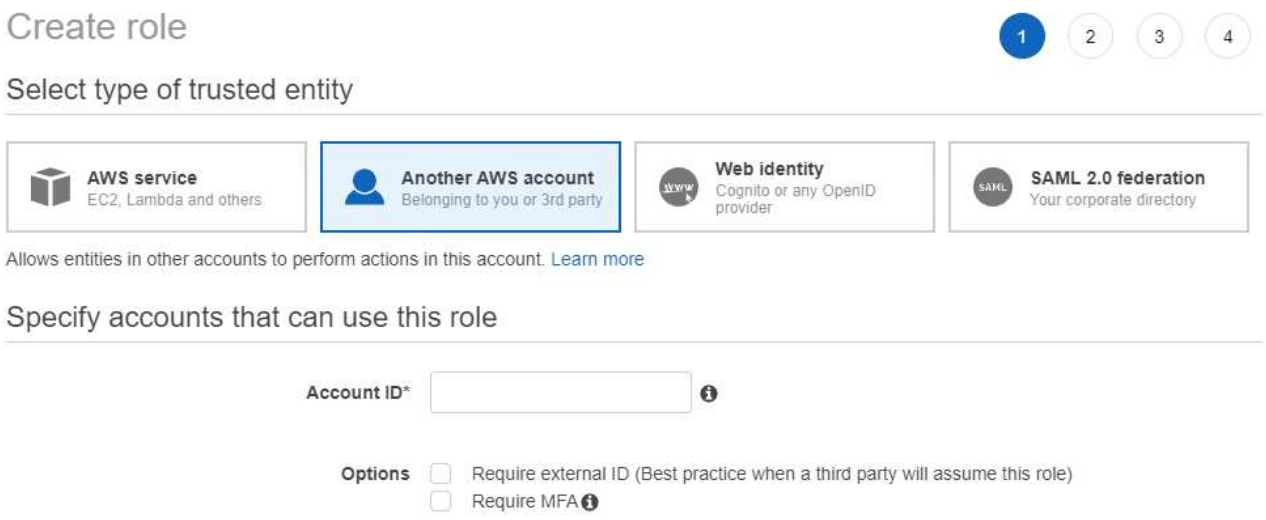
Você pode configurar uma relação de confiança entre a conta da AWS de origem na qual implantou a instância do Connector e outras contas da AWS usando funções do IAM. Em seguida, você fornecerá ao Cloud Manager o ARN das funções do IAM das contas confiáveis.

Passos

1. Vá para a conta de destino onde você deseja implantar o Cloud Volumes ONTAP e criar uma função do IAM selecionando **outra conta da AWS**.

   Certifique-se de fazer o seguinte:

   - Insira o ID da conta onde reside a instância do conetor.
   - Anexe a política do IAM do Cloud Manager, que está disponível no "Página de políticas do Cloud Manager".



2. Vá para a conta de origem onde reside a instância do conetor e selecione a função do IAM que está anexada à instância.

   a. Clique em **Anexar políticas** e, em seguida, clique em **criar política**.

   b. Crie uma política que inclua a ação "sts:AssumeRole" e o ARN da função que você criou na conta de destino.

Exemplo

```
{
 "Version": "2012-10-17",
 "Statement": {
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": "arn:aws:iam::ACCOUNT-B-ID:role/ACCOUNT-B-ROLENAME"
}
}
```

Resultado

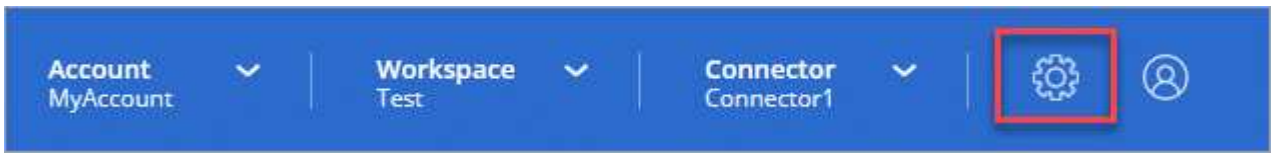
A conta agora tem as permissões necessárias. Agora você pode adicioná-lo ao Cloud Manager.

Adição de credenciais da AWS ao Cloud Manager

Depois de fornecer uma conta da AWS com as permissões necessárias, você pode adicionar as credenciais dessa conta ao Cloud Manager. Isso permite que você inicie sistemas Cloud Volumes ONTAP nessa conta.

Passos

1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **credenciais**.



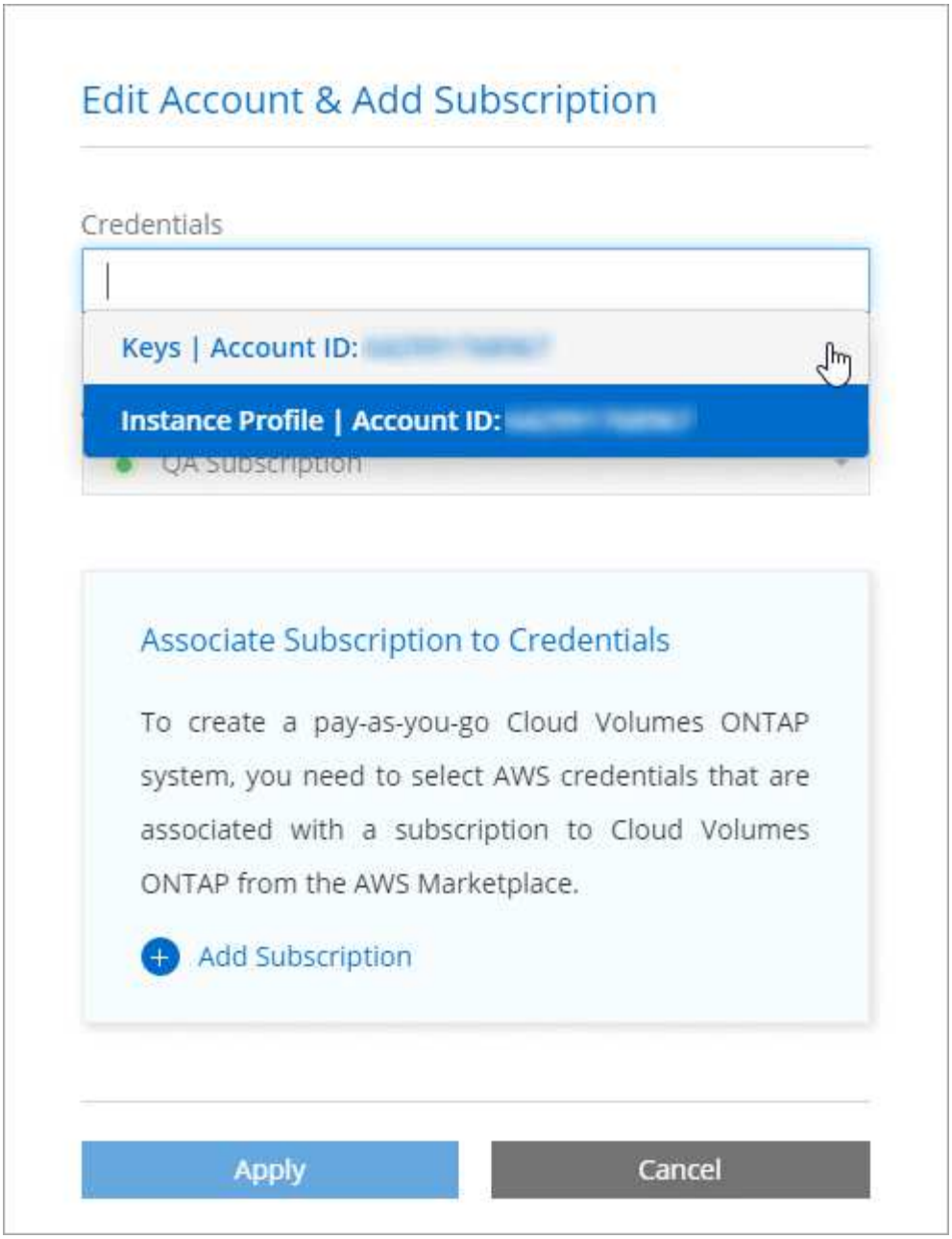
2. Clique em **Adicionar credenciais** e selecione **AWS**.
3. Forneça chaves da AWS ou o ARN de uma função IAM confiável.
4. Confirme se os requisitos da política foram atendidos e clique em **continuar**.
5. Escolha a assinatura paga conforme o uso que você deseja associar às credenciais ou clique em **Adicionar assinatura** se você ainda não tiver uma.

   Para criar um sistema Cloud Volumes ONTAP com pagamento conforme o uso, as credenciais da AWS devem estar associadas a uma assinatura do Cloud Volumes ONTAP no mercado AWS.

6. Clique em **Add**.

Resultado

Agora você pode alternar para um conjunto diferente de credenciais da página Detalhes e credenciais ao criar um novo ambiente de trabalho:



Associando uma assinatura da AWS às credenciais

Depois de adicionar suas credenciais da AWS ao Cloud Manager, você pode associar uma assinatura do AWS Marketplace a essas credenciais. A assinatura permite criar um sistema Cloud Volumes ONTAP com pagamento conforme o uso e usar outros serviços de nuvem da NetApp.

Há dois cenários em que você pode associar uma assinatura do AWS Marketplace depois de adicionar as credenciais ao Cloud Manager:

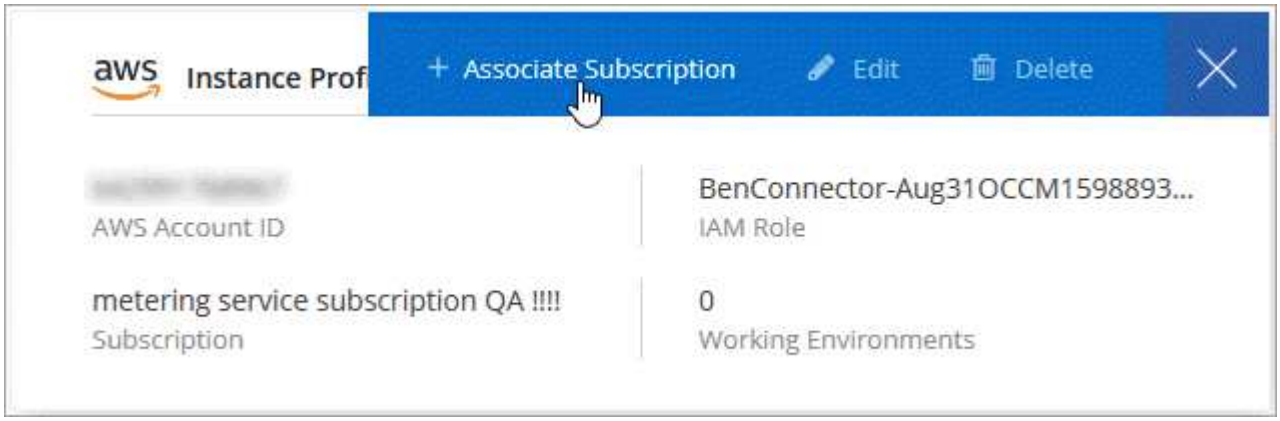
- Você não associou uma assinatura quando adicionou inicialmente as credenciais ao Cloud Manager.
- Você deseja substituir uma assinatura existente do AWS Marketplace por uma nova assinatura.

O que você vai precisar

Você precisa criar um conetor antes de alterar as configurações do Cloud Manager. "Saiba como".

Passos

1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **credenciais**.
2. Passe o Mouse sobre um conjunto de credenciais e clique no menu de ação.
3. No menu, clique em **assinatura associada**.



4. Selecione uma assinatura na lista suspensa ou clique em **Adicionar assinatura** e siga as etapas para criar uma nova assinatura.

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

Azure

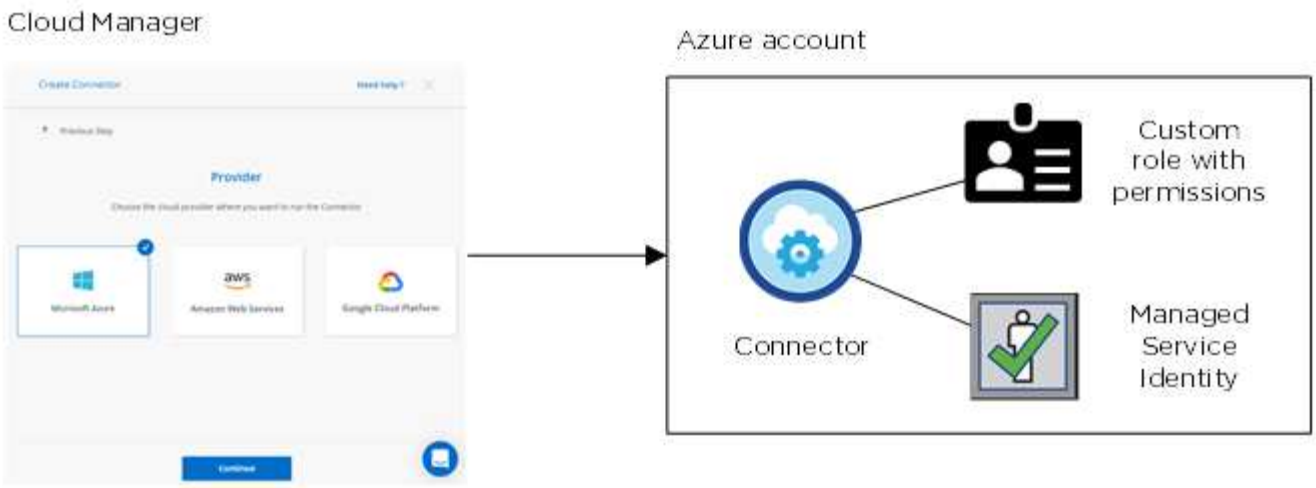
Credenciais e permissões do Azure

O Cloud Manager permite que você escolha as credenciais do Azure a serem usadas ao implantar o Cloud Volumes ONTAP. Você pode implantar todos os seus sistemas Cloud Volumes ONTAP usando as credenciais iniciais do Azure ou adicionar credenciais adicionais.

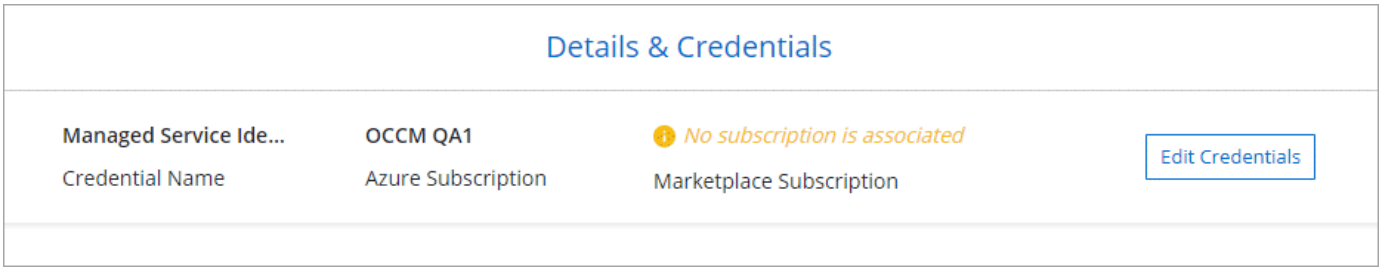
Credenciais iniciais do Azure

Ao implantar um conetor do Cloud Manager, você precisa usar uma conta do Azure que tenha permissões para implantar a máquina virtual do Connector. As permissões necessárias estão listadas no "Política de implantação do Connector para Azure".

Quando o Cloud Manager implanta a máquina virtual Connector no Azure, ele ativa uma "identidade gerenciada atribuída ao sistema" máquina virtual on, cria uma função personalizada e a atribui à máquina virtual. A função fornece ao Cloud Manager permissões para gerenciar recursos e processos dentro dessa assinatura do Azure. "Veja como o Cloud Manager usa as permissões".



O Cloud Manager seleciona essas credenciais do Azure por padrão quando você cria um novo ambiente de trabalho para o Cloud Volumes ONTAP:

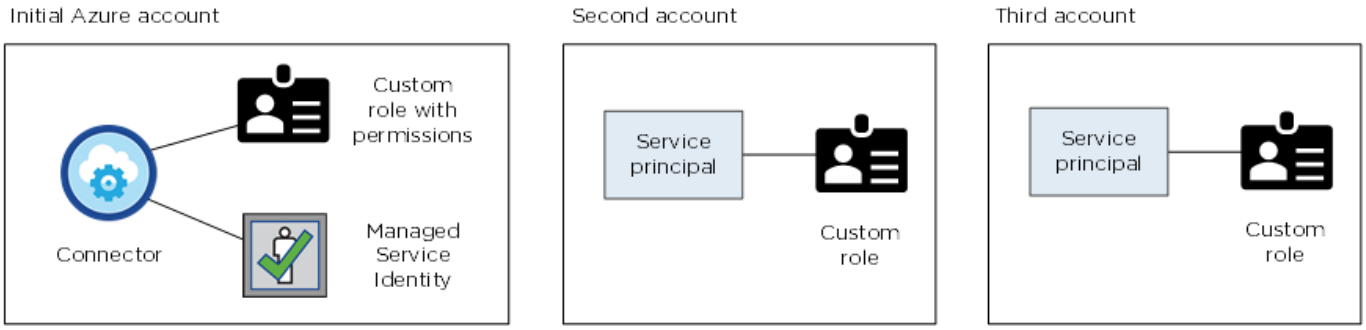


Subscrições adicionais do Azure para uma identidade gerida

A identidade gerenciada está associada à assinatura na qual você lançou o conetor. Se você quiser selecionar uma assinatura diferente do Azure, precisará "associe a identidade gerenciada a essas assinaturas"do .

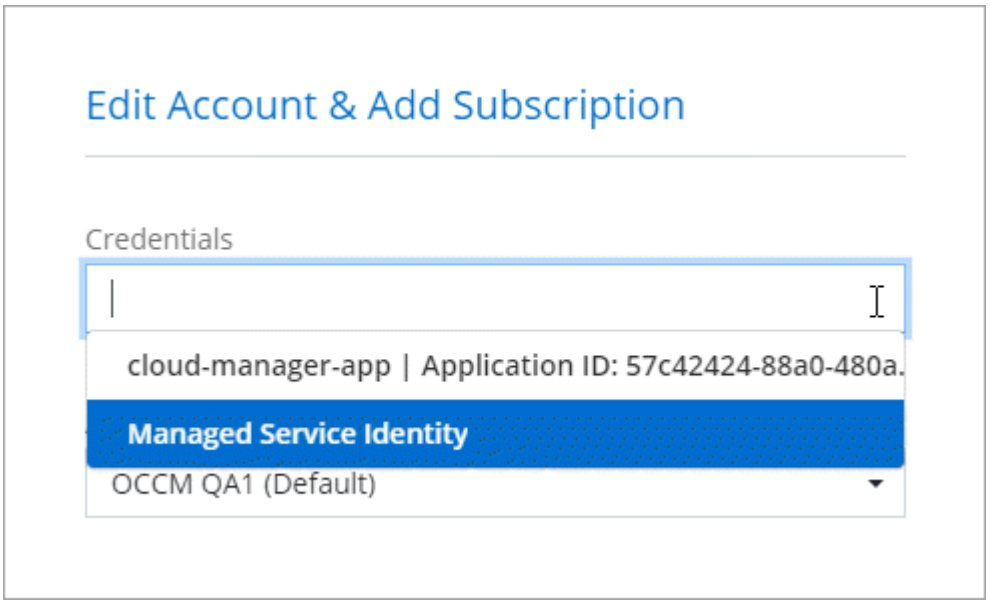
Credenciais adicionais do Azure

Se você quiser implantar o Cloud Volumes ONTAP usando diferentes credenciais do Azure, você deve conceder as permissões necessárias para "Criando e configurando um princípio de serviço no Azure ative Directory"cada conta do Azure. A imagem a seguir mostra duas contas adicionais, cada uma configurada com uma função principal de serviço e personalizada que fornece permissões:



Em seguida, você "Adicione as credenciais da conta ao Cloud Manager"forneceria detalhes sobre o diretor de serviço do AD.

Depois de adicionar outro conjunto de credenciais, você pode alternar para elas ao criar um novo ambiente de trabalho:



E quanto às implantações do Marketplace e às implantações locais?

As seções acima descrevem o método de implantação recomendado para o conetor, que é do NetApp Cloud Central. Você também pode implantar um conetor no Azure a partir do "Azure Marketplace", e pode "Instale o conetor no local".

Se você usar o Marketplace, as permissões serão fornecidas da mesma maneira. Você só precisa criar e configurar manualmente a identidade gerenciada para o conetor e, em seguida, fornecer permissões para quaisquer contas adicionais.

Para implantações locais, não é possível configurar uma identidade gerenciada para o conetor, mas você pode fornecer permissões da mesma forma que faria para contas adicionais usando um princípio de serviço.

Gerenciamento de credenciais e assinaturas do Azure para o Cloud Manager

Ao criar um sistema Cloud Volumes ONTAP, você precisa selecionar as credenciais do Azure e a assinatura do Marketplace para usar com esse sistema. Se você gerenciar várias assinaturas do Azure Marketplace, poderá atribuir cada uma delas a diferentes credenciais do Azure na página credenciais.

Há duas maneiras de gerenciar credenciais do Azure no Cloud Manager. Primeiro, se você quiser implantar o Cloud Volumes ONTAP em diferentes contas do Azure, precisará fornecer as permissões necessárias e adicionar as credenciais ao Cloud Manager. A segunda maneira é associar assinaturas adicionais à identidade gerenciada do Azure.

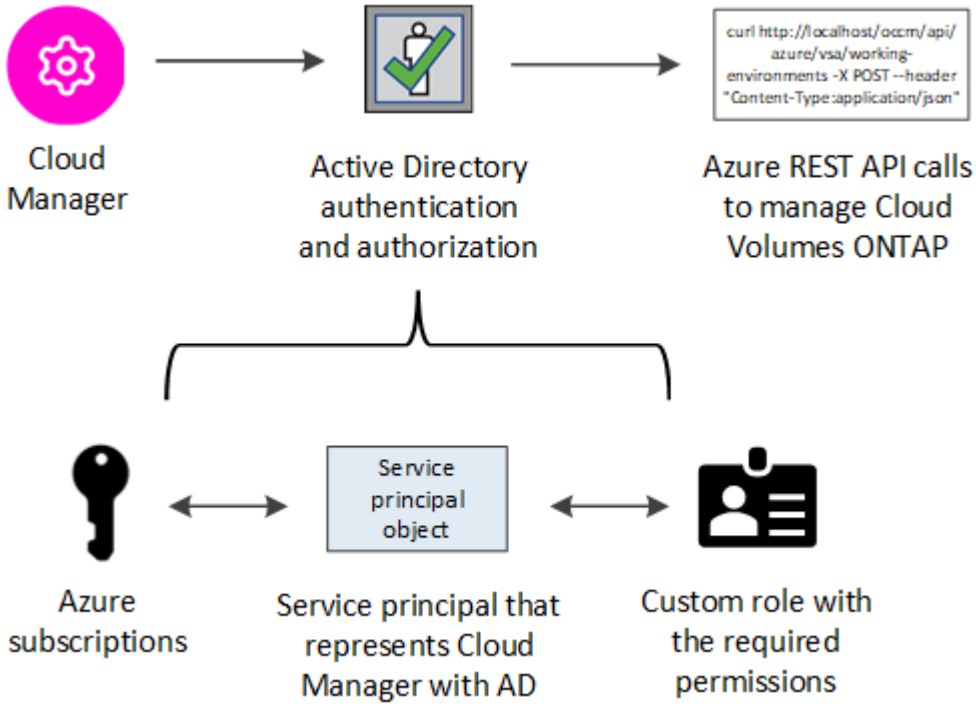
Ao implantar um conetor do Cloud Manager, o Cloud Manager adiciona automaticamente a conta do Azure na qual você implantou o conetor. Uma conta inicial não será adicionada se você tiver instalado manualmente o software Connector em um sistema existente. "Saiba mais sobre as contas e permissões do Azure".

Concessão de permissões do Azure usando um princípio de serviço

O Cloud Manager precisa de permissões para executar ações no Azure. Você pode conceder as permissões necessárias a uma conta do Azure criando e configurando um responsável de serviço no Azure ative Directory e obtendo as credenciais do Azure de que o Cloud Manager precisa.

Sobre esta tarefa

A imagem a seguir mostra como o Cloud Manager obtém permissões para executar operações no Azure. Um objeto principal de serviço, vinculado a uma ou mais assinaturas do Azure, representa o Cloud Manager no Azure ative Directory e é atribuído a uma função personalizada que permite as permissões necessárias.



Passos

1. Crie uma aplicação Azure ative Directory.
2. Atribua a aplicação a uma função.
3. Adicione permissões da API de Gerenciamento de Serviços do Windows Azure.
4. Obtenha o ID do aplicativo e o ID do diretório.
5. Crie um segredo de cliente.

Criando um aplicativo Azure ative Directory

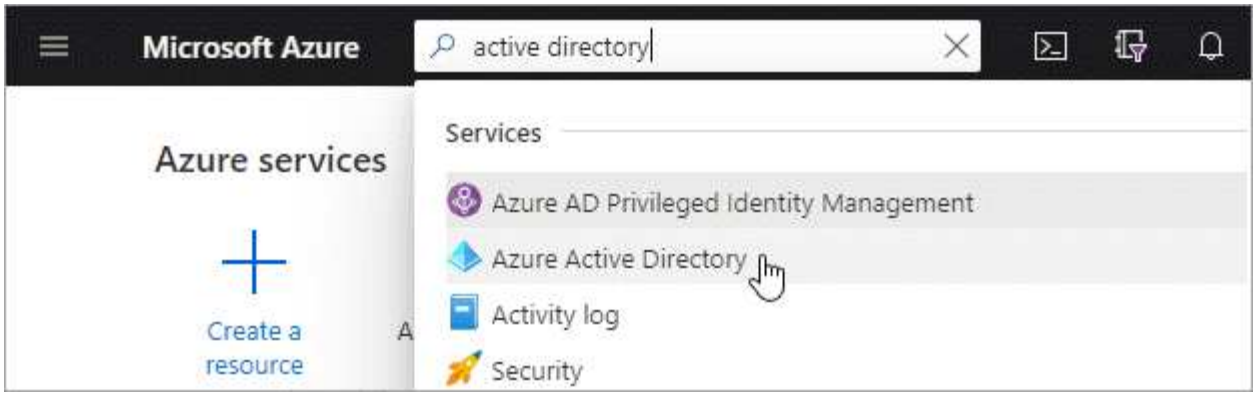
Crie um aplicativo e um diretor de serviço do Azure ative Directory (AD) que o Cloud Manager pode usar para controle de acesso baseado em funções.

Antes de começar

Você deve ter as permissões certas no Azure para criar um aplicativo do ative Directory e atribuir o aplicativo a uma função. Para obter detalhes, "Documentação do Microsoft Azure: Permissões necessárias" consulte .

Passos

1. No portal do Azure, abra o serviço **Azure ative Directory**.



2. No menu, clique em **inscrições de aplicativos**.
3. Clique em **novo registo**.
4. Especifique detalhes sobre o aplicativo:
   - **Nome**: Insira um nome para o aplicativo.
   - **Tipo de conta**: Selecione um tipo de conta (qualquer funcionará com o Cloud Manager).
   - * URI de redirecionamento*: Selecione **Web** e, em seguida, insira qualquer URL, por exemplo, https://url
5. Clique em **Register**.

Resultado

Você criou o aplicativo AD e o principal de serviço.

Atribuindo a aplicação a uma função

Você deve vincular o principal de serviço a uma ou mais assinaturas do Azure e atribuir-lhe a função personalizada "Operador do Gerenciador de nuvem do OnCommand" para que o Gerenciador de nuvem tenha permissões no Azure.

Passos

1. Crie uma função personalizada:

   a. Faça download do "Política do Azure do Cloud Manager".

   b. Modifique o arquivo JSON adicionando IDs de assinatura do Azure ao escopo atribuível.

   Você deve adicionar o ID para cada assinatura do Azure a partir da qual os usuários criarão sistemas Cloud Volumes ONTAP.

   Exemplo

   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

   c. Use o arquivo JSON para criar uma função personalizada no Azure.

O exemplo a seguir mostra como criar uma função personalizada usando a CLI do Azure 2,0:

```
az role definition create --role-definition
C:\Policy_for_cloud_Manager_Azure_3.8.7.json
```

Agora você deve ter uma função personalizada chamada *Cloud Manager Operator*.

2. Atribua o aplicativo à função:

   a. No portal do Azure, abra o serviço **Subscrições**.

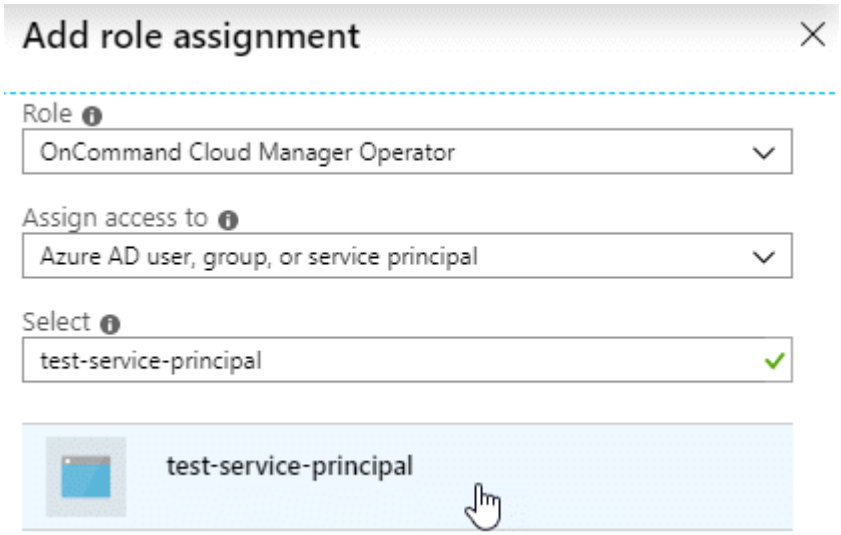
   b. Selecione a subscrição.

   c. Clique em **Access control (IAM) > Add > Add Role assignment** (Adicionar > Adicionar atribuição de função*).

   d. Selecione a função **Operador do Cloud Manager**.

   e. Mantenha **Usuário, grupo ou responsável de serviço do Azure AD** selecionado.

   f. Procure o nome do aplicativo (você não pode encontrá-lo na lista rolando).



   g. Selecione o aplicativo e clique em **Salvar**.

   O responsável de serviço do Cloud Manager agora tem as permissões necessárias do Azure para essa assinatura.

Se você quiser implantar o Cloud Volumes ONTAP a partir de várias assinaturas do Azure, então você deve vincular o principal de serviço a cada uma dessas assinaturas. O Cloud Manager permite que você selecione a assinatura que deseja usar ao implantar o Cloud Volumes ONTAP.

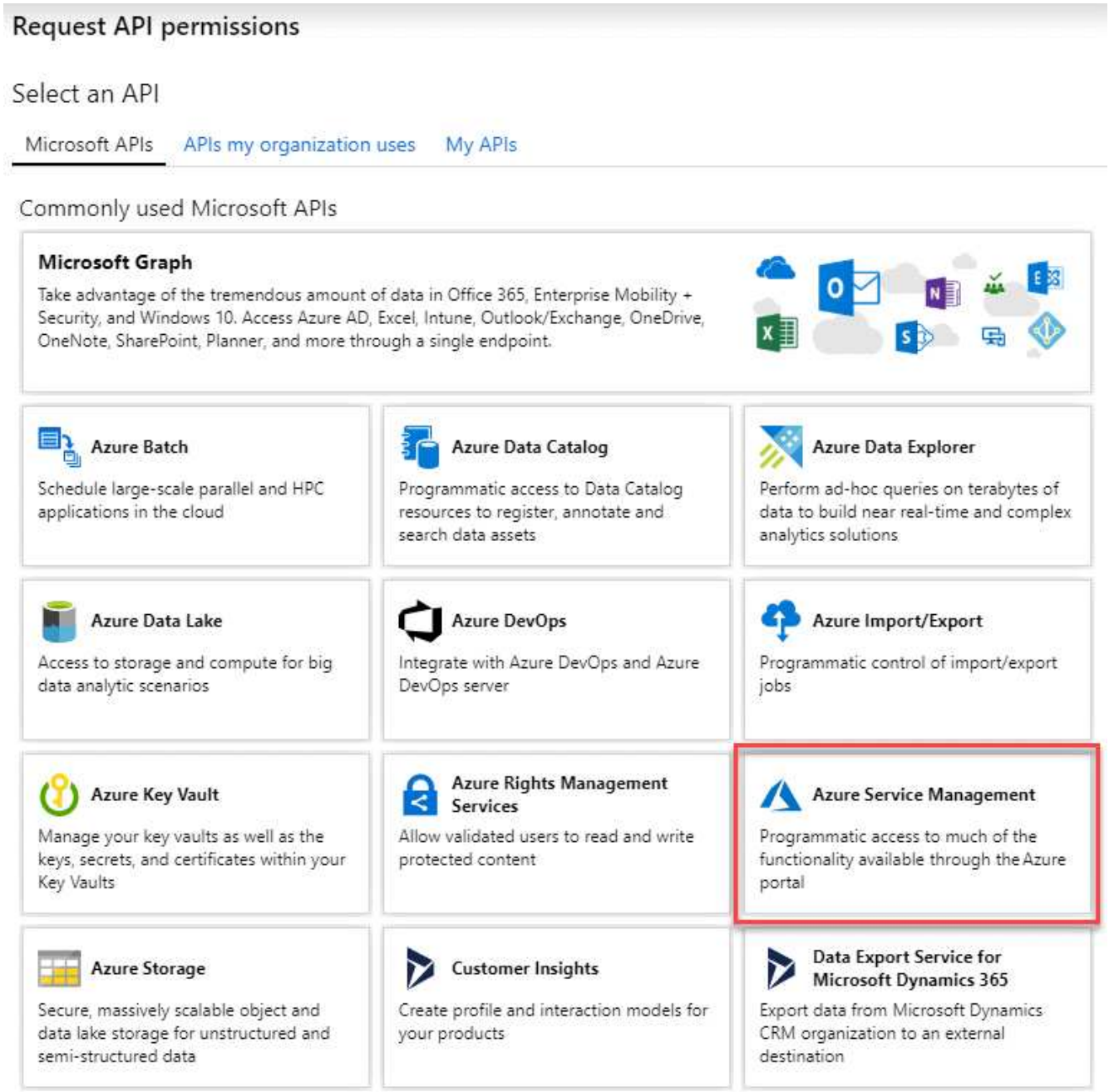
Adicionando permissões de API de Gerenciamento de Serviços do Windows Azure

O responsável do serviço deve ter permissões "Windows Azure Service Management API".

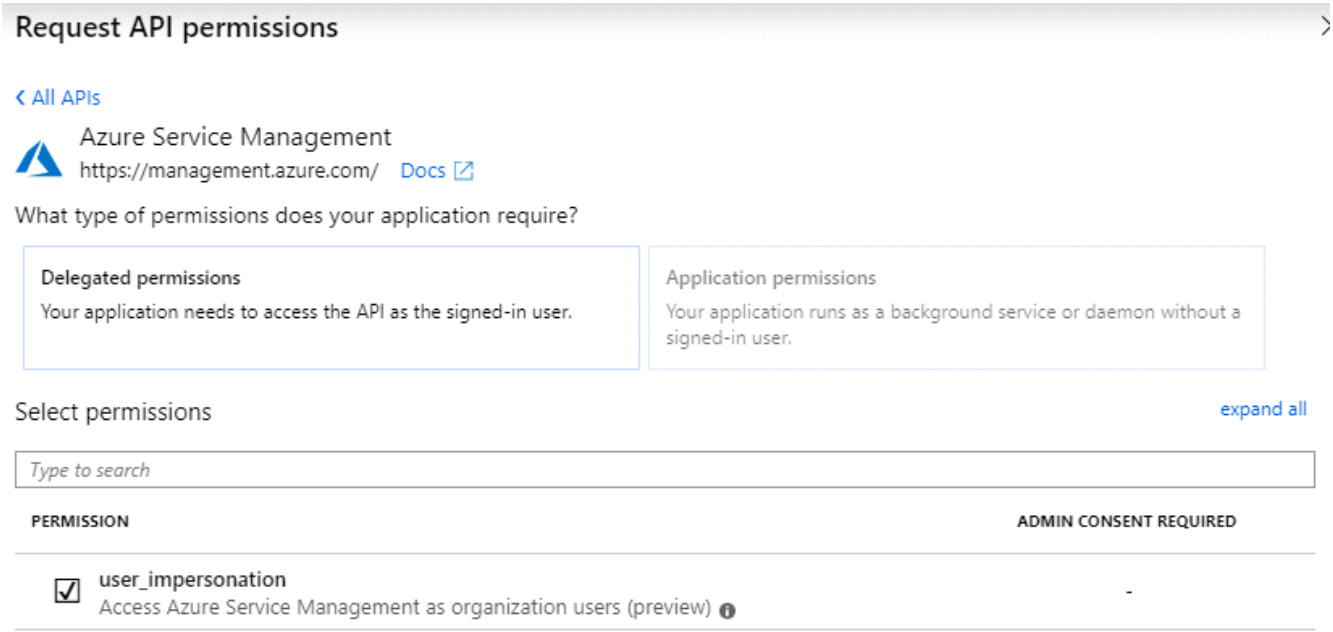
Passos

1. No serviço **Azure ative Directory**, clique em **inscrições de aplicativos** e selecione o aplicativo.
2. Clique em **permissões de API > Adicionar uma permissão**.

3. Em **Microsoft APIs**, selecione **Azure Service Management**.



4. Clique em **Acesse o Gerenciamento de Serviços do Azure como usuários da organização** e clique em **Adicionar permissões**.

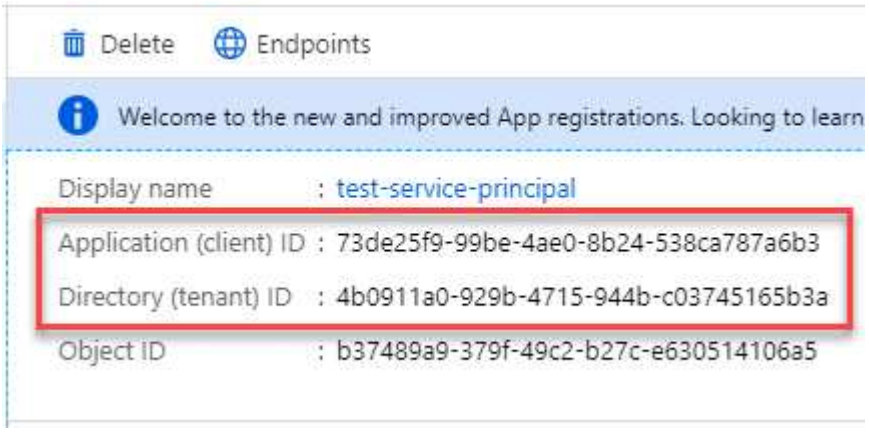


Obtendo o ID do aplicativo e o ID do diretório

Quando você adiciona a conta do Azure ao Cloud Manager, você precisa fornecer o ID do aplicativo (cliente) e o ID do diretório (locatário) para o aplicativo. O Cloud Manager usa as IDs para fazer login programaticamente.

Passos

1. No serviço **Azure ative Directory**, clique em **inscrições de aplicativos** e selecione o aplicativo.
2. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.



Criando um segredo de cliente

Você precisa criar um segredo de cliente e, em seguida, fornecer ao Cloud Manager o valor do segredo para que o Cloud Manager possa usá-lo para autenticar com o Azure AD.

Quando você adiciona a conta ao Cloud Manager, o Cloud Manager se refere ao segredo do cliente como a chave do aplicativo.

Passos

1. Abra o serviço **Azure ative Directory**.
2. Clique em **inscrições de aplicativos** e selecione sua inscrição.
3. Clique em **certificados e segredos > segredo de novo cliente**.
4. Forneça uma descrição do segredo e uma duração.
5. Clique em **Add**.
6. Copie o valor do segredo do cliente.

Resultado

Seu responsável de serviço está configurado e você deve ter copiado o ID do aplicativo (cliente), o ID do diretório (locatário) e o valor do segredo do cliente. Você precisa inserir essas informações no Cloud Manager ao adicionar uma conta do Azure.

Adição de credenciais do Azure ao Cloud Manager

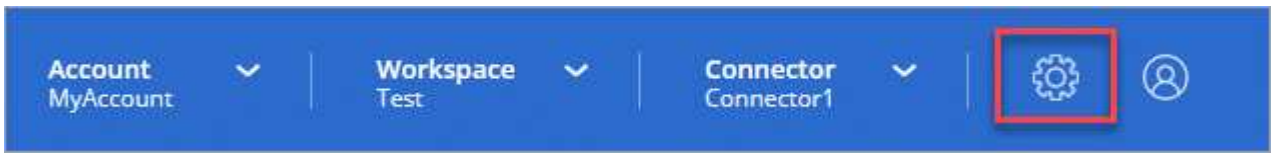
Depois de fornecer uma conta do Azure com as permissões necessárias, você pode adicionar as credenciais dessa conta ao Cloud Manager. Isso permite que você inicie sistemas Cloud Volumes ONTAP nessa conta.

O que você vai precisar

Você precisa criar um conetor antes de alterar as configurações do Cloud Manager. "Saiba como".

Passos

1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **credenciais**.



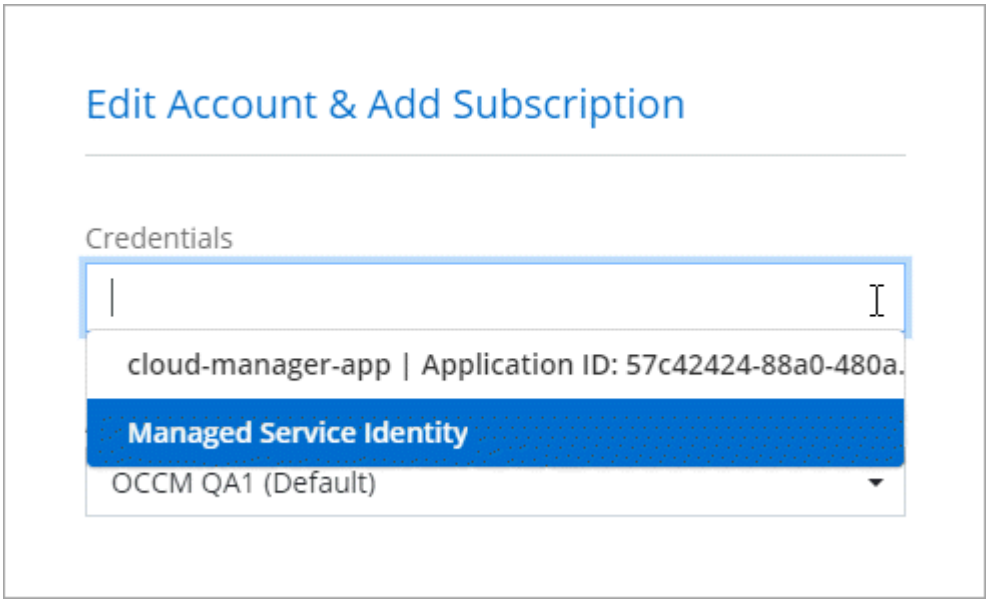
2. Clique em **Adicionar credenciais** e selecione **Microsoft Azure**.
3. Insira informações sobre o principal de serviço do Azure ative Directory que concede as permissões necessárias:
   - ID da aplicação (cliente): Obtendo o ID do aplicativo e o ID do diretórioConsulte .
   - ID do diretório (locatário): Obtendo o ID do aplicativo e o ID do diretórioConsulte .
   - Segredo do cliente: Criando um segredo de clienteConsulte .
4. Confirme se os requisitos da política foram atendidos e clique em **continuar**.
5. Escolha a assinatura paga conforme o uso que você deseja associar às credenciais ou clique em **Adicionar assinatura** se você ainda não tiver uma.

Para criar um sistema Cloud Volumes ONTAP com pagamento conforme o uso, as credenciais do Azure devem estar associadas a uma assinatura do Cloud Volumes ONTAP no mercado Azure.

6. Clique em **Add**.

Resultado

Agora você pode alternar para diferentes conjuntos de credenciais na página Detalhes e credenciais "ao criar um novo ambiente de trabalho":



Associar uma subscrição do Azure Marketplace às credenciais

Depois de adicionar suas credenciais do Azure ao Cloud Manager, você pode associar uma assinatura do Azure Marketplace a essas credenciais. A assinatura permite criar um sistema Cloud Volumes ONTAP com pagamento conforme o uso e usar outros serviços de nuvem da NetApp.

Há dois cenários em que você pode associar uma assinatura do Azure Marketplace depois de já ter adicionado as credenciais ao Cloud Manager:

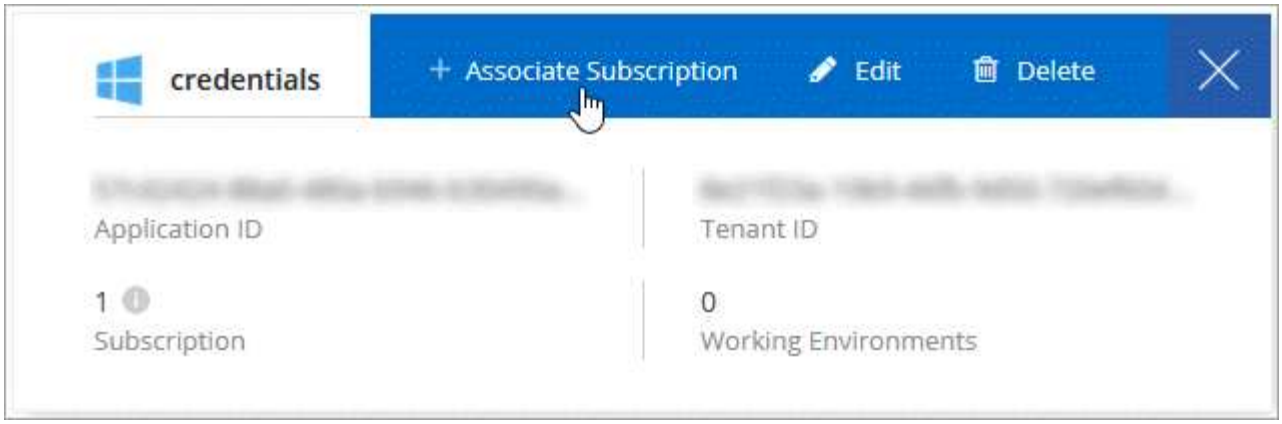
- Você não associou uma assinatura quando adicionou inicialmente as credenciais ao Cloud Manager.
- Você deseja substituir uma assinatura existente do Azure Marketplace por uma nova assinatura.

O que você vai precisar

Você precisa criar um conetor antes de alterar as configurações do Cloud Manager. "Saiba como".

Passos

1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **credenciais**.
2. Passe o Mouse sobre um conjunto de credenciais e clique no menu de ação.
3. No menu, clique em **assinatura associada**.



4. Selecione uma assinatura na lista suspensa ou clique em **Adicionar assinatura** e siga as etapas para criar uma nova assinatura.

   O vídeo a seguir começa no contexto do assistente de ambiente de trabalho, mas mostra o mesmo fluxo de trabalho depois de clicar em **Adicionar assinatura**:

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

Associar subscrições adicionais do Azure a uma identidade gerida

O Cloud Manager permite que você escolha as credenciais do Azure e a assinatura do Azure na qual você deseja implantar o Cloud Volumes ONTAP. Não é possível selecionar uma assinatura diferente do Azure para o perfil de identidade gerenciado, a menos que você associe a "identidade gerenciada" essas assinaturas.

Sobre esta tarefa

Uma identidade gerenciada é "A conta inicial do Azure" quando você implementa um conetor do Cloud Manager. Quando você implantou o conetor, o Cloud Manager criou a função Operador do Cloud Manager e atribuiu-a à máquina virtual do conetor.

Passos

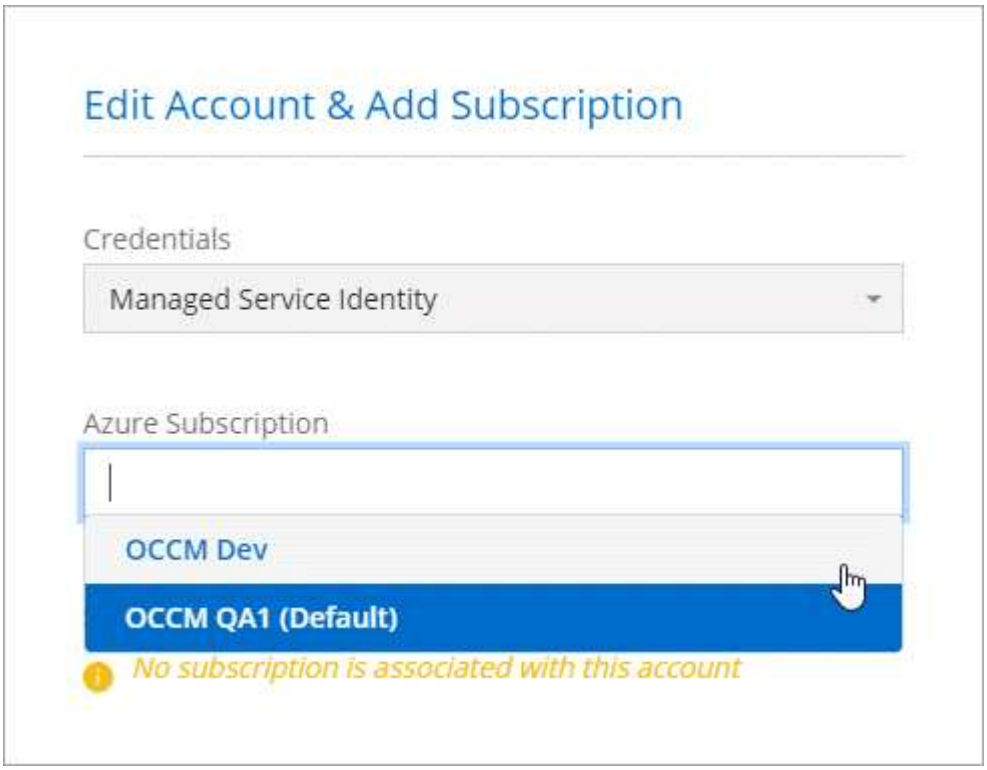
1. Faça login no portal do Azure.
2. Abra o serviço **assinaturas** e selecione a assinatura na qual deseja implantar o Cloud Volumes ONTAP.
3. Clique em **Access Control (IAM)**.
   a. Clique em **Adicionar** > **Adicionar atribuição de função** e, em seguida, adicione as permissões:
      - Selecione a função **Operador do Cloud Manager**.

        Operador do Cloud Manager é o nome padrão fornecido no "Política do Cloud Manager". Se você escolher um nome diferente para a função, selecione esse nome em vez disso.

      - Atribua acesso a uma **Máquina Virtual**.
      - Selecione a assinatura na qual a máquina virtual do conetor foi criada.
      - Selecione a máquina virtual do conetor.
      - Clique em **Salvar**.
4. Repita estes passos para subscrições adicionais.

Resultado

Ao criar um novo ambiente de trabalho, agora você deve ter a capacidade de selecionar entre várias assinaturas do Azure para o perfil de identidade gerenciado.



GCP

Projetos, permissões e contas do Google Cloud

Uma conta de serviço fornece ao Cloud Manager permissões para implantar e gerenciar sistemas Cloud Volumes ONTAP no mesmo projeto que o Cloud Manager ou em projetos diferentes.

Projeto e permissões para o Cloud Manager

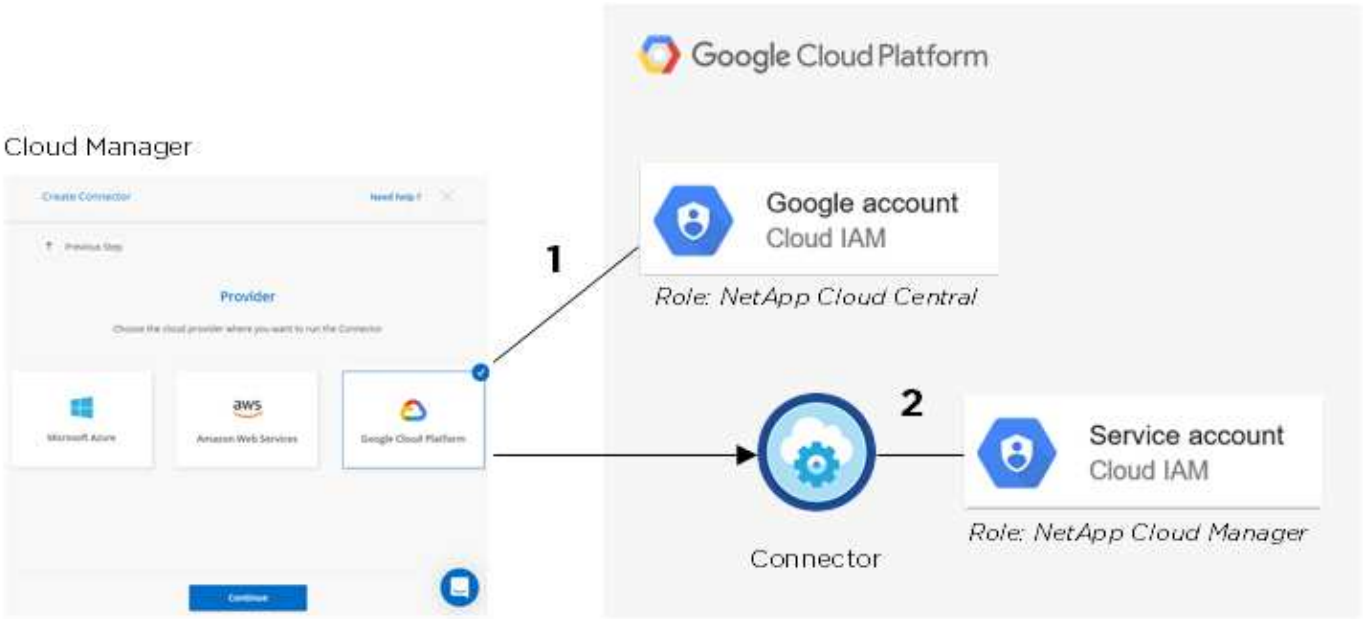
Antes de implantar o Cloud Volumes ONTAP no Google Cloud, você deve primeiro implantar um conetor em um projeto do Google Cloud. O conetor não pode ser executado em suas instalações ou em um provedor de nuvem diferente.

Dois conjuntos de permissões devem estar em vigor antes de implantar um conetor diretamente do Cloud Manager:

1. Você precisa implantar um conetor usando uma conta do Google que tenha permissões para iniciar a instância de VM do Connector do Cloud Manager.
2. Ao implantar o conetor, você será solicitado a selecionar um "conta de serviço" para a instância de VM. O Cloud Manager obtém permissões da conta de serviço para criar e gerenciar sistemas Cloud Volumes ONTAP em seu nome. As permissões são fornecidas anexando uma função personalizada à conta de serviço.

Nós configuramos dois arquivos YAML que incluem as permissões necessárias para o usuário e a conta de serviço. "Saiba como usar os arquivos YAML para configurar permissões".

A imagem a seguir mostra os requisitos de permissão descritos nos números 1 e 2 acima:



Projeto para Cloud Volumes ONTAP

O Cloud Volumes ONTAP pode residir no mesmo projeto que o conetor, ou em um projeto diferente. Para implantar o Cloud Volumes ONTAP em um projeto diferente, você precisa primeiro adicionar a conta de serviço do Connector e a função a esse projeto.

- "Saiba como configurar a conta de serviço (consulte o passo 2)".
- "Saiba como implantar o Cloud Volumes ONTAP no GCP e selecione um projeto".

Conte com a categorização de dados

O Cloud Manager requer uma conta do GCP para o Cloud Volumes ONTAP 9,6, mas não para 9,7 e posterior. Para usar a disposição de dados em categorias com o Cloud Volumes ONTAP 9,7, siga a etapa 4 em "Introdução ao Cloud Volumes ONTAP no Google Cloud Platform".

É necessário adicionar uma conta do Google Cloud ao Cloud Manager para habilitar a disposição de dados em categorias em um sistema Cloud Volumes ONTAP 9,6. A categorização de dados categoriza automaticamente os dados inativos no storage de objetos de baixo custo, permitindo que você recupere espaço no storage primário e diminua o storage secundário.

Ao adicionar a conta, você precisa fornecer ao Cloud Manager uma chave de acesso ao storage para uma conta de serviço que tenha permissões de administrador do storage. O Cloud Manager usa as chaves de acesso para configurar e gerenciar um bucket do Cloud Storage para categorização de dados.

Depois de adicionar uma conta do Google Cloud, é possível habilitar a disposição em categorias de dados em volumes individuais ao criá-los, modificá-los ou replicá-los.

- "Saiba como configurar e adicionar contas do GCP ao Cloud Manager".
- "Saiba como categorizar dados inativos em armazenamento de objetos de baixo custo".

Gerenciamento de credenciais e assinaturas do GCP para o Cloud Manager

Você pode gerenciar dois tipos de credenciais do Google Cloud Platform a partir do Cloud Manager: As credenciais associadas à instância de VM Connector e às chaves de acesso ao storage usadas com um sistema Cloud Volumes ONTAP 9,6 para "categorização de dados".

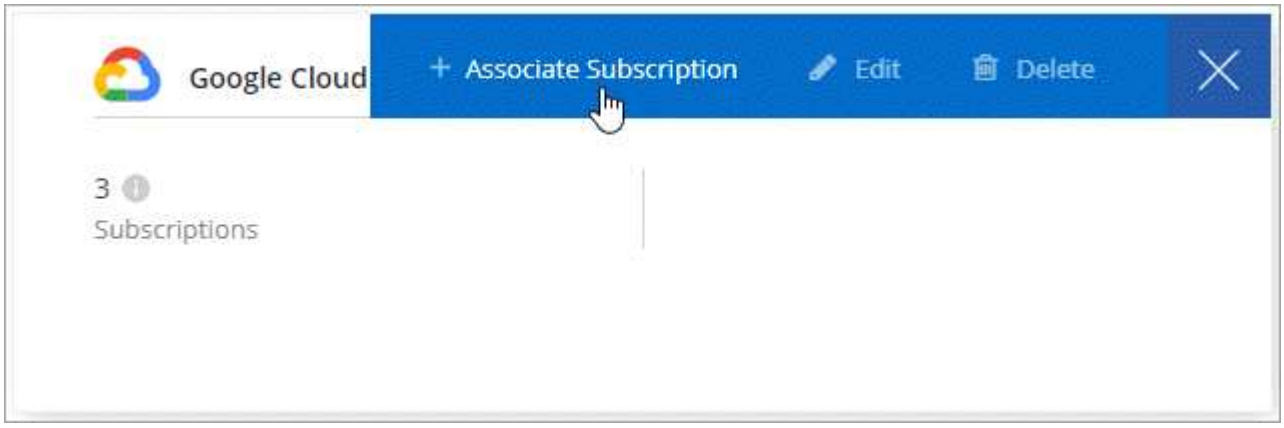
Associar uma assinatura do Marketplace às credenciais do GCP

Ao implantar um conetor no GCP, o Cloud Manager cria um conjunto padrão de credenciais associadas à instância de VM do Connector. Essas são as credenciais que o Cloud Manager usa para implantar o Cloud Volumes ONTAP.

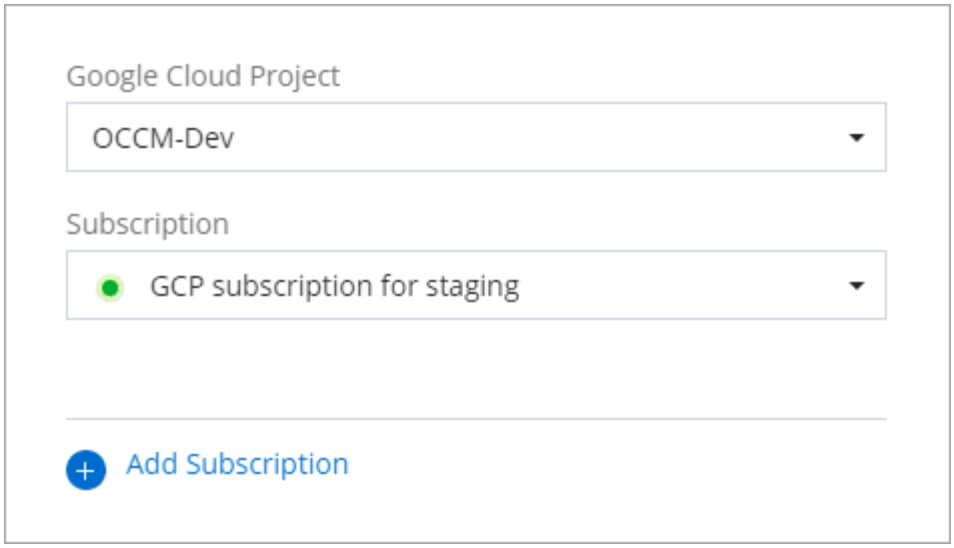
A qualquer momento, você pode alterar a assinatura do Marketplace associada a essas credenciais. A assinatura permite criar um sistema Cloud Volumes ONTAP com pagamento conforme o uso e usar outros serviços de nuvem da NetApp.

Passos

1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **credenciais**.
2. Passe o Mouse sobre um conjunto de credenciais e clique no menu de ação.
3. No menu, clique em **assinatura associada**.



4. Selecione um projeto e uma assinatura do Google Cloud na lista suspensa ou clique em **Adicionar assinatura** e siga as etapas para criar uma nova assinatura.



5. Clique em **Associate**.

Configuração e adição de contas do GCP para categorização de dados com o Cloud Volumes ONTAP 9,6

Se você quiser habilitar um sistema Cloud Volumes ONTAP 9,6 para "categorização de dados", você precisa fornecer ao Cloud Manager uma chave de acesso ao armazenamento para uma conta de serviço que tenha permissões de administrador de armazenamento. O Cloud Manager usa as chaves de acesso para configurar e gerenciar um bucket do Cloud Storage para categorização de dados.

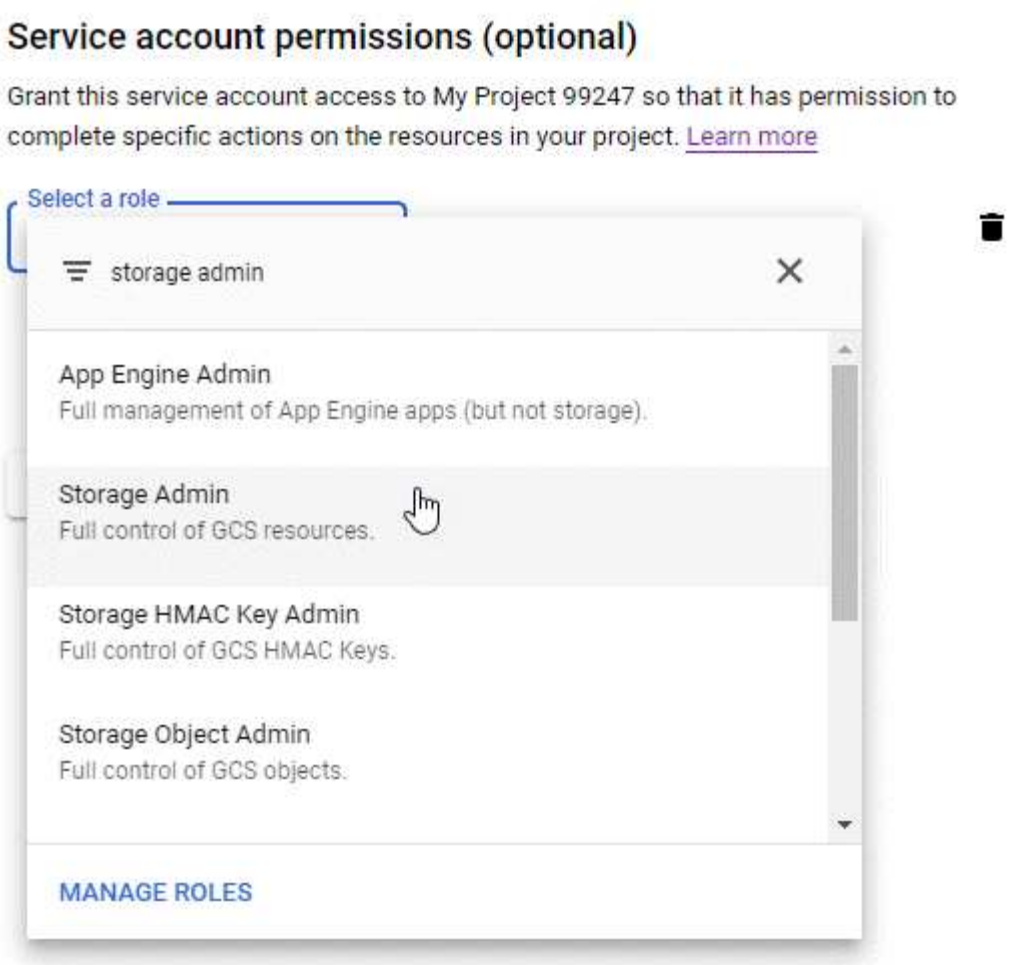
Para usar a disposição de dados em categorias com o Cloud Volumes ONTAP 9,7, siga a etapa 4 em "Introdução ao Cloud Volumes ONTAP no Google Cloud Platform".

Configurar uma conta de serviço e chaves de acesso para o Google Cloud Storage

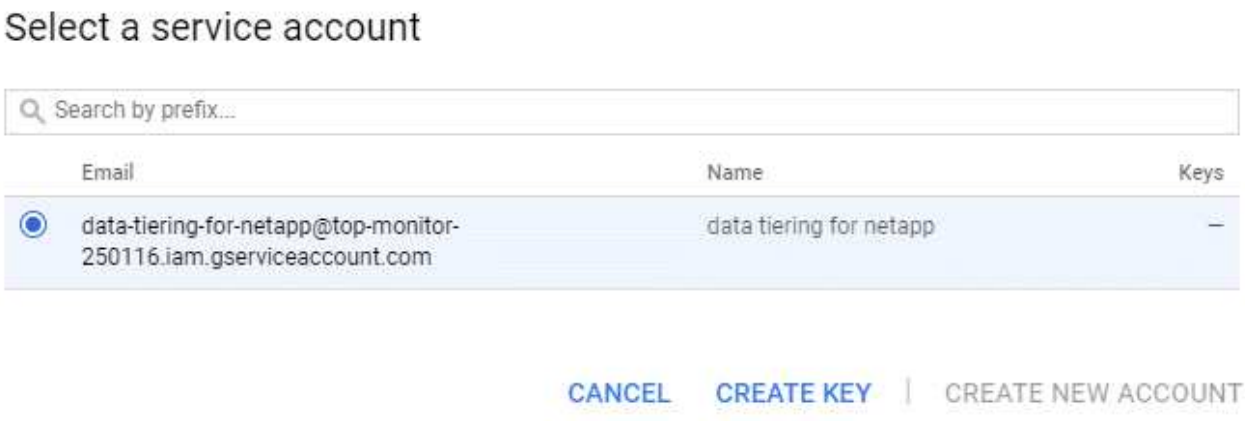
Uma conta de serviço permite que o Cloud Manager autentique e acesse buckets do Cloud Storage usados para categorização de dados. As chaves são necessárias para que o Google Cloud Storage saiba quem está fazendo a solicitação.

Passos

1. Abra o console do IAM do GCP e "Crie uma conta de serviço que tenha a função Administrador do storage"o .



2. Vá para "Configurações de armazenamento do GCP".
3. Se você for solicitado, selecione um projeto.
4. Clique no separador **interoperabilidade**.
5. Se ainda não o tiver feito, clique em **Ativar acesso à interoperabilidade**.
6. Em **chaves de acesso para contas de serviço**, clique em **criar uma chave para uma conta de serviço**.
7. Selecione a conta de serviço criada na etapa 1.



8. Clique em **criar chave**.

9. Copie a chave de acesso e o segredo.

   Você precisará inserir essas informações no Cloud Manager ao adicionar a conta do GCP para categorização de dados.

Adicionando uma conta do GCP ao Cloud Manager

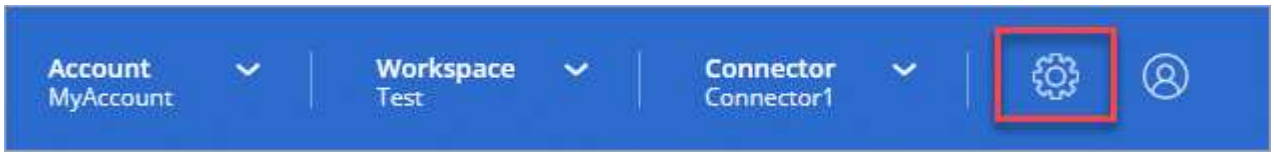
Agora que você tem uma chave de acesso para uma conta de serviço, pode adicioná-la ao Cloud Manager.

O que você vai precisar

Você precisa criar um conetor antes de alterar as configurações do Cloud Manager. "Saiba como".

Passos

1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **credenciais**.



2. Clique em **Adicionar credenciais** e selecione **Google Cloud**.
3. Introduza a chave de acesso e o segredo da conta de serviço.

   As chaves permitem que o Cloud Manager configure um bucket do Cloud Storage para categorização de dados.

4. Confirme se os requisitos da política foram atendidos e clique em **criar conta**.

O que se segue?

Agora é possível habilitar a disposição de dados em categorias em volumes individuais em um sistema Cloud Volumes ONTAP 9,6 ao criá-los, modificá-los ou replicá-los. Para obter detalhes, "Disposição em camadas dos dados inativos em storage de objetos de baixo custo"consulte .

Mas antes de fazer isso, certifique-se de que a sub-rede na qual o Cloud Volumes ONTAP reside esteja configurada para o acesso privado do Google. Para obter instruções, "Documentação do Google Cloud: Configurando o acesso privado do Google" consulte .

Adicionar contas do site de suporte da NetApp ao Cloud Manager

É necessário adicionar sua conta do site de suporte da NetApp ao Cloud Manager para implantar um sistema BYOL. Também é necessário Registrar sistemas pay-as-you-go e atualizar o software ONTAP.

Assista ao vídeo a seguir para saber como adicionar contas do site de suporte da NetApp ao Cloud Manager. Ou role para baixo para ler os passos.

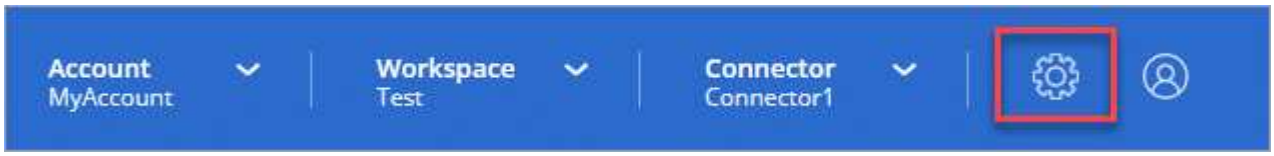
[] | *https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg*

O que você vai precisar

Você precisa criar um conetor antes de alterar as configurações do Cloud Manager. "Saiba como".

Passos

1. Se você ainda não tiver uma conta do site de suporte da NetApp, "registre-se para um".
2. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **credenciais**.



3. Clique em **Adicionar credenciais** e selecione **Site de suporte da NetApp**.
4. Especifique um nome para a conta e, em seguida, introduza o nome de utilizador e a palavra-passe.
   - A conta deve ser uma conta de cliente (não uma conta de convidado ou temporária).
   - Se você planeja implantar sistemas BYOL:
     - A conta deve estar autorizada a acessar os números de série dos sistemas BYOL.
     - Se você comprou uma assinatura BYOL segura, então uma conta NSS segura será necessária.
5. Clique em **criar conta.**

O que se segue?

Os usuários agora podem selecionar a conta ao criar novos sistemas Cloud Volumes ONTAP e ao Registrar sistemas existentes.

- "Iniciando o Cloud Volumes ONTAP na AWS"
- "Iniciar o Cloud Volumes ONTAP no Azure"
- "Registar sistemas de pagamento conforme o uso"
- "Saiba como o Cloud Manager gerencia arquivos de licença"

Gerenciamento de usuários, workspaces, conetores e assinaturas

"Depois de executar a configuração inicial", Talvez seja necessário administrar as configurações da conta posteriormente gerenciando usuários, espaços de trabalho, conetores e assinaturas.

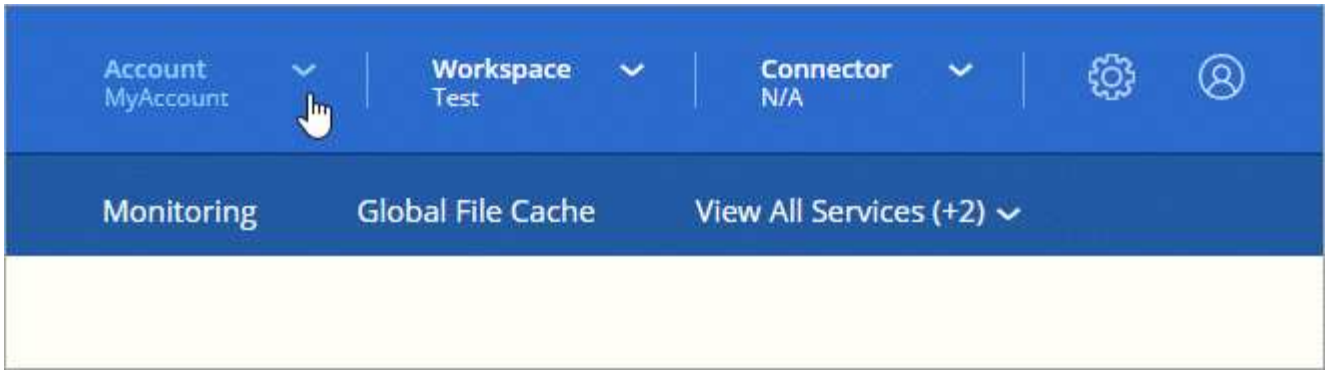
"Saiba mais sobre como as contas do Cloud Central funcionam".

Adicionando usuários

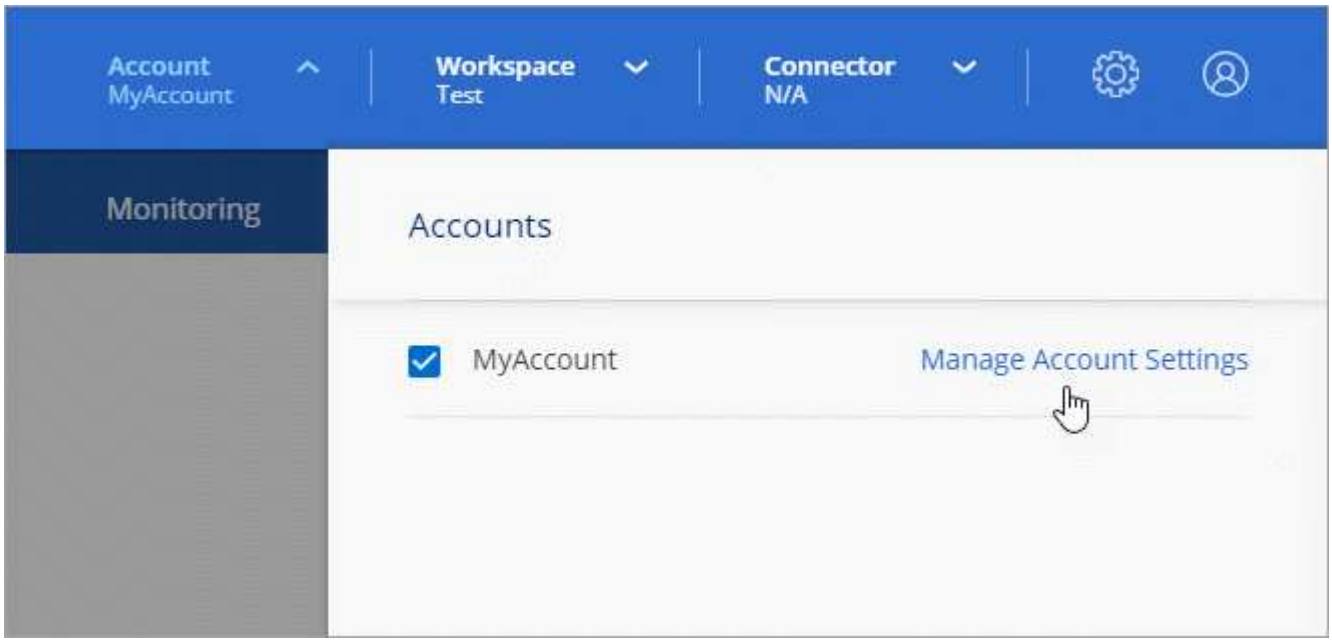
Associe usuários do Cloud Central à conta do Cloud Central para que esses usuários possam criar e gerenciar ambientes de trabalho no Cloud Manager.

Passos

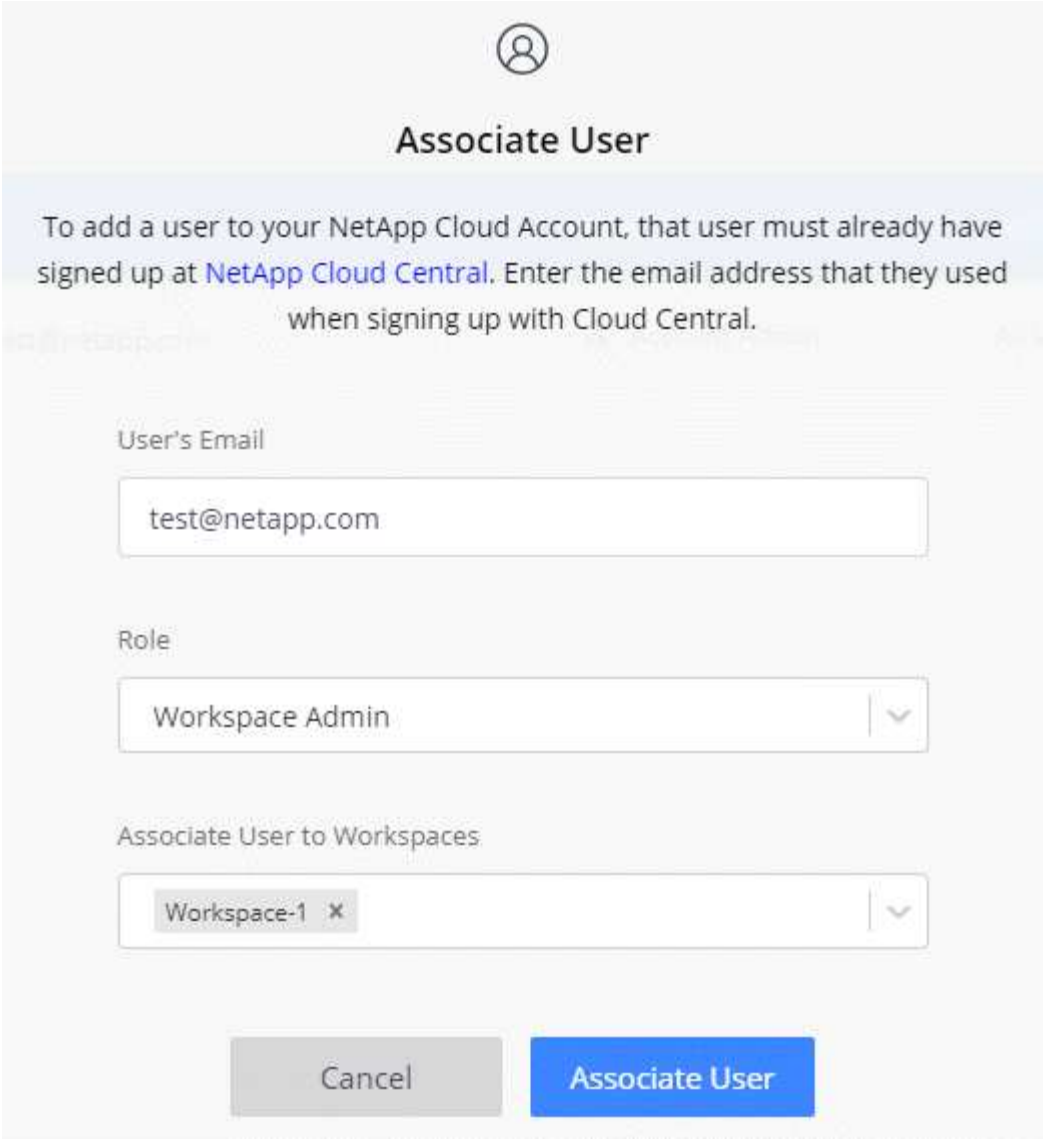
1. Se o usuário ainda não tiver feito isso, peça ao usuário para ir "Centro de nuvem da NetApp" e se inscrever.
2. Na parte superior do Cloud Manager, clique no menu suspenso **Account**.



3. Clique em **Gerenciar conta** ao lado da conta selecionada no momento.



4. Na guia usuários, clique em **Usuário associado**.
5. Insira o endereço de e-mail do usuário e selecione uma função para o usuário:
   - **Admin da conta**: Pode executar qualquer ação no Cloud Manager.
   - **Workspace Admin**: Pode criar e gerenciar recursos em workspaces atribuídos.
   - **Visualizador de conformidade**: Só pode visualizar informações de conformidade e gerar relatórios para espaços de trabalho que eles têm permissão para acessar.
6. Se você selecionou Workspace Admin ou Compliance Viewer, selecione um ou mais workspaces para associar a esse usuário.



7. Clique em **Usuário associado**.

Resultado

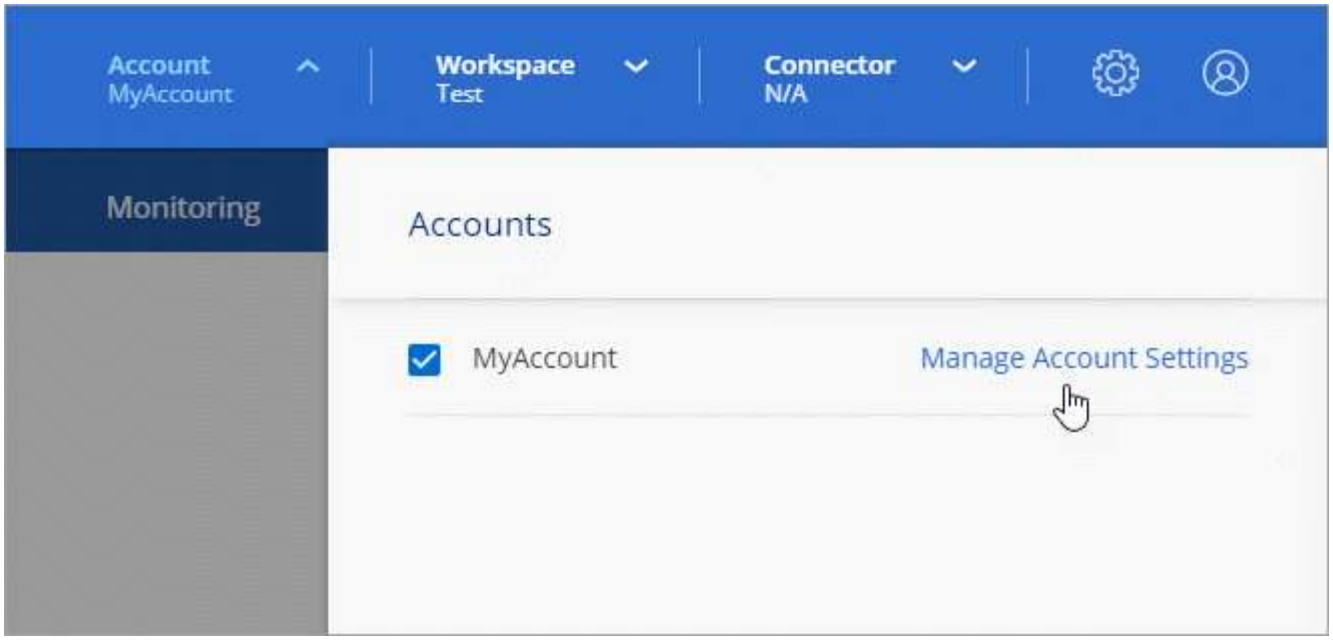
O usuário deve receber um e-mail do NetApp Cloud Central intitulado "Associação de Contas". O e-mail inclui as informações necessárias para acessar o Cloud Manager.

Removendo usuários

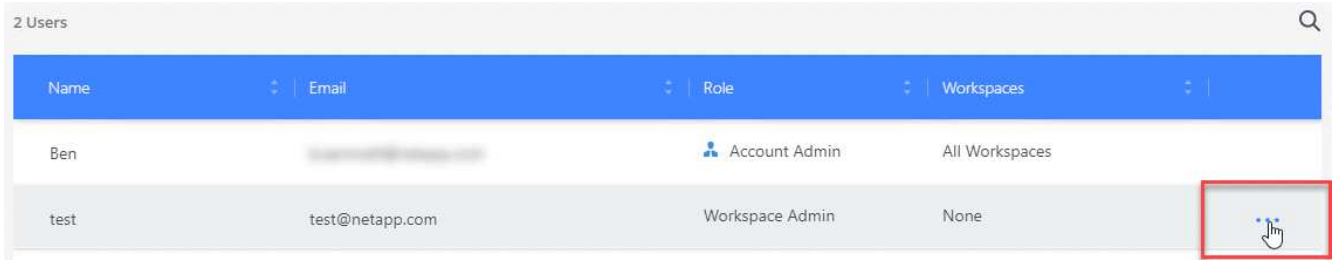
A desassociação de um usuário faz com que ele não possa mais acessar os recursos em uma conta do Cloud Central.

Passos

1. Na parte superior do Cloud Manager, clique no menu suspenso **Account** e clique em **Manage Account**.



2. Na guia usuários, clique no menu de ação na linha que corresponde ao usuário.



3. Clique em **Disassocie User** e clique em **Disassocie** para confirmar.

Resultado

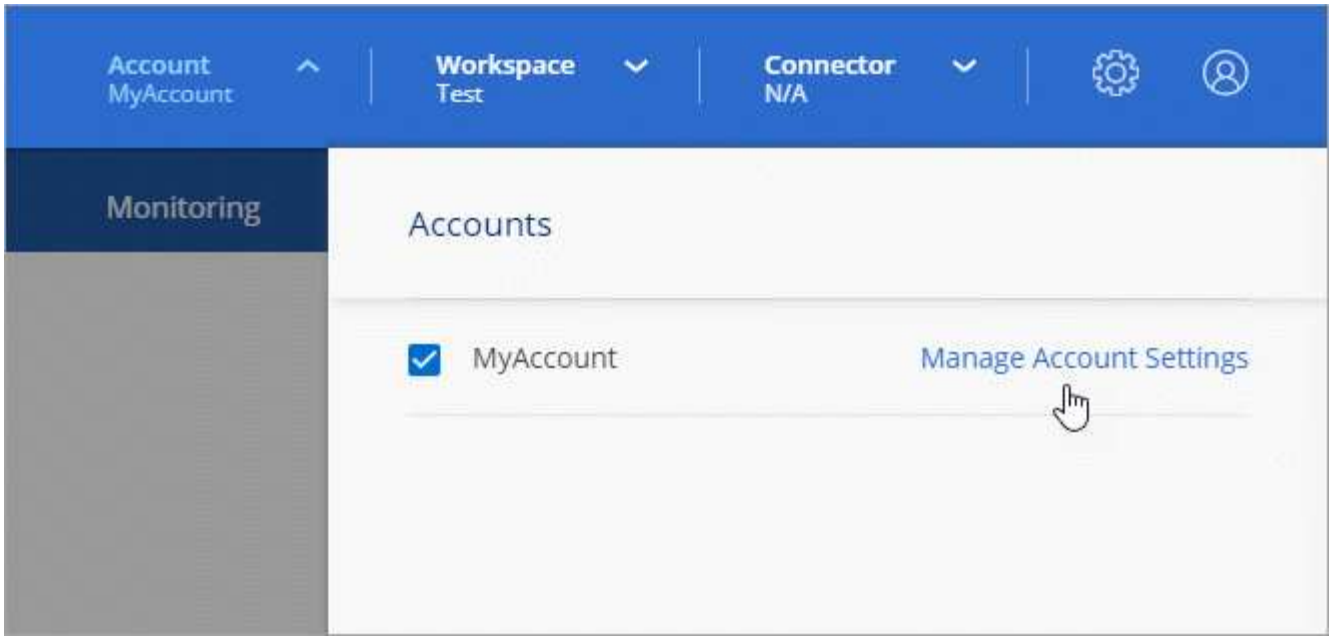
O usuário não pode mais acessar os recursos dessa conta do Cloud Central.

Gerenciando os workspaces de um administrador do espaço de trabalho

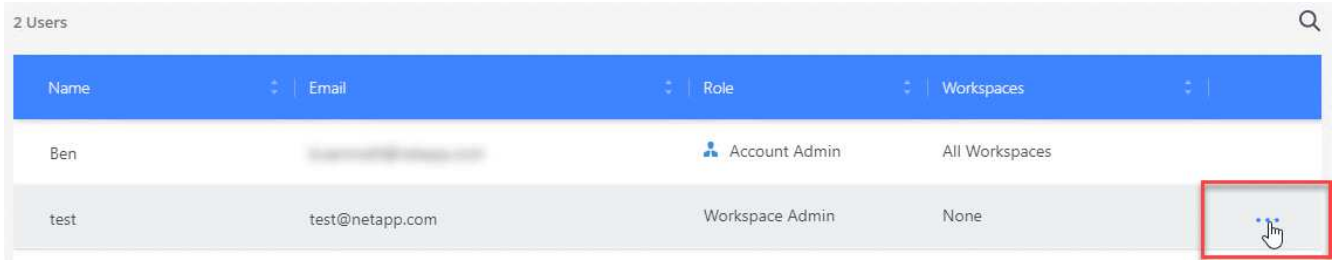
Você pode associar e desassociar administradores do Workspace a workspaces a qualquer momento. Associar o usuário permite que ele crie e visualize os ambientes de trabalho nesse espaço de trabalho.

Passos

1. Na parte superior do Cloud Manager, clique no menu suspenso **Account** e clique em **Manage Account**.



2. Na guia usuários, clique no menu de ação na linha que corresponde ao usuário.



3. Clique em **Gerenciar espaços de trabalho**.
4. Selecione os espaços de trabalho a associar ao utilizador e clique em **aplicar**.

Resultado

O usuário agora pode acessar esses workspaces a partir do Cloud Manager, desde que o conetor também esteja associado aos workspaces.

Gerenciando espaços de trabalho

Gerencie seus workspaces criando, renomeando e excluindo-os. Observe que não é possível excluir um workspace se ele contiver recursos. Deve estar vazio.

Passos

1. Na parte superior do Cloud Manager, clique no menu suspenso **Account** e clique em **Manage Account**.
2. Clique em **Workspaces**.
3. Escolha uma das seguintes opções:
   - Clique em **Adicionar novo espaço de trabalho** para criar um novo espaço de trabalho.
   - Clique em **Renomear** para renomear a área de trabalho.
   - Clique em **Excluir** para excluir a área de trabalho.

Gerenciando espaços de trabalho de um conetor

Você precisa associar o conetor aos workspaces para que os administradores do Workspace possam acessar esses workspaces a partir do Cloud Manager.

Se você tiver apenas administradores de conta, associar o conetor com workspaces não será necessário. Administradores de conta têm a capacidade de acessar todos os espaços de trabalho no Cloud Manager por padrão.

"Saiba mais sobre usuários, workspaces e conetores".

Passos

1. Na parte superior do Cloud Manager, clique no menu suspenso **Account** e clique em **Manage Account**.
2. Clique em **Connector**.
3. Clique em **Manage Workspaces** (gerir espaços de trabalho) para o conetor que pretende associar.
4. Selecione os espaços de trabalho a associar ao conetor e clique em **Apply**.

Gerenciamento de assinaturas

Depois de se inscrever no marketplace de um provedor de nuvem, cada assinatura estará disponível no widget Configurações de conta. Você tem a opção de renomear uma assinatura e desassociar a assinatura de uma ou mais contas.

Por exemplo, digamos que você tem duas contas e cada uma é cobrada através de assinaturas separadas. Você pode desassociar uma assinatura de uma das contas para que os usuários dessa conta não escolham acidentalmente a assinatura errada ao criar um ambiente de trabalho do Cloud volume ONTAP.

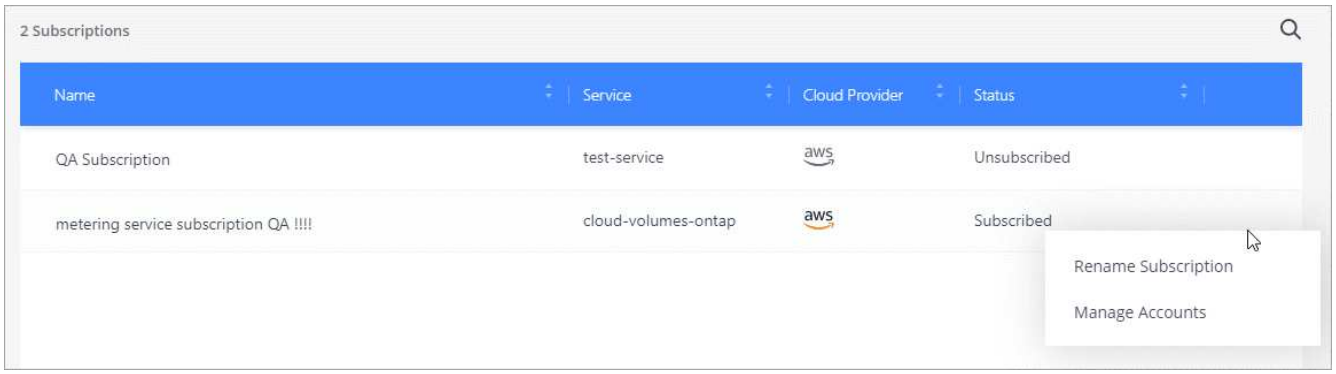
"Saiba mais sobre assinaturas".

Passos

1. Na parte superior do Cloud Manager, clique no menu suspenso **Account** e clique em **Manage Account**.
2. Clique em **Subscrições**.

   Você só verá as assinaturas associadas à conta que você está visualizando no momento.

3. Clique no menu de ação na linha que corresponde à assinatura que você deseja gerenciar.



4. Escolha para renomear a assinatura ou gerenciar as contas associadas à assinatura.

Alterar o nome da conta

Altere o nome da sua conta a qualquer momento para alterá-lo para algo significativo para você.

Passos

1. Na parte superior do Cloud Manager, clique no menu suspenso **Account** e clique em **Manage Account**.
2. Na guia **Visão geral**, clique no ícone de edição ao lado do nome da conta.
3. Digite um novo nome de conta e clique em **Salvar**.

Ativar ou desativar a plataforma SaaS

Não recomendamos desativar a plataforma SaaS a menos que você precise para cumprir com as políticas de segurança da sua empresa. Desativar a plataforma SaaS limita sua capacidade de usar os serviços de nuvem integrados da NetApp.

Os serviços a seguir não estarão disponíveis no Cloud Manager se você desativar a plataforma SaaS:

- Conformidade com a nuvem
- Kubernetes
- Disposição em camadas na nuvem
- Cache de arquivos global
- Monitoramento (Cloud Insights)

Passos

1. Na parte superior do Cloud Manager, clique no menu suspenso **Account** e clique em **Manage Account**.
2. Na guia **Visão geral**, alterne a opção para ativar o uso da plataforma SaaS.

Gerenciamento de um certificado HTTPS para acesso seguro

Por padrão, o Cloud Manager usa um certificado autoassinado para acesso HTTPS ao console da Web. Você pode instalar um certificado assinado por uma autoridade de certificação (CA), que fornece melhor proteção de segurança do que um certificado autoassinado.

Antes de começar

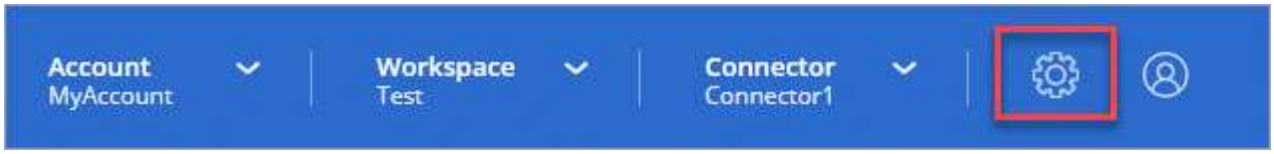
Você precisa criar um conetor antes de alterar as configurações do Cloud Manager. "Saiba como".

Instalar um certificado HTTPS

Instale um certificado assinado por uma CA para acesso seguro.

Passos

1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **Configuração HTTPS**.

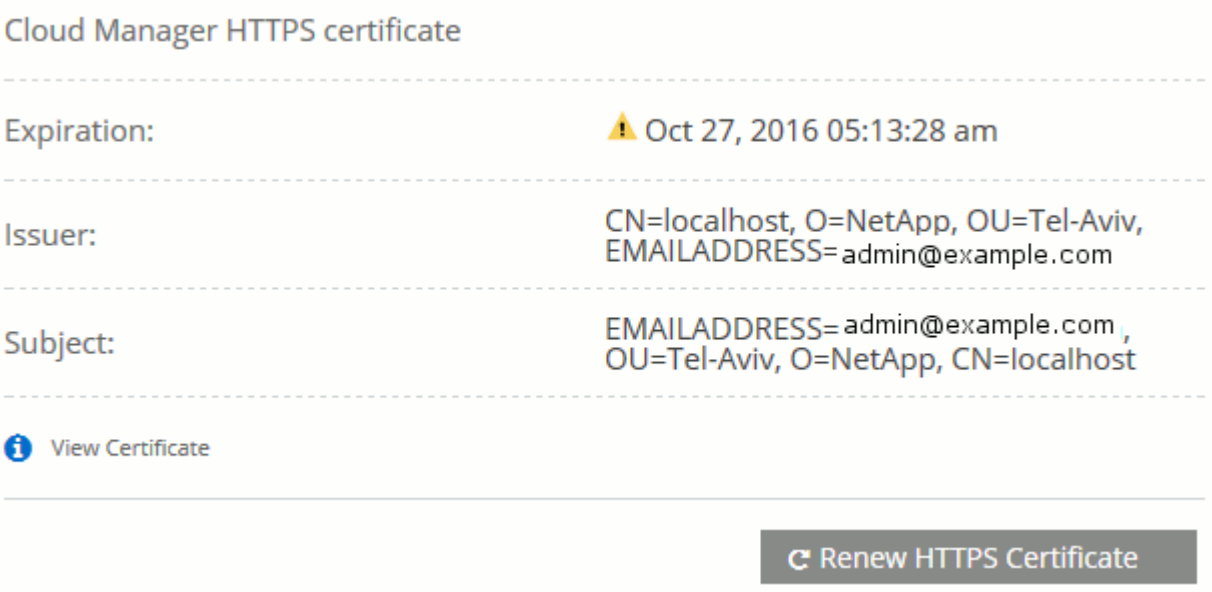


2. Na página Configuração HTTPS, instale um certificado gerando uma solicitação de assinatura de certificado (CSR) ou instalando seu próprio certificado assinado pela CA:

Opção	Descrição
Gerar um CSR	a. Insira o nome do host ou DNS do host do conetor (seu Nome Comum) e clique em **Generate CSR**. O Cloud Manager exibe uma solicitação de assinatura de certificado. b. Use o CSR para enviar uma solicitação de certificado SSL a uma CA. O certificado deve usar o formato X,509 codificado base-64 de Email Avançado de Privacidade (PEM). c. Copie o conteúdo do certificado assinado, cole-o no campo certificado e clique em **Instalar**.
Instale o seu próprio certificado assinado pela CA	a. Selecione **Instalar certificado assinado pela CA**. b. Carregue o arquivo de certificado e a chave privada e, em seguida, clique em **Install**. O certificado deve usar o formato X,509 codificado base-64 de Email Avançado de Privacidade (PEM).

Resultado

O Cloud Manager agora usa o certificado assinado pela CA para fornecer acesso HTTPS seguro. A imagem a seguir mostra um sistema do Cloud Manager configurado para acesso seguro:



Renovando o certificado HTTPS do Cloud Manager

Você deve renovar o certificado HTTPS do Cloud Manager antes de expirar para garantir acesso seguro ao console da Web do Cloud Manager. Se você não renovar o certificado antes que ele expire, um aviso será exibido quando os usuários acessarem o console da Web usando HTTPS.

Passos

1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **Configuração HTTPS**.

   Detalhes sobre os relatórios do certificado do Cloud Manager, incluindo a data de expiração.

2. Clique em **renovar certificado HTTPS** e siga as etapas para gerar um CSR ou instalar seu próprio certificado assinado pela CA.

Resultado

O Cloud Manager usa o novo certificado assinado pela CA para fornecer acesso HTTPS seguro.

Remoção de ambientes de trabalho do Cloud Volumes ONTAP

O administrador da conta pode remover um ambiente de trabalho do Cloud Volumes ONTAP para movê-lo para outro sistema ou para solucionar problemas de descoberta.

Sobre esta tarefa

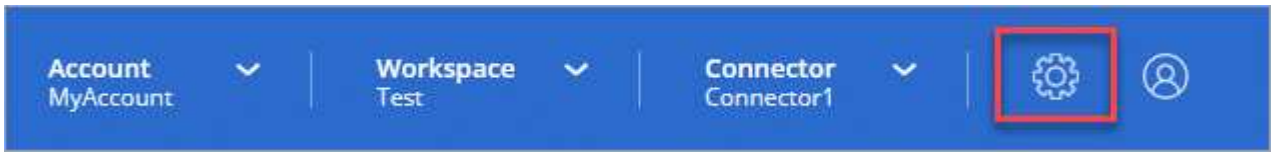
A remoção de um ambiente de trabalho do Cloud Volumes ONTAP remove-o do Cloud Manager. Ele não exclui o sistema Cloud Volumes ONTAP. Mais tarde, você pode redescobrir o ambiente de trabalho.

A remoção de um ambiente de trabalho do Cloud Manager permite que você faça o seguinte:

- Redescubra-o em outro espaço de trabalho
- Redescubra-o a partir de outro sistema Cloud Manager
- Redescubra se você teve problemas durante a descoberta inicial

Passos

1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **Ferramentas**.



2. Na página Ferramentas, clique em **Iniciar**.
3. Selecione o ambiente de trabalho do Cloud Volumes ONTAP que deseja remover.
4. Na página Revisão e aprovação, clique em **ir**.

Resultado

O Cloud Manager remove o ambiente de trabalho. Os usuários podem redescobrir esse ambiente de trabalho a partir da página ambientes de trabalho a qualquer momento.

Configurando um conetor para usar um servidor proxy

Se suas políticas corporativas determinarem que você usa um servidor proxy para toda a comunicação HTTP com a Internet, então você deve configurar seus conetores para usar esse servidor proxy. O servidor proxy pode estar na nuvem ou na rede.

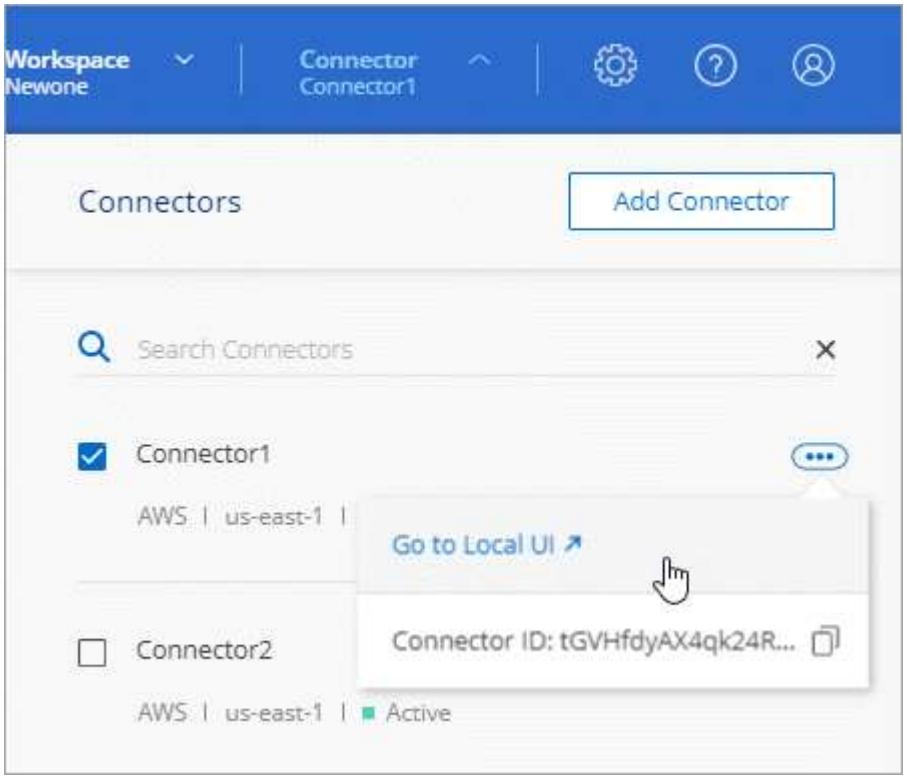
Quando você configura um conetor para usar um servidor proxy, esse conetor e os sistemas Cloud Volumes ONTAP que ele gerencia (incluindo quaisquer mediadores de HA), todos usam o servidor proxy.

Passos

1. "Faça login na interface SaaS do Cloud Manager" De uma máquina que tenha uma conexão de rede com a instância do conetor.

   Se o conetor não tiver um endereço IP público, você precisará de uma conexão VPN ou precisará se conetar a partir de um host de salto que esteja na mesma rede que o conetor.

2. Clique no menu suspenso **Connector** e clique em **Go to local UI** para obter um conetor específico.



   A interface do Cloud Manager em execução no conetor é carregada em uma nova guia do navegador.

3. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **Configurações do Cloud Manager**.

4. Em Proxy HTTP, digite o servidor usando a sintaxe http://address:port, especifique um nome de usuário e senha se a

autenticação básica for necessária para o servidor e clique em Salvar.

O Cloud Manager não suporta senhas que incluem o caractere A.

Resultado

Depois de especificar o servidor proxy, os novos sistemas Cloud Volumes ONTAP são configurados automaticamente para usar o servidor proxy ao enviar mensagens AutoSupport. Se você não especificou o servidor proxy antes que os usuários criem sistemas Cloud Volumes ONTAP, eles devem usar o Gerenciador do sistema para definir manualmente o servidor proxy nas opções do AutoSupport para cada sistema.

Substituindo bloqueios CIFS para o Cloud Volumes ONTAP HA no Azure

O administrador de conta pode habilitar uma configuração no Gerenciador de nuvem que impede problemas com failover de storage do Cloud Volumes ONTAP durante eventos de manutenção do Azure. Quando você ativa essa configuração, o Cloud Volumes ONTAP veta o CIFS bloqueia e redefine as sessões ativas do CIFS.

Sobre esta tarefa

O Microsoft Azure agenda eventos de manutenção periódica em suas máquinas virtuais. Quando ocorre um evento de manutenção em um nó em um par de HA do Cloud Volumes ONTAP, o par de HA inicia o takeover do storage. Se houver sessões CIFS ativas durante esse evento de manutenção, os bloqueios em arquivos CIFS podem impedir o failover de armazenamento.

Se ativar esta definição, o Cloud Volumes ONTAP vetará os bloqueios e redefinirá as sessões CIFS ativas. Como resultado, o par de HA pode concluir o failover de storage durante esses eventos de manutenção.

Esse processo pode ser disruptivo para clientes CIFS. Os dados que não forem comprometidos com clientes CIFS podem ser perdidos.

O que você vai precisar

Você precisa criar um conetor antes de alterar as configurações do Cloud Manager. "Saiba como".

Passos

1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **Configurações do Cloud Manager**.

2. Em **HA CIFS Locks**, marque a caixa de seleção e clique em **Save**.

Referência

Funções

As funções Admin da conta, Admin do espaço de trabalho e Visualizador de conformidade na nuvem fornecem permissões específicas aos usuários.

Tarefa	Administrador da conta	Admin da área de trabalho	Visualizador de conformidade na nuvem
Gerenciar ambientes de trabalho	Sim	Sim	Não
Ativar serviços em ambientes de trabalho	Sim	Sim	Não
Exibir status de replicação de dados	Sim	Sim	Não
Veja a linha do tempo	Sim	Sim	Não
Alterne entre espaços de trabalho	Sim	Sim	Sim
Ver os resultados da verificação de conformidade	Sim	Sim	Sim
Eliminar ambientes de trabalho	Sim	Não	Não
Conecte clusters do Kubernetes a ambientes de trabalho	Sim	Não	Não
Receba o relatório Cloud Volumes ONTAP	Sim	Não	Não
Crie conetores	Sim	Não	Não
Gerenciar contas do Cloud Central	Sim	Não	Não
Gerenciar credenciais	Sim	Não	Não
Modifique as configurações do Cloud Manager	Sim	Não	Não
Visualize e gerencie o Painel de suporte	Sim	Não	Não
Remova os ambientes de trabalho do Cloud Manager	Sim	Não	Não
Instale um certificado HTTPS	Sim	Não	Não

Links relacionados

- "Configurando espaços de trabalho e usuários na conta do Cloud Central"
- "Gerenciamento de espaços de trabalho e usuários na conta do Cloud Central"

Como o Cloud Manager usa permissões de provedor de nuvem

O Cloud Manager requer permissões para executar ações no seu provedor de nuvem. Essas permissões estão incluídas no "As políticas fornecidas pela NetApp". você pode

querer entender o que o Cloud Manager faz com essas permissões.

O que o Cloud Manager faz com as permissões da AWS

O Cloud Manager usa uma conta da AWS para fazer chamadas de API para vários serviços da AWS, incluindo EC2, S3, CloudFormation, IAM, o Security Token Service (STS) e o Key Management Service (KMS).

Ações	Finalidade
"EC2:StartInstances", "EC2:StopInstances", "EC2:DescribeInstances", "EC2:DescribeInstanceStatus", "EC2:RunInstances", "EC2:TerminateInstances", "EC2:ModifyInstanceAttribute",	Inicia uma instância do Cloud Volumes ONTAP e pára, inicia e monitora a instância.
"EC2:DescribeInstanceAttribute",	Verifica se a rede aprimorada está habilitada para tipos de instâncias compatíveis.
"EC2:DescribeRouteTables", "EC2:DescribeImages",	Inicia uma configuração Cloud Volumes ONTAP HA.
"EC2:CreateTags",	Marca todos os recursos que o Cloud Manager cria com as tags "WorkingEnvironment" e "WorkingEnvironmentId". O Cloud Manager usa essas tags para manutenção e alocação de custos.
"EC2:Createvolume", "EC2:DescribeVolumes", "EC2:ModifyVolumeAttribute", "EC2:Attachvolume", "EC2:Deletevolume", "EC2:Detachvolume",	Gerencia os volumes do EBS que o Cloud Volumes ONTAP usa como armazenamento back-end.
"EC2:CreateSecurityGroup", "EC2:DeleteSecurityGroup", "EC2:DescribeSecurityGroups", "EC2:RevokeSecurityGroupEgress", "EC2:AuthorizeSecurityGroupEgress", "EC2:AuthorizeSecurityGroupIngress", "EC2:RevokeSecurityGroupIngress",	Cria grupos de segurança predefinidos para o Cloud Volumes ONTAP.
"EC2:CreateNetworkInterface", "EC2:DescribeNetworkInterfaces", "EC2:DeleteNetworkInterface", "EC2:ModifyNetworkInterfaceAttribute",	Cria e gerencia interfaces de rede para Cloud Volumes ONTAP na sub-rede de destino.
"EC2:DescribeSubnets", "EC2:DescribeVPCs",	Obtém a lista de sub-redes de destino e grupos de segurança, que é necessário ao criar um novo ambiente de trabalho para o Cloud Volumes ONTAP.
"EC2:DescribeDhcpOptions",	Determina os servidores DNS e o nome de domínio padrão ao iniciar instâncias do Cloud Volumes ONTAP.
"EC2:CreateSnapshot", "EC2:DeleteSnapshot", "EC2:DescribeSnapshots",	Tira instantâneos dos volumes do EBS durante a configuração inicial e sempre que uma instância do Cloud Volumes ONTAP é interrompida.
"EC2:GetConsoleOutput",	Captura o console do Cloud Volumes ONTAP, que está conetado às mensagens do AutoSupport.

Ações	Finalidade
"EC2:DescribeKeyPairs",	Obtém a lista de pares de chaves disponíveis ao iniciar instâncias.
"EC2:DescribeRegiões",	Obtém uma lista de regiões da AWS disponíveis.
"EC2:DeleteTags", "EC2:DescribeTags",	Gerencia tags para recursos associados às instâncias do Cloud Volumes ONTAP.
"Cloudformation:CreateStack", "cloudformation:DeleteStack", "cloudformation:DescribeStacks", "cloudformation:DescribeStackEvents", "cloudformation:ValidateTemplate",	Inicia instâncias do Cloud Volumes ONTAP.
"IAM:PassRole", "IAM:CreateRole", "IAM:DeleteRole", "IAM:PutRolePolicy", "IAM:CreateInstanceProfile", "IAM:DeleteRolePolicy", "iam:RoleAddToInstanceProfile", "iam:RemveRoleDeInstanceInstanceProfile", "iam:DeleteProfile", "iam:DeleteAddOutreAddOutreAddToInstanceProfile"	Inicia uma configuração Cloud Volumes ONTAP HA.
"iam:ListInstanceProfiles", "STS:DedeAuthorizationMessage", "EC2:AssociateIamInstanceProfile", "EC2:DescribeIamInstanceAssociations", "EC2:DisassociateIamInstanceProfile", "DescribeIamInstanceProfile",	Gerencia perfis de instâncias para instâncias do Cloud Volumes ONTAP.
"S3:GetBucketTagging", "S3:GetBucketLocation", "S3:ListAllMyBuckets", "S3:ListBucket"	Obtém informações sobre os buckets do AWS S3 para que o Cloud Manager possa se integrar ao serviço NetApp Data Fabric Cloud Sync.
"S3 S3:CreateBucket", "S3 S3 S3:DeleteBucket", "S3 S3:GetLifecycleConfiguration", "S3:PutLifecycleConfiguration", "S3:PutBucketTagging", "S3:ListBucketVersions", "S3:GetBucketPolicyStatus"	Gerencia o bucket do S3 usado pelo sistema Cloud Volumes ONTAP como uma camada de capacidade para categorização de dados.
"Kms:Lista*", "kms:Recriptografar*", "kms:descrever*", "kms:CreateGrant",	Permite a criptografia de dados do Cloud Volumes ONTAP usando o AWS Key Management Service (KMS).
"ce:GetReservationUtilization", "ce:GetDimensionValues", "ce:GetCostAndUsage", "ce:GetTags"	Obtém dados de custo da AWS para o Cloud Volumes ONTAP.
"EC2:CreatePlacementGroup", "EC2:DeletePlacementGroup"	Ao implantar uma configuração de HA em uma única zona de disponibilidade da AWS, o Cloud Manager inicia os dois nós de HA e o mediador em um grupo de posicionamento de spread da AWS.
"EC2:DescribeReservedInstancesOferings"	O Cloud Manager usa a permissão como parte da implantação do Cloud Compliance para escolher qual tipo de instância usar.

Ações	Finalidade
"S3 S3 S3:DeleteBucket", "S3 S3 S3 S3:GetLifecycleConfiguration", "S3 S3 S3 S3:PutLifecycleConfiguration", "S3:PutBucketTagging", "S3:ListBucketVersions", "S3:GetObject", "S3	O Cloud Manager usa essas permissões quando você ativa o serviço Backup to S3.

O que o Cloud Manager faz com as permissões do Azure

A política do Azure inclui as permissões que o Cloud Manager precisa para implantar e gerenciar o Cloud Volumes ONTAP no Azure.

Ações	Finalidade
"Microsoft.Compute/locations/operations/read", "Microsoft.Compute/locations/vmSizes/read", "Microsoft.Compute/operations/read", "Microsoft.Compute/virtualMachines/instanceView/read", "Microsoft.Compute/virtualMachines/powerOff/action", "Microsoft.Compute/virtualMachines/read", "Microsoft.Compute/virtualMachines/restart/action", "Microsoft.Compute/virtualMachines/start/action", "Microsoft.Compute/virtualMachines/deallocate/action", "Microsoft.Compute/virtualMachines/vmSizes/read","Microsoft.Compute/virtualMachines/write",	Cria Cloud Volumes ONTAP e pára, inicia, exclui e obtém o status do sistema.
"Microsoft.Compute/images/write", "Microsoft.Compute/images/read",	Permite a implantação do Cloud Volumes ONTAP a partir de um VHD.
"Microsoft.Compute/disks/delete", "Microsoft.Compute/disks/read", "Microsoft.Compute/disks/write", "Microsoft.Storage/checknameavailability/read", "Microsoft.Storage/operations/read", "Microsoft.Storage/storageAccounts/listkeys/action", "Microsoft.Storage/storageAccounts/read", "Microsoft.Storage	Gerencia contas e discos de armazenamento do Azure e anexa os discos ao Cloud Volumes ONTAP.
"Microsoft.Network/networkInterfaces/read", "Microsoft.Network/networkInterfaces/write", "Microsoft.Network/networkInterfaces/join/action",	Cria e gerencia interfaces de rede para Cloud Volumes ONTAP na sub-rede de destino.
"Microsoft.Network/networkSecurityGroups/read", "Microsoft.Network/networkSecurityGroups/write", "Microsoft.Network/networkSecurityGroups/join/action",	Cria grupos de segurança de rede predefinidos para o Cloud Volumes ONTAP.

Ações	Finalidade
"Microsoft.resources/Subscrições/locations/read", "Microsoft.Network/locations/operationResults/read", "Microsoft.Network/locations/operations/read", "Microsoft.Network/virtualNetworks/read", "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read", "Microsoft.Network/virtualNetworks/subnets/read", "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read", "Microsoft.Network/virtualNetworks/virtualMachines/read", "Microsoft.Network/virtualNetworks/subnets/join/action",	Obtém informações de rede sobre regiões, a rede VNet de destino e a sub-rede e adiciona Cloud Volumes ONTAP aos VNets.
"Microsoft.Network/virtualNetworks/subnets/write", "Microsoft.Network/routeTables/join/action",	Habilita pontos de extremidade do serviço VNet para categorização de dados.
"Microsoft.resources/deployments/operations/read", "Microsoft.resources/deployments/deployments/write",	Implanta o Cloud Volumes ONTAP a partir de um modelo.
"Microsoft.resources/deploys/operations/read", "Microsoft.resources/deployments/deployments/write", "Microsoft.resources/resources/resources/lease", "Microsoft.resources	Cria e gerencia grupos de recursos para o Cloud Volumes ONTAP.
"Microsoft.Compute/snapshots/write", "Microsoft.Compute/snapshots/read", "Microsoft.Compute/disks/beginGetAccess/action"	Cria e gerencia snapshots gerenciados do Azure.
"Microsoft.Compute/availabilitySets/write", "Microsoft.Compute/availabilitySets/read",	Cria e gerencia conjuntos de disponibilidade para o Cloud Volumes ONTAP.
"Microsoft.MarketplaceOrdering/offertypes/publishers/offertyes/offertyes/offertyes/offertyes/offerments/plans/agreements/write"	Habilita implantações programáticas no Azure Marketplace.
"Microsoft.Network/loadBalancers/read", "Microsoft.Network/loadBalancers/write", "Microsoft.Network/loadBalancers/delete", "Microsoft.Network/loadBalancers/backendAddressPools/read", "Microsoft.Network/loadBalancers/backendAddressPools/join/action", "Microsoft.Network/loadBalancers/frontendIPConfigurations/read", "Microsoft.Network/loadBalancers/loadBalancingRules/read", "Microsoft.Network/loadBalancers/probes/read", "Microsoft.Network/loadBalancers/probes/join/action","	Gerencia um balanceador de carga do Azure para pares de HA.
"Microsoft.Authorization/Locks/*"	Permite o gerenciamento de bloqueios em discos Azure.
"Microsoft.Authorization/roleDefinitions/write", "Microsoft.Authorization/roleAssignments/write", "Microsoft.Web/Sites/*"	Gerencia o failover em pares de HA.

Ações	Finalidade
"Microsoft.Network/privateEndpoints/write", "Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action", "Microsoft.Storage/storageAccounts/privateEndpointConnections/read", "Microsoft.Network/privateEndpoints/read", "Microsoft.Network/privateDnsZones/write", "Microsoft.Network/privateDnsZones/virtualNetworkLinks/write", "Microsoft.Network/virtualNetworks/join/action", "Microsoft.Network/privateDnsZones/A/write", "Microsoft.Network/privateDnsZones/read", "Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",""	Permite o gerenciamento de endpoints privados. Os endpoints privados são usados quando a conetividade não é fornecida para fora da sub-rede. O Cloud Manager cria a conta de storage para HA com apenas conetividade interna na sub-rede.
"Microsoft.NetApp/netAppAccount/capacityPools/volumes/delete",	Permite que o Cloud Manager exclua volumes para Azure NetApp Files.
"Microsoft.resources/deployments/operationStatuses/read"	O Azure requer essa permissão para algumas implantações de máquinas virtuais (depende do hardware físico subjacente usado durante a implantação).
"Microsoft.resources/deployments/operationStatuses/read", "Microsoft.Insights/Metrics/Read", "Microsoft.Compute/virtualMachines/extensions/write", "Microsoft.Compute/virtualMachines/extensions/read", "Microsoft.Compute/virtualMachines/extensions/delete", "Microsoft.Compute/virtualMachines/delete", "Microsoft.Network/networkInterfaces/delete", "Microsoft.Network/networkSecurityGroups/delete", "Microsoft.resources/deployments/delete",	Permite que você use o Global File Cache.
"Microsoft.Compute/diskEncryptionSets/read"	Permite que o Cloud Manager criptografe discos gerenciados do Azure em sistemas Cloud Volumes ONTAP de nó único usando chaves externas de outra conta. Esse recurso é compatível com APIs.

O que o Cloud Manager faz com as permissões do GCP

A política do Cloud Manager do GCP inclui as permissões necessárias para implantar e gerenciar o Cloud Volumes ONTAP.

Ações	Finalidade
- Compute.disks.create - Compute.disks.createSnapshot - compute.disks.delete - Compute.disks.get - Compute.disks.list - compute.disks.setLabels - compute.disks.use.	Para criar e gerenciar discos para Cloud Volumes ONTAP.
- compute.firewalls.create - compute.firewalls.delete - compute.firewalls.get - compute.firewalls.list	Para criar regras de firewall para o Cloud Volumes ONTAP.

Ações	Finalidade
- Compute.globalOperations.get	Para obter o status das operações.
- Compute.images.get - Compute.images.getFromFamily - Compute.images.list - compute.images.useReadOnly	Para obter imagens para instâncias de VM.
- compute.instances.attachDisk - compute.instances.detachDisk	Para anexar e desanexar discos ao Cloud Volumes ONTAP.
- compute.instances.create - compute.instances.delete	Para criar e excluir instâncias de VM do Cloud Volumes ONTAP.
- compute.instances.get	Para listar instâncias de VM.
- compute.instances.getSerialPortOutput	Para obter logs de console.
- compute.instances.list	Para recuperar a lista de instâncias em uma zona.
- compute.instances.setDeletionProtection	Para definir a proteção de exclusão na instância.
- compute.instances.setLabels	Para adicionar etiquetas.
- compute.instances.setMachineType	Para alterar o tipo de máquina para Cloud Volumes ONTAP.
- compute.instances.setMetadata	Para adicionar metadados.
- compute.instances.setTags	Para adicionar etiquetas para regras de firewall.
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Para iniciar e parar o Cloud Volumes ONTAP.
- Compute.machineTypes.get	Para obter os números de núcleos para verificar qoutas.
- compute.projects.get	Para apoiar multi-projetos.
- Compute.snapshots.create - compute.snapshots.delete - Compute.snapshots.get - Compute.snapshots.list - compute.snapshots.setLabels	Para criar e gerenciar snapshots persistentes em disco.
- compute.networks.get - compute.networks.list - Compute.regions.get - Compute.regions.list - Compute.subnetworks.get - Compute.subnetworks.list - Compute.zoneOperations.get - Compute.zones.get - Compute.zones.list	Para obter as informações de rede necessárias para criar uma nova instância de máquina virtual Cloud Volumes ONTAP.
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - deploymentmanager.manifests.get - deploymentmanager.manifests.list - deploymentmanager.operations.get - deploymentmanager.operations.list	Para implantar a instância de máquina virtual do Cloud Volumes ONTAP usando o Gerenciador de implantação do Google Cloud.
- LogEntries.list - logging.privateLogEntries.list	Para obter unidades de log de pilha.

Ações	Finalidade
- resourcemanager.projects.get	Para apoiar multi-projetos.
- storage.buckets.create - storage.buckets.delete - storage.buckets.get - storage.buckets.list - storage.buckets.update	Para criar e gerenciar um bucket do Google Cloud Storage para categorização de dados.
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.list - cloudkms.keyrings.list	Para usar chaves de criptografia gerenciadas pelo cliente a partir do Serviço de gerenciamento de chaves na nuvem com o Cloud Volumes ONTAP.
- compute.instances.setServiceAccount - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list	Para definir uma conta de serviço na instância do Cloud Volumes ONTAP. Essa conta de serviço fornece permissões para categorização de dados em um bucket do Google Cloud Storage.

Páginas do AWS Marketplace para o Cloud Manager e o Cloud Volumes ONTAP

Várias ofertas estão disponíveis no AWS Marketplace for Cloud Manager e no Cloud Volumes ONTAP. Se precisar de ajuda para entender o propósito de cada página, leia as descrições abaixo.

Em todos os casos, lembre-se de que você não pode iniciar o Cloud Volumes ONTAP no AWS a partir do AWS Marketplace. Você precisa iniciá-lo diretamente do Cloud Manager.

Meta	Página do AWS Marketplace para usar	Mais informações
Habilite o uso do Cloud Volumes ONTAP PAYGO, disposição em camadas na nuvem, conformidade com a nuvem e outros serviços complementares	"Gerenciador de nuvem - implantar Gerenciar Serviços de dados de nuvem da NetApp"	Esta subscrição permite o carregamento da versão PAYGO do Cloud Volumes ONTAP 9,6 e posterior. Ele também permite cobrança pelo Cloud Tiering, pelo Cloud Compliance e por outros serviços complementares. Você deve assinar essa oferta quando o Cloud Manager solicitar e redirecioná-lo para a página. O Cloud Manager solicita no assistente de ambiente de trabalho ou quando você adiciona novas credenciais nas Configurações. Esta página não permite que você inicie o Cloud Manager na AWS. Isso deve ser feito a partir de "Centro de nuvem da NetApp", ou, alternativamente, usando o AMI listado na linha 3 desta tabela.

Meta	Página do AWS Marketplace para usar	Mais informações
Habilite o uso do Cloud Volumes ONTAP PAYGO, disposição em camadas na nuvem, conformidade com a nuvem e outros serviços complementares *usando um contrato anual*	"Gerenciador de nuvem (contratos) - implantar Gerenciar serviços de dados de nuvem da NetApp"	Esta subscrição é uma alternativa à subscrição na primeira linha. Ele permite que você obtenha um pagamento antecipado anual para os anúncios. É principalmente para parceiros da NetApp.
Implante o Cloud Manager no AWS Marketplace usando uma AMI	"Cloud Manager - Instalação manual sem chaves de acesso"	Recomendamos que você inicie o Cloud Manager na AWS a partir "Centro de nuvem da NetApp"do , mas você pode iniciá-lo a partir desta página do AWS Marketplace, se preferir.
Ativar a implantação do Cloud Volumes ONTAP PAYGO (9,5 ou anterior)	• "Cloud Volumes ONTAP para AWS" • "Cloud Volumes ONTAP para AWS: Alta disponibilidade"	Essas páginas do AWS Marketplace permitem que você assine as versões de nó único ou HA do Cloud Volumes ONTAP PAYGO para as versões 9,5 e anteriores. A partir da versão 9,6, você precisa se inscrever na página do AWS Marketplace listada na linha 1 desta tabela para implantações PAYGO.

Use APIs e automação

Recursos de automação para infraestrutura como código

Use os recursos desta página para obter ajuda para integrar o Cloud Manager e o Cloud Volumes ONTAP ao "infraestrutura como código" seu .

As equipes de DevOps usam diversas ferramentas para automatizar a configuração de novos ambientes, o que permite que elas tratem a infraestrutura como código. Uma dessas ferramentas é o Terraform. Desenvolvemos um fornecedor Terraform que as equipes de DevOps podem usar com o Cloud Manager para automatizar e integrar o Cloud Volumes ONTAP à infraestrutura como código.

"Veja o provedor NetApp-cloudmmanager".

- Ligações relacionadas*
- "Blog da nuvem NetApp: Usando APIs REST do Cloud Manager com acesso federado"
- "Blog de nuvem da NetApp: Automação da nuvem com Cloud Volumes ONTAP e REST"
- "Blog de nuvem da NetApp: Clonagem automatizada de dados para testes baseados na nuvem de aplicações de software"
- "Blog do NetApp: Aceleração da infraestrutura como código (IAC) com NetApp"
- "NetApp thePub: Gerenciamento de configuração Automação com Ansible"
- "NetApp thePub: Funções para uso do Ansible ONTAP"

Onde obter ajuda e encontrar mais informações

Você pode obter ajuda e encontrar mais informações sobre o Cloud Manager e o Cloud Volumes ONTAP por meio de vários recursos, incluindo vídeos, fóruns e suporte.

- "Suporte à NetApp Cloud Volumes ONTAP"

  Acesse recursos de suporte para obter ajuda e solucionar problemas com o Cloud Volumes ONTAP.

- "Vídeos para Cloud Manager e Cloud Volumes ONTAP"

  Assista a vídeos que mostram como implantar e gerenciar o Cloud Volumes ONTAP e como replicar dados na nuvem híbrida.

- "Políticas para o Cloud Manager"

  Baixe arquivos JSON que incluem as permissões que o Cloud Manager precisa para executar ações em um provedor de nuvem.

- "Guia do desenvolvedor de API do Cloud Manager"

  Leia uma visão geral das APIs, exemplos de como usá-las e uma referência de API.

- Treinamento para Cloud Volumes ONTAP
  - "Fundamentos do Cloud Volumes ONTAP"
  - "Implantação e gerenciamento do Cloud Volumes ONTAP para Azure"
  - "Implantação e gerenciamento do Cloud Volumes ONTAP para AWS"
- Relatórios técnicos
  - "Relatório Técnico da NetApp 4383: Caraterização de desempenho do Cloud Volumes ONTAP em Serviços Web da Amazon com cargas de trabalho de aplicativos"
  - "Relatório técnico da NetApp 4671: Caraterização de desempenho do Cloud Volumes ONTAP no Azure com cargas de trabalho de aplicação"
  - "Relatório técnico da NetApp 4816: Caraterização de desempenho do Cloud Volumes ONTAP para o Google Cloud"
- Recuperação de desastres da SVM

  A recuperação de desastres do SVM é o espelhamento assíncrono dos dados da SVM e da configuração de uma fonte SVM para um SVM de destino. Você pode ativar rapidamente um SVM de destino para acesso aos dados se a fonte SVM não estiver mais disponível.

  - "Guia expresso de preparação para recuperação de desastres da Cloud Volumes ONTAP 9 SVM"

    Descreve como configurar rapidamente um SVM de destino em preparação para a recuperação de desastres.

  - "Guia expresso de recuperação de desastres da Cloud Volumes ONTAP 9 SVM"

    Descreve como ativar rapidamente um SVM de destino após um desastre e, em seguida, reativar o SVM de origem.

- "Guia de energia do FlexCache volumes para acesso mais rápido aos dados"

  Descreve como criar e gerenciar volumes do FlexCache no mesmo cluster ou cluster diferente do volume de origem para acelerar o acesso aos dados.

- "Avisos de segurança"

  Identificar vulnerabilidades conhecidas (CVEs) para produtos NetApp, incluindo ONTAP. Observe que você pode corrigir vulnerabilidades de segurança para o Cloud Volumes ONTAP seguindo a documentação do ONTAP.

- "Centro de Documentação do ONTAP 9"

  Acesse a documentação do produto para o ONTAP, que pode ajudá-lo enquanto você usa o Cloud Volumes ONTAP.

- "Comunidade NetApp: Serviços de dados em nuvem"

  Conete-se com colegas, faça perguntas, troque ideias, encontre recursos e compartilhe as melhores práticas.

- "Centro de nuvem da NetApp"

  Encontre informações sobre produtos e soluções adicionais da NetApp para a nuvem.

- "Documentação do produto NetApp"

  Procure na documentação do produto NetApp instruções, recursos e respostas.

Versões anteriores da documentação do Cloud Manager

A documentação para versões anteriores do Cloud Manager está disponível caso você não esteja executando a versão mais recente.

- "Cloud Manager 3,7"
- "Cloud Manager 3,6"

Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

Direitos de autor

http://www.netapp.com/us/legal/copyright.aspx

Marcas comerciais

NetApp, o logotipo DA NetApp e as marcas listadas na página de marcas comerciais da NetApp são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respetivos proprietários.

http://www.netapp.com/us/legal/netapptmlist.aspx

Patentes

Uma lista atual de patentes de propriedade da NetApp pode ser encontrada em:

https://www.netapp.com/us/media/patents-page.pdf

Política de privacidade

https://www.netapp.com/us/legal/privacypolicy/index.aspx

Código aberto

Os arquivos de aviso fornecem informações sobre direitos autorais de terceiros e licenças usadas no software NetApp.

- "Aviso para o Cloud Manager 3.8.7"
- "Aviso para o Cloud Manager 3.8.6"
- "Aviso para o Cloud Manager 3.8.5"
- "Aviso para o Cloud Manager 3.8.4"
- "Aviso para o Cloud Manager 3.8.3"
- "Aviso para o Cloud Manager 3.8.2"
- "Aviso para o Cloud Manager 3.8.1"
- "Aviso para o Cloud Manager 3,8"
- "Aviso para o Cloud Backup Service"
- "Aviso para Global File Cache"
- "Aviso para conformidade com a nuvem"

Informações sobre direitos autorais

Informações sobre marcas comerciais